

ENTERPRISE INFORMATION SYSTEMS ||

ENTERPRISE INFORMATION SYSTEMS – A CAPSULE FOR QUICK REVISION

The capsule on Intermediate Paper 7A: Enterprise Information Systems that covers the entire syllabus of the subject is another step of Board of Studies in its endeavour to provide quality academic inputs to the Intermediate students of Chartered Accountancy Course. This concise capsule of the subject intends to assist students in their quick revision of the subject and should not be taken as a substitute for the detailed study of the subject. Students are advised to refer to the relevant Study Material and Revision Test Paper for comprehensive study and revision.

CHAPTER 1: AUTOMATED BUSINESS PROCESSES

This chapter deals with the basic concepts of Business Process, its automation and implementation; risks and controls associated with various business processes and provides comprehensive knowledge about the specific Regulatory and Compliance requirements of The Companies Act and The IT Act.

An **Enterprise Information System (EIS)** may be defined as any kind of information system which improves the functions of an enterprise business processes by integration. This means classically offering high quality services, dealing with large volumes of data and capable of supporting some huge and possibly complex organization or enterprise. All parts of EIS should be usable at all levels of an enterprise as relevant. A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal.

Categories of Business Processes		
Operational Processes	Supporting Processes	Management Processes
Operational or Primary Processes deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives.	Supporting Processes back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety.	Management Processes measure, monitor and control activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting and infrastructure or capacity management.
Example - Order to Cash (O2C) cycle.	Example- HR Process	Example - Budgeting

BUSINESS PROCESS AUTOMATION (BPA)

Business Process Automation (BPA) is the tactic a business uses to automate processes to operate efficiently and effectively.

CONFIDENTIALITY

To ensure that data is only available to persons who have right to see the same.

INTEGRITY

To ensure that no unauthorized amendments can be made in data.

BPA Objectives

AVAILABILITY

To ensure that data is available when asked for.

TIMELINESS

To ensure that data is made available at the right time.

Benefits of Automating Business Processes

QUALITY & CONSISTENCY

- Ensures that every action is performed identically - resulting in high quality, reliable results and stakeholders consistently experience the same level of service.

TIME SAVING

- Automation reduces the number of tasks employees would otherwise need to do manually, thus allowing innovation and increasing employees' levels of motivation.

VISIBILITY

- Automated processes are controlled and consistently operate accurately within the defined timeline. It gives visibility of the process status to the organization.

IMPROVED OPERATIONAL EFFICIENCY

- Automation reduces the time it takes to achieve a task, the effort required to undertake it and the cost of completing it successfully.
- Automation not only ensures systems run smoothly and efficiently, but that errors are eliminated and that best practices are constantly leveraged.

GOVERNANCE & RELIABILITY

- The consistency of automated processes means stakeholders can rely on business processes to operate and offer reliable processes to customers, maintaining a competitive advantage.

REDUCED TURNAROUND TIMES

- Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection.
- This adjustment of processes distills operational performance and reduces the turnaround times for both staff and external customers.

REDUCED COSTS

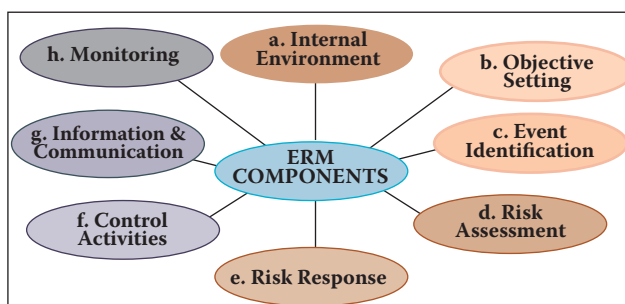
- Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more. Automation allows us to accomplish more by utilizing fewer resources.

Steps involved in the Implementation of BPA

- | | |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1: Define why we plan to implement BPA? | The answer to this question will provide justification for implementing BPA. |
| Step 2: Understand rules/regulation under which it needs to comply with? | The underlying issue is that any BPA created needs to comply with applicable laws and regulations. |
| Step 3: Document the process, we wish to automate. | The current processes which are planned to be automated need to be correctly and completely documented at this step. |
| Step 4: Define the objectives/goals to be achieved by implementing BPA. | This enables the developer and user to understand the reasons for going for BPA. The goals need to be precise and clear. |
| Step 5: Engage business process consultant. | Once the entity has been able to define the above, the entity needs to appoint an expert, who can implement it for the entity. |

ENTERPRISE INFORMATION SYSTEMS

Step 6: Calculate the RoI for project.	The answer to this question can be used for convincing top management to say 'yes' to the BPA exercise.
Step 7: Development of BPA.	Once the top management grant their approval, the right business solution has to be procured and implemented or developed and implemented covering necessary BPA.
Step 8: Testing the BPA.	Before making the process live, the BPA solutions should be fully tested.



ENTERPRISE RISK MANAGEMENT (ERM)

May be defined as a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Benefits of Enterprise Risk Management (ERM)

Align risk appetite and strategy	Risk appetite is degree of risk, on a broad-based level that an enterprise is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
Link growth, risk and return	Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
Enhance risk response decisions	ERM provides the rigor to identify and select among alternative risk responses - risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
Minimize operational surprises and losses	Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
Identify and manage cross-enterprise risks	Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
Provide integrated responses to multiple risks	Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.
Seize opportunities	Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
Rationalize capital	More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

a. Internal Environment	Encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
b. Objective Setting	ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.
c. Event Identification	Event identification includes identifying factors - internal and external - that influence how potential events may affect strategy implementation and achievement of objectives.
d. Risk Assessment	Identified risks are analyzed to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected.
e. Risk Response	Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of strategy and objectives.
f. Control Activities	Policies and procedures are established and executed to help ensure that the risk responses management selected, are effectively carried out.
g. Information and Communication	Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities.
h. Monitoring	Monitoring is accomplished through ongoing management activities, separate evaluations of the ERM processes or a combination of the both.

RISKS AND CONTROLS

Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence.

Risks of Business Process Automation		Types of Business Risks	
Input & Access	All input transaction data may not be accurate, complete and authorised.	Strategic	Risk that would prevent an organisation from accomplishing its objectives.
File & Data Transmission	All files and data transmitted may not be processed accurately and completely, due to network error.	Financial	Risk that could result in a negative financial impact to the organisation.

ENTERPRISE INFORMATION SYSTEMS ||

Risks of Business Process Automation		Types of Business Risks	
Output	Is not complete and accurate due to program error or bugs and is distributed to unauthorised personnel due to weak access control.	Reputational	Risk that could expose the organisation to negative publicity.
Processing	Valid input data may not have been processed accurately and completely due to program error or bugs.	Regulatory (Compliance)	Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.
Data	Master data and transaction data may be changed by unauthorised personnel due to weak access control.	Operational	Risk that could prevent the organisation from operating in the most effective and efficient manner or be disruptive to other operations.
Infrastructure	All data & programs could be lost if there is no proper backup in the event of a disaster and the business could come to a standstill.		

Control	Defined as policies, procedures, practices and organisation structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.
Internal Controls	<ul style="list-style-type: none"> These are a system consisting of specific policies and procedures; Designed to provide management with reasonable assurance that the goals and objectives it believes important to the entity, will be met.
An Internal Control System	<ul style="list-style-type: none"> Facilitates the effectiveness and efficiency of operations. Helps ensure the reliability of internal and external financial reporting. Assists compliance with applicable laws and regulations. Helps safeguarding the assets of the entity.

COMPONENTS OF INTERNAL CONTROL	
Control Environment	Set of standards, processes, and structures that provide the basis for carrying out internal control across the organisation.
Risk Assessment	This forms the basis for determining how risks will be managed. A precondition to risk assessment is establishment of objectives, linked at different levels of entity.
Control Activities	Actions established through policies and procedures that ensure management's directives to mitigate risks to the achievement of objectives are carried out.
Information and Communication	Communication is the continual, iterative process of providing, sharing & obtaining necessary information.
Monitoring of Controls	Ongoing evaluations, separate evaluations, or some combination of two are used to ascertain whether each of five components of internal control, including controls are present and functioning.

Controls should be checked at the following three levels

Configuration

- Refers to the methodical process of defining options that are provided.
- Defines how software functions and what menu options are displayed.

Masters

- Refers to the way various parameters are set up for all modules of software like Purchase, Sales, Inventory, Finance etc.
- Set up first time during installation and these are changed whenever the business process rules or parameters are changed.
- Examples are Vendor Master, Customer Master, Material Master, Accounts Master, Employee Master etc.

Transactions

- Refers to the actual transactions entered through menus and functions in the application software, through which all transactions for specific modules are initiated, authorized or approved.
- For example: Sales transactions, Purchase transactions, Stock transfer transactions, Journal entries and Payment transactions.

BUSINESS PROCESSES - DIAGRAMMATIC REPRESENTATION

Flowcharts

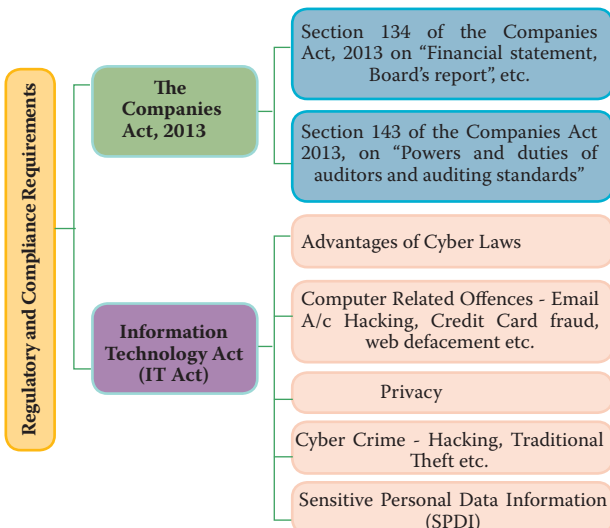
Are used in designing and documenting simple processes or programs. Like other types of diagrams, they help visualize what is going on and thereby help understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it.

Data Flow Diagrams (DFDs)

DFD basically provides an overview of:

- What data a system processes;
- What transformations are performed;
- What data are stored; and
- What results are produced and where they flow.

REGULATORY AND COMPLIANCE REQUIREMENTS



Section 134 of the Companies Act, 2013 on "Financial statement, Board's report, etc." states inter alia: The Directors' Responsibility Statement referred to in clause (c) of sub-section (3) shall state that:

The Directors had taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of this Act for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities; The Directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

|| ENTERPRISE INFORMATION SYSTEMS

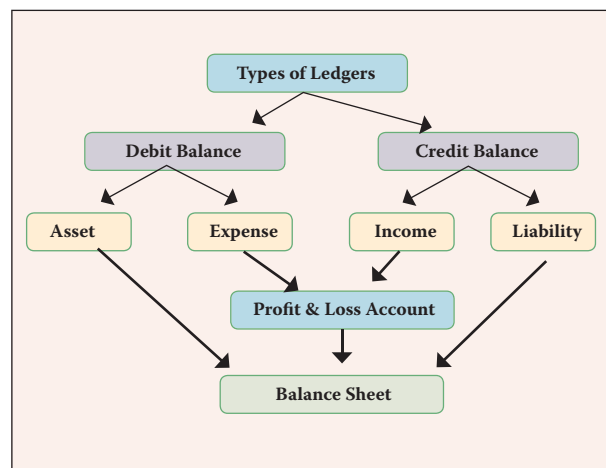
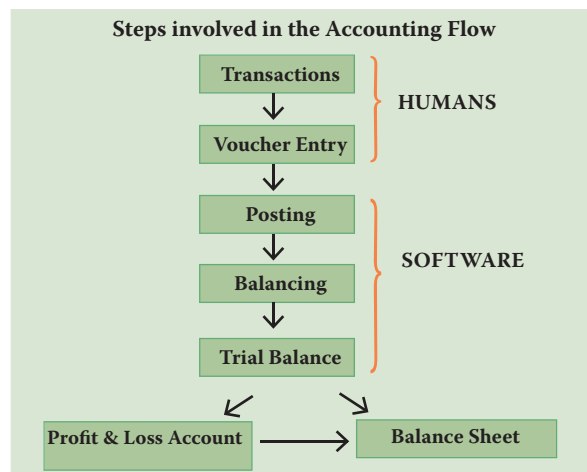
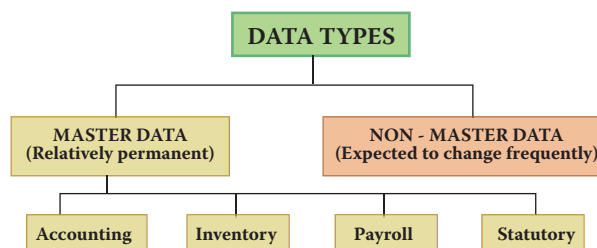
CHAPTER 2: FINANCIAL AND ACCOUNTING SYSTEMS

This chapter provides an in-depth knowledge about the concept of Financial and Accounting Systems, Integrated and Non-integrated Systems and further acquaint the students about Regulatory and Compliance requirements with Financial and Accounting systems.

In accounting language, a **Voucher** is a documentary evidence of a transaction. There may be different documentary evidences for different types of transactions.

Voucher Types			
1	Contra	Accounting	For recording of four types of transactions as under : <ul style="list-style-type: none">• Cash deposit in bank• Cash withdrawal from bank• Cash transfer from one location to another.• Fund transfer from our one bank account to our own another bank account.
2	Payment		For recording of all types of payments. Whenever the money is going out of business by any mode (cash/bank).
3	Receipt		For recording of all types of receipts. Whenever money is being received into business from outside by any mode (cash/bank)
4	Journal		For recording of all non-cash/bank transactions. E.g. Depreciation, Provision, Write-off, Write-back, discount given/ received, Purchase/Sale of fixed assets on credit, etc.
5	Sales		For recording all types of trading sales by any mode (cash/bank/credit).
6	Purchase		For recording all types of trading purchase by any mode (cash/bank/credit).
7	Credit Note		For making changes / corrections in already recorded sales / purchase transactions.
8	Debit Note		For making changes/corrections in already recorded sales/purchase transactions.
9	Memo-randum		For recording of transaction which will be in the system but will not affect the trial balance.
10	Purchase Order	Inventory	For recording of a purchase order raised on a vendor.
11	Sales Order		For recording of a sales order received from a customer.
12	Stock Journal		For recording of physical movement of stock from one location to another.
13	Physical Stock		For making corrections in stock after physical counting.
14	Delivery Note		For recording of physical delivery of goods sold to a customer.
15	Receipt Note		For recording of physical receipt of goods purchased from a vendor.
16	Attendance	Payroll	For recording of attendance of employees.
17	Payroll		For salary calculations.

From a business perspective, a **Process** is a coordinated and standardized flow of activities performed by people or machines, which can traverse functional or departmental boundaries to achieve a business objective and creates value for internal or external customers.



ENTERPRISE INFORMATION SYSTEMS ||

Installed Applications Vs. Web Applications		
Particulars	Installed Application	Web Application
Installation & Maintenance	As software is installed on hard disc of the computer used by user, it needs to be installed on every computer one by one. Maintenance & updating of s/w may take lot time and efforts.	As s/w is installed on only one computer. Hence, maintenance/updating of s/w becomes extremely easy.
Accessibility	As software is installed on the hard disc of the user's computer, user needs to go to the computer only. It cannot be used from any computer.	As software is not installed on the hard disc of user's computer and its used through browser and internet, it can be used from any computer in the world 24 x 7.
Mobile App.	Using the software through mobile application is difficult in this case.	Using mobile application becomes very easy as data is available 24 x 7.
Data Storage	Data is physically stored in the premises of the user, i.e. on the hard disc of the user's server computer. Thus user has full control over data.	Data is not stored in the user's server computer. It is stored on a web server. Hence user will not have any control over the data.
Data Security	As the data is in physical control of the user, user shall have the full physical control over the data and he/she can ensure that it is not accessed without proper access.	Data security is a big challenge in case of web application as the data is not in control of the user or owner of data. It is maintained on a web server.
Performance	A well written installed application shall always be faster than web application.	As data is picked from web server using internet, speed of operation may be slower.
Flexibility	Installed applications shall have more flexibility and controls as compared to web application.	Web applications do not even compare to the flexibility of desktop applications.

ENTERPRISE RESOURCE PLANNING (ERP)

An **ERP System** is based on a common database and a modular software design. The common database can allow every department of a business to store and retrieve information in real-time. The information should be reliable, accessible, and easily shared. An ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management.

Advantages of an ERP System

- Ability to customize an organization's requirements;
- Integrate business operations with accounting & financial reporting function;
- Increased data security and application controls;
- Build strong access and segregation of duties controls;
- Automate many manual processes thus eliminating errors;
- Process huge volumes of data within short time frames; and
- Strong reporting capabilities which aids management and other stakeholders in appropriate decision making.

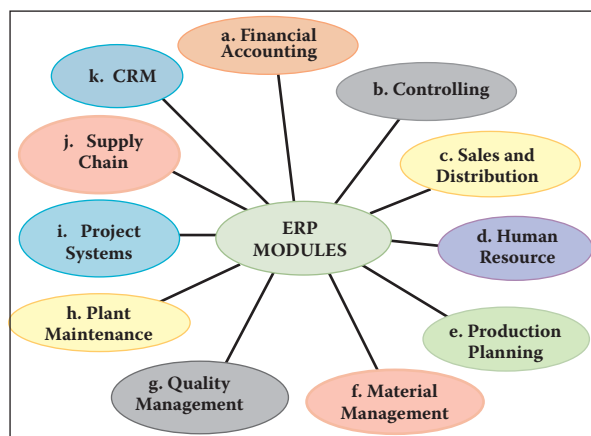
Features of an Ideal ERP System

- **Manufacturing:** Some of the functions include engineering, capacity, workflow management, quality control, bills of material, manufacturing process, etc.
- **Financials:** Accounts payable, accounts receivable, fixed assets, general ledger and cash management, etc.
- **Human Resources:** Benefits, training, payroll, time and attendance, etc.
- **Supply Chain Management:** Inventory, supply chain planning, supplier scheduling, claim processing, order entry, purchasing, etc.
- **Projects:** Costing, billing, activity management, time and expense, etc.
- **Customer Relationship Management (CRM):** CRM software is used to support processes, such as sales, marketing, customer service, training, professional development, performance management, HR Development, and compensation etc., storing information on current and prospective customers.
- **Data Warehouse:** Data warehouse is a repository of an organization's electronically stored data. These are designed to facilitate reporting and analysis. The process of transforming data into information and making it available to the user in a timely enough manner to make a difference is known as data warehousing.

Risks and Controls associated with ERP

Aspect	Risk Associated	Control Required
Data Access	Data is stored centrally and all the departments access central data. This creates a possibility of access to non-relevant data.	Access rights need to be defined very carefully. Access to be given on "Need to know" and "Need to do" basis only.
Data Safety	As there is only one set of data, if this data is lost, whole business may come to stand still.	Back up arrangement needs to be very strong. Also, strict physical control is needed for data.
Speed of Operation	As data is maintained centrally, gradually the data size becomes more and more and it may reduce the speed of operation.	This can be controlled by removing redundant data, using techniques like data warehousing and updating hardware on a continuous basis.
Change in process	As the overall system is integrated, a small change in process for one department may require lot of efforts and money.	All the processes must be documents carefully in beginning of implementation itself to avoid any discomfort in future.
Staff Turnover	As the overall system is integrated & connected with each other department, it becomes complicated and difficult to understand.	This can be controlled and minimized with help of proper staff training system, having help manuals, having backup plans for staff turnover, etc.
System Failure	As everybody is connected to a single system and central database, in case of failure of system, the whole business may come to stand still, may get affected badly.	This can be controlled and minimized by having proper and updated back up of data as well as alternate hardware / internet arrangements.

ENTERPRISE INFORMATION SYSTEMS



- a. Financial Accounting Module** { This module is the most important module of the overall ERP System and it connects all the modules to each other.
- b. Controlling Module** { This module facilitates coordinating, monitoring, and optimizing all the processes in an organization.
- c. Sales and Distribution Module** { This is used by organizations to support sales and distribution activities of products and services, starting from enquiry to order and then ending with delivery.
- d. Human Resource Module** { This module enhances the work process and data management within HR department of enterprises.
- e. Production Planning (PP) Module** { PP module is another important module that includes software designed specifically for production planning and management.
- f. Material Management (MM) Module** { MM module as the term suggests manages materials required, processed and produced in enterprises.
- g. Quality Management Module** { Quality Management module helps in management of quality in productions across processes in an organization
- h. Plant Maintenance Module** { This is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules.
- i. Project Systems** { Project systems are used for planning and managing projects.
- j. Supply Chain Module** { This module provides extensive functionality for logistics, manufacturing, planning, and analytics.
- k. Customer Relationship Management (CRM)** { Customer Relationship Management is a system which aims at improving the relationship with existing customers, finding new prospective customers, and winning back former customers.

Management Information Systems (MIS) Report

IT is a tool that managers use to evaluate business processes and operations.

Type of Information in an MIS Report

An MIS report for this would likely contain data such as:

- The number of calls your staff takes;
- The number of emails that come in each day;
- The average amount of time it takes to answer a phone call or email; and
- The number of questions that your staff answers correctly vs. the number that are incorrect.

The information must meet following criteria to become useful for the user:

Relevant	Timely	Accurate	Structured
MIS reports need to be specific to the business area they address. This is important because a report that includes unnecessary information might be ignored.	Managers need to know what's happening now or in the recent past to make decisions about the future.	It's critical that numbers add up and that dates and times are correct. Financial information is often required to be accurate to the dollar.	Try to break long passages of information into more readable blocks or chunks and give these chunks meaningful headings.

Data Analytics

Data Analytics is the process of examining data sets to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software.

Business Intelligence (BI)

BI encompasses a wide variety of tools, applications and methodologies that enable organizations to collect data from internal systems and external sources, prepare it for analysis, develop and run queries against the data, and create reports, dashboards and data visualizations to make the analytical results available to corporate decision makers as well as operational workers.

Business Reporting

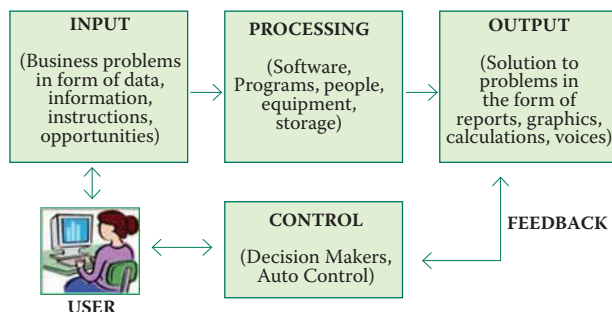
- It is the public reporting of operating and financial data by a business enterprise, or the regular provision of information to decision-makers within an organization to support them in their work.
- **XBRL (eXtensible Business Reporting Language)** is a freely available and global standard for exchanging business information. XBRL allows the expression of semantic meaning commonly required in business reporting.
- **Who uses XBRL?**
Regulators; Companies; Governments; Data Providers; Analysts and investors and Accountants.
- **Important features of XBRL**
 - ❖ Clear Definitions
 - ❖ Testable Business Rules
 - ❖ Multi-lingual Support
 - ❖ Strong Software Support

ENTERPRISE INFORMATION SYSTEMS ||

CHAPTER 3: INFORMATION SYSTEMS AND ITS COMPONENTS

This chapter provides a deep understanding about various components of an Information system and its working, types of threats and their mitigating controls and audit aspects of various components of Information Systems.

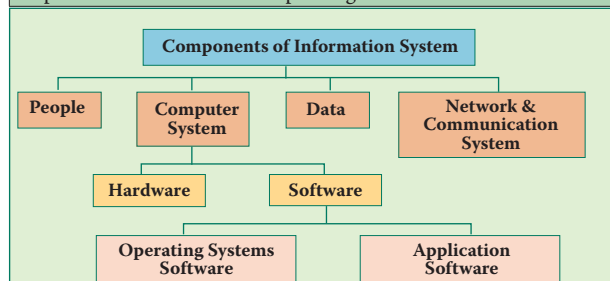
An **Information System** is a combination of people, hardware, software, communicating devices, network and data resources that processes can be storing, retrieving, transforming information) data and information for a specific purpose.



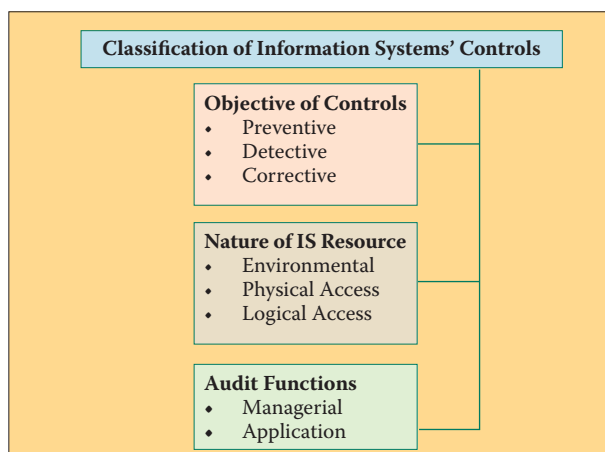
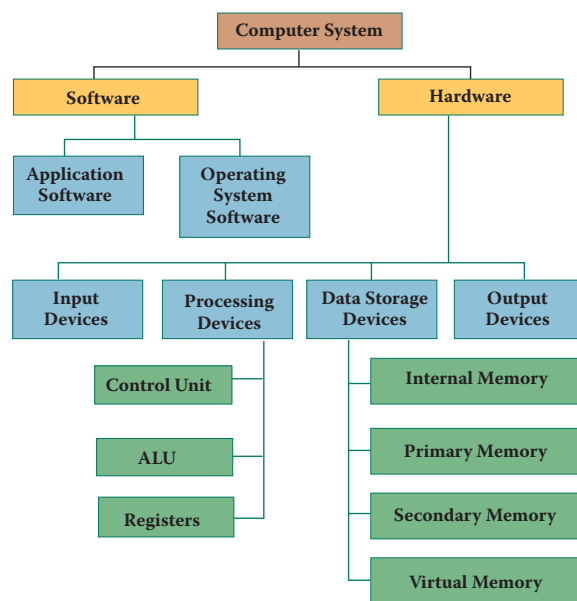
Data	Data are the raw bits and pieces of information with no context. Data can either be quantitative which is numeric (the result of a measurement, count, or some other mathematical calculation) or Qualitative data which is descriptive.
Networking and Communication Systems	These consist of both physical devices and software, links the various pieces of hardware and transfers the data from one physical location to another. Computers and communications equipment can be connected in networks for sharing voice, data, images, sound and video.

Functions of an Information System	
Input	Data is collected from an organization or from external environments and converted into suitable format required for processing.
Process	A process is a series of steps undertaken to achieve desired outcome or goal.
Output	Then information is stored for future use or communicated to user after application of respective procedure on it.

Three basic activities of an Information System that are defined above, helps enterprise in making decisions, control operations, analyze problems and create new products or services as an output. Apart from these activities, information systems also need feed-back that is returned to appropriate members of the enterprises to help them to evaluate at the input stage.



People	The people involved include users of the system and information systems personnel, including all the people who manage, run, program, and maintain the system.
Computer System	<p>Hardware: Information Systems hardware is the part of Information Systems that we can touch-the physical components of technology. Computers, keyboards, hard drives, iPads and flash drives are all examples of Information Systems hardware.</p> <p>Software: Software is a set of instructions that tells the hardware what to do. Software is not tangible it cannot be touched.</p> <ul style="list-style-type: none"> • An Operating System (OS) is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs. • Application software includes all that computer software that cause a computer to perform useful tasks beyond the running of the computer itself.

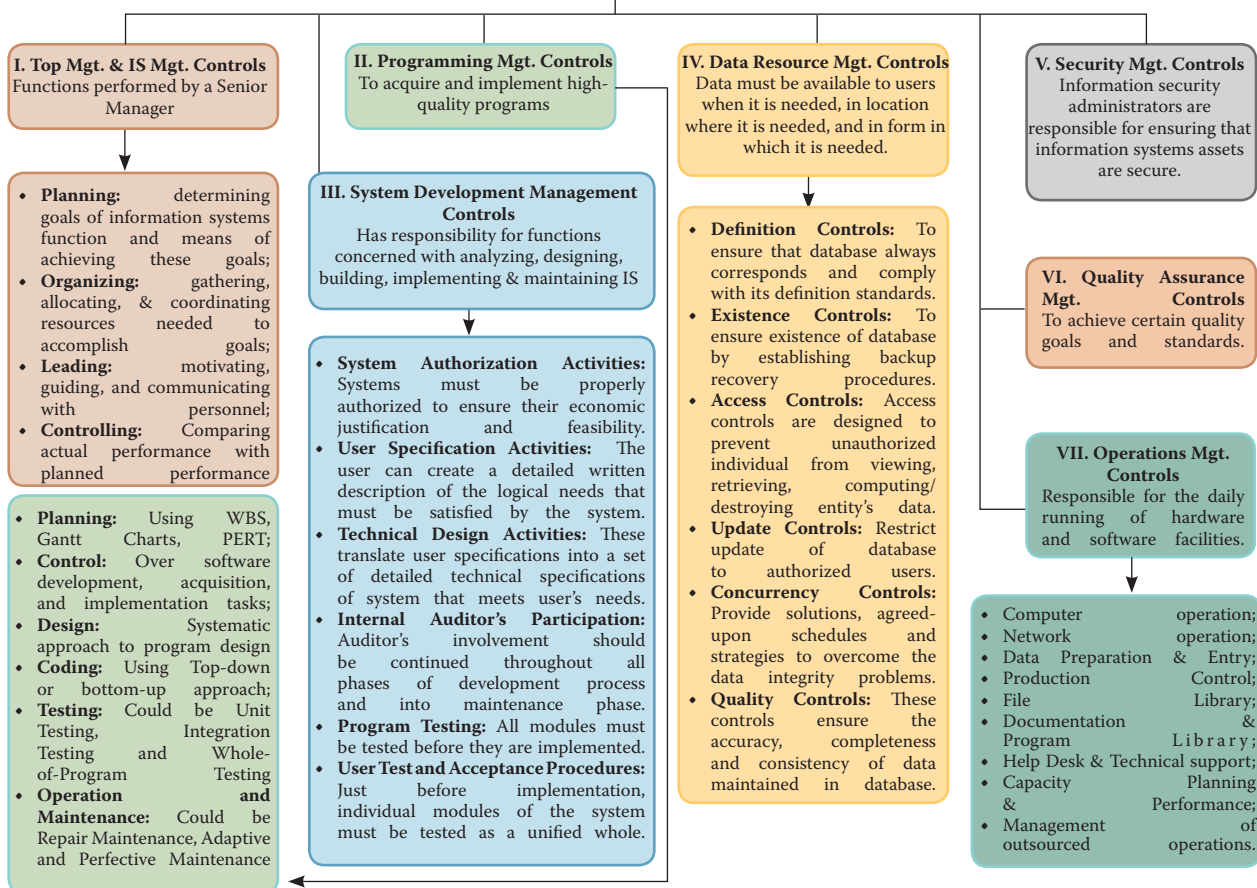


ENTERPRISE INFORMATION SYSTEMS

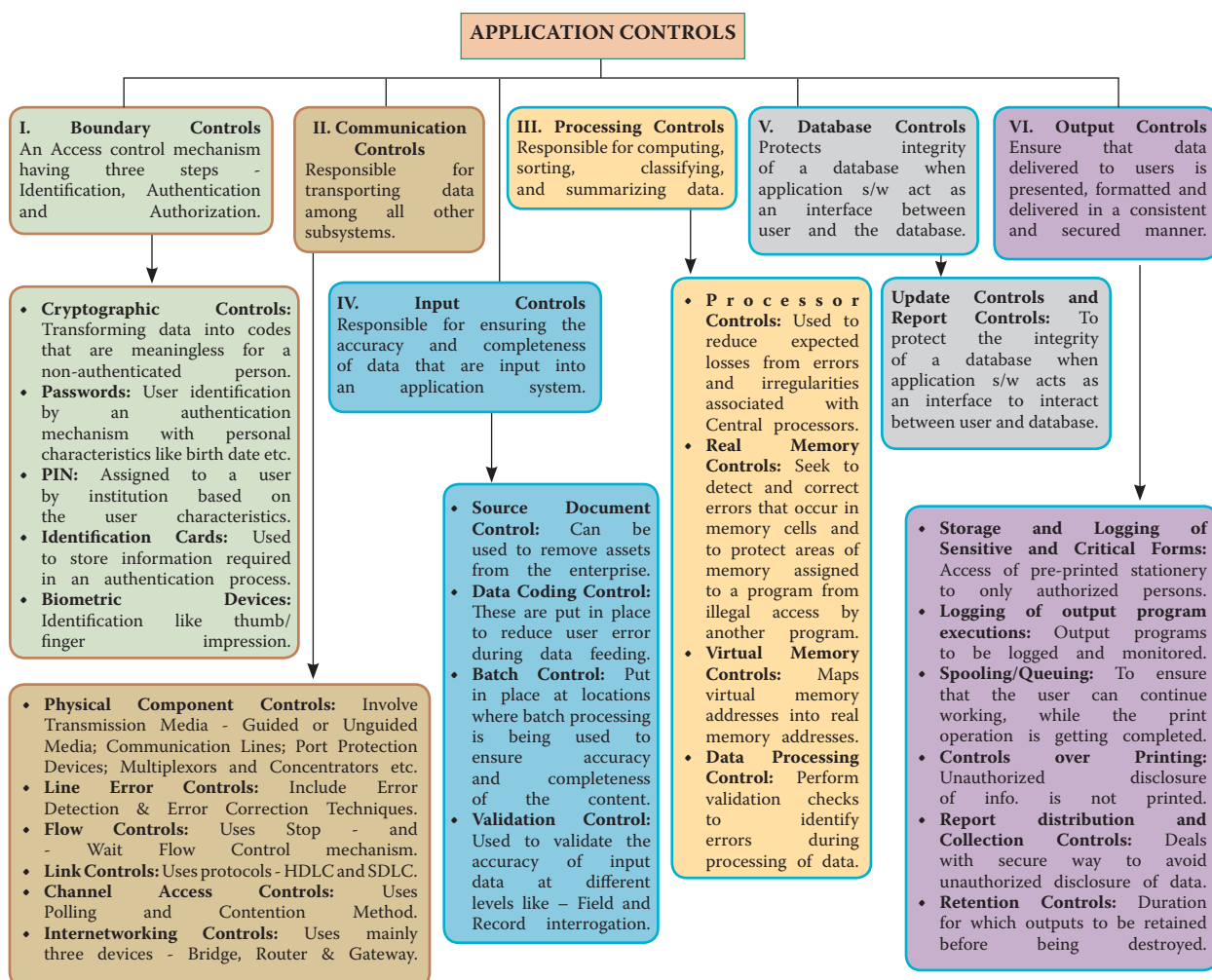
Objectives of Controls	
Preventive Controls	Prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered in numeric fields, access controls that protect sensitive data/ system resources from unauthorised people, and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.
Detective Controls	These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities.
Corrective Controls	These controls correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors, to identifying and removing unauthorised users or software from systems or networks, to recovery from incidents, disruptions, or disasters.
Nature of Information Systems' Resources	
Environmental Controls	These are the controls relating to IT environment such as power, air-conditioning, Un-interrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc.
Physical Access Controls	These are the controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. These include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc.

Logical Access Controls	These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.
Audit Functions	
Managerial Controls	The controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated and maintained on a day-to-day basis.
Application Controls	These include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements.

MANAGERIAL CONTROLS

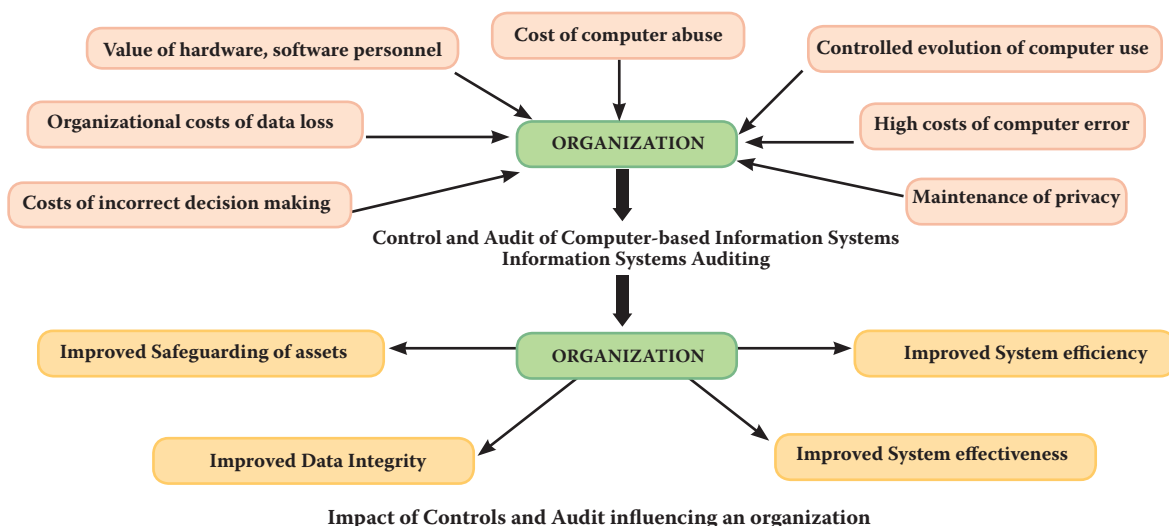


ENTERPRISE INFORMATION SYSTEMS ||



INFORMATION SYSTEM'S AUDITING

It is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both.



ENTERPRISE INFORMATION SYSTEMS

Need and Control of Information Systems' Audit

Organisational Costs of Data Loss	Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
Cost of Incorrect Decision Making	Management and operational controls taken by managers involve detection, investigations and correction of the processes.
Value of Computer Hardware, Software and Personnel	These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
Costs of Computer Abuse	Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets.
Controlled evolution of Computer Use	Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
High Costs of Computer Error	In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
Maintenance of Privacy	Data collected in a business process contains private information about an individual that needs to be maintained.

Information Systems' Audit Objectives

Asset Safeguarding Objectives	The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
Data Integrity Objectives	Data integrity important from the business perspective of the decision maker, competition and the market environment.
System Effectiveness Objectives	Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
System Efficiency Objectives	To optimize the use of various information system resources along with the impact on its computing environment.

TYPES OF AUDIT TOOLS

Snapshots

Tracing a transaction is a computerized system that can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

Integrated Test Facility (ITF)

The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system.

System Control Audit Review File (SCARF)

The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up.

Continuous and Intermittent Simulation (CIS)

This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system.

Audit Hooks

There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy.

AUDIT TRAILS

Audit Trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives.

- The **Accounting Audit Trail** shows the source and nature of data and processes that update the database.
- The **Operations Audit Trail** maintains a record of attempted or actual resource consumption within a system.

Managerial Controls and their Audit Trails

Managerial Controls	Scope	Audit Trails
Top Management and Information Systems Management Controls	Discusses the top management's role in planning, organizing, leading and controlling the information systems function. Also, provides advice to top management in relation to long-run policy.	<ul style="list-style-type: none"> • Planning: Auditors need to evaluate whether top management has formulated a high-quality IS's plan that is appropriate to the needs of an organization or not. • Organizing: Auditors should be concerned about how well top management acquires and manages staff resources. • Leading: Auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. • Controlling: Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.
System Development Management Controls	Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.	<ul style="list-style-type: none"> • Concurrent Audit: Auditors assist the team in improving the quality of systems development for the specific system they are building and implementing. • Post-implementation Audit: Auditors seek to help an organization learn from its experiences in the development of a specific application system. • General Audit: Auditors seek to determine whether they can reduce extent of substantive testing needed to form an audit opinion about management's assertions relating to financial statements for systems effectiveness and efficiency.
Programming Management Controls	Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.	<ul style="list-style-type: none"> • Planning: Auditors must evaluate how well the planning work is being undertaken. • Control: Auditors must evaluate whether the nature of and extent of control activities undertaken are appropriate for different types of s/w that are developed or acquired.

ENTERPRISE INFORMATION SYSTEMS ||

Managerial Controls	Scope	Audit Trails
		<ul style="list-style-type: none"> • Design: Auditors should find out whether programmers use some type of systematic approach to design. • Coding: Auditors should seek evidence to check whether programmers employ automated facilities to assist them with their coding work. • Testing: Auditor's primary concern is to see that unit testing; integration testing of the system testing has been undertaken appropriately. • Operation & Maintenance: Auditors need to ensure effectively & timely reporting of maintenance needs that occur & maintenance is carried out in a well-controlled manner.
Data Resource Management Controls	Discusses the role of database administrator and the controls that should be exercises in each phase.	Auditors should determine what controls are exercised to maintain data integrity. They might employ test data to evaluate whether access controls and update controls are working.
Quality Assurance Management Controls	Discusses major functions that quality assurance management should perform to ensure that development, implementation, operation, and maintenance of information systems conform to quality standards.	Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
Security Management Controls	Discusses major functions performed by operations by security administrators to identify major threats to IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.	Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not.
Operations Management Controls	Discusses the major functions performed by management to ensure the day-to-day operations of the IS function are well controlled.	Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

Application Controls And Their Audit Trails

Application Controls	Accounting Audit Trail	Operations Audit Trail
BOUNDARY CONTROLS This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. This includes Identity of the would-be user of the system; Authentication information supplied; Resources requested; Action privileges requested; Terminal Identifier; Start and Finish Time; Number of Sign-on attempts; and Resources provided/denied.	Action privileges allowed/denied.	<ul style="list-style-type: none"> • Resource usage from log-on to log-out time. • Log of Resource consumption.

Application Controls	Accounting Audit Trail	Operations Audit Trail
INPUT CONTROLS This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.	<ul style="list-style-type: none"> • The identity of the person (organisation) who was the source of the data; • The identity of the person (organisation) who entered the data into the system; • The time and date when the data was captured; • The identifier of the physical device used to enter the data into the system; • The account or record to be updated by the transaction; • The standing data to be updated by the transaction; • The details of the transaction; and • The number of the physical or logical batch to which the transaction belongs. 	<ul style="list-style-type: none"> • Time to key in a source document or an instrument at a terminal; • Number of read errors made by an optical scanning device; • Number of keying errors identified during verification; • Frequency with which an instruction in a command language is used; and • Time taken to invoke an instruction using a light pen versus a mouse.
COMMUNICATION CONTROLS This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.	<ul style="list-style-type: none"> • Unique identifier of the source/sink node; • Unique identifier of each node in the network that traverses the message; • Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched; • Time and date at which the message was received by the sink node; • Time and date at which node in the network was traversed by the message; and • Message sequence number; and the image of the message received at each node traversed in the network. 	<ul style="list-style-type: none"> • Number of messages that have traversed each link and each node; • Queue lengths at each node; • Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors; • Log of system restarts; and • Message transit times between nodes and at nodes.
PROCESSING CONTROLS The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.	<ul style="list-style-type: none"> • To trace and replicate the processing performed on a data item. • To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values. • To check for existence of any data flow diagrams or flowcharts that describe data flow in the transaction, and whether such diagrams or flowcharts correctly identify the flow of data. • To check whether audit log entries recorded the changes made in the data items at any time including who made them. 	<ul style="list-style-type: none"> • A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used. • A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

|| ENTERPRISE INFORMATION SYSTEMS

Application Controls	Accounting Audit Trail	Operations Audit Trail
DATABASE CONTROLS The audit trail maintains the chronology of events that occur either to the database definition or the database itself.	<ul style="list-style-type: none"> To confirm whether an application properly accepts, processes, and stores information. To attach a unique time stamp to all transactions. To attach before-images and after-images of the data item on which a transaction is applied to the audit trail. Any Modifications or corrections to audit trail transactions accommodating the changes that occur within an application system. To not only test the stated input, calculation, and output rules for data integrity, but also should assess the efficacy of the rules themselves. 	<ul style="list-style-type: none"> To maintain a chronology of resource consumption events that affects the database definition or the database.

Application Controls	Accounting Audit Trail	Operations Audit Trail
OUTPUT CONTROLS The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.	<ul style="list-style-type: none"> What output was presented to users; Who received the output; When the output was received; and What actions were taken with the output? 	<ul style="list-style-type: none"> To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

Segregation of Duties (SoD) ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data. Segregation of Duties (SoD) Controls are Preventive and Detective controls that should be put into place to manage segregation of duties matters. Some examples of SoD Controls are Transaction Authorization, Split custody of high-value assets, workflow and periodic reviews.

CHAPTER 4: E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

This chapter provides an insight about meaning, components and architecture of E-Commerce, various risks and controls associated with e-commerce and applicable laws and guidance governing e-commerce. The chapter further deals with the emerging technologies like Cloud Computing, Mobile Computing, Green Computing etc. and their perspectives.

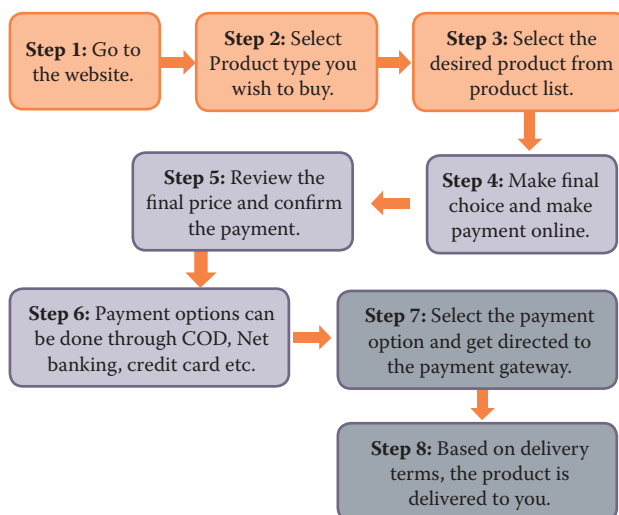
TRADITIONAL COMMERCE Vs. E-COMMERCE

Base For Comparison	Traditional Commerce	E-Commerce
Definition	Includes all those activities which encourage exchange, in some way or the other of goods / services which are manual and non-electronic.	Means carrying out commercial transactions or exchange of information, electronically on the internet.
Transaction Processing	Manual	Electronically
Availability for commercial transactions	For limited time. This time may be defined by law. Like special stores which may run 24 hours, but in general available for limited time.	24 × 7 × 365
Nature of purchase	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
Customer interaction	Face-to-face.	Screen-to-face.
Business Scope	Limited to particular area.	Worldwide reach
Information exchange	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
Resource focus	Supply side	Demand side

Base For Comparison	Traditional Commerce	E-Commerce
Marketing	One way marketing	One-to-one marketing
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer, Cash in Delivery, Payment Wallets, UPCI application etc.
Delivery of goods	Instantly	Takes time, but now e-commerce websites have created options of same day delivery, or delivery within 4 hours.
Layers of Delivery (Profit Impact)	Reduced layers of delivery from manufacturer to customers.	(i) Increases profit margin of manufacturers. (ii) Above (i) allow manufacturers to give discounts to customers. (iii) Customers get better prices.
Layers of Delivery (Time Impact)	Reduced layers of delivery from manufacturer to customers.	(i) This helps customers get faster product deliveries. (ii) Manufacturers can have better inventory management. As they will always know what products customers are buying. They shall be able to maintain inventory on JIT (Just in Time) basis.

ENTERPRISE INFORMATION SYSTEMS ||

Illustration of E-Commerce Transaction



Benefits of E-Commerce

Benefits to Customer / Individual / User

- Convenience
- Various Options
- Coupon and Deals
- Time saving
- Easy to find reviews
- Anytime Access

Benefits to Business / Sellers

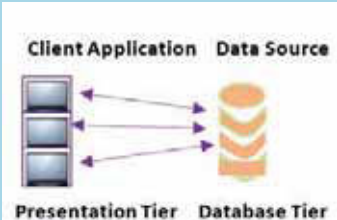

- Increased Customer Base
- Instant Transaction
- Reduction in costs
- Creation of new markets
- Better quality of goods
- Recurring payments made easy
- Provides a dynamic market
- Efficiency improvement
- Easier entry into new markets
- Elimination of Time Delays

Benefits to Government

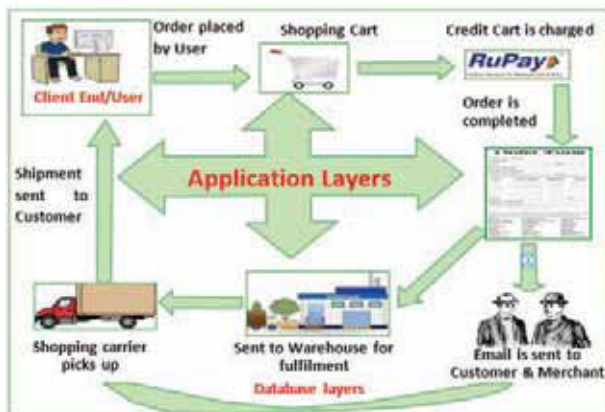
- Instrument to fight corruption
- Reduction in use of ecologically damaging materials

ARCHITECTURE OF NETWORKED SYSTEMS

Architecture is a term to define the style of design and method of construction used in generally for buildings and other physical structures. In e-commerce, it denotes the way network architectures are built.

Advantages	Two-Tier Architecture	Disadvantages
<ul style="list-style-type: none"> • The system performance is higher because business logic and database are physically close. • More users could interact with system. • It is easy to setup and maintain entire system smoothly. 	 <ul style="list-style-type: none"> • Presentation Tier (Client Application/Client Tier): This is the interface that allows user to interact with the e-commerce / m-commerce vendor. • Database Tier (Data Tier): The product data / price data / customer data and other related data are kept here. 	<ul style="list-style-type: none"> • Performance deteriorates if number of users increases. • There is restricted flexibility and choice of DBMS since data language used in the server is proprietary to each vendor.
Advantages	Three Tier Architecture	Disadvantages
<ul style="list-style-type: none"> • Clear separation of user-interface-control and data presentation from application-logic. • Dynamic load balancing possible if bottlenecks in terms of performance occurs. • Change management is easy and faster. 	 <ul style="list-style-type: none"> • Presentation Tier: Occupies the top level and displays information related to services available on a website. • Application Tier: Also, called the Middle Tier, Logic Tier, Business Logic or Logic Tier; it controls application functionality by performing detailed processing. • Database Tier: This tier houses the database servers where information is stored and retrieved. 	<ul style="list-style-type: none"> • Increased need for network traffic management, server load balancing, and fault tolerance. • Current tools relatively immature and more complex. • Maintenance tools currently inadequate.

E-Commerce Architecture Vide Internet



- **Client / User Interface:** This layer e-commerce connects to help the customer and e-commerce merchant.
- **Application Layer:** Through these application's customer logs to merchant systems. This layer allows customer to check the products available on merchant's website.
- **Database Layer:** This layer is accessible to user through application layer.

Risks and Controls

Risk is possibility of loss. The same may be result of intentional or un-intentional action by individuals. Risks associated with e-commerce transactions are high compared to general internet activities. These include the following:

Infrastructure	Quality issues	Delay in goods and Hidden Costs
Repudiation of contract	Security and credit card issues	Problem of anonymity
Lack of authenticity of transactions	Needs Access to internet and lack of personal touch	Data Loss or theft or duplication
Attack from hackers	Denial of Service	Non-recognition of electronic transactions
Lack of audit trails	Problem of piracy	Privacy and Security

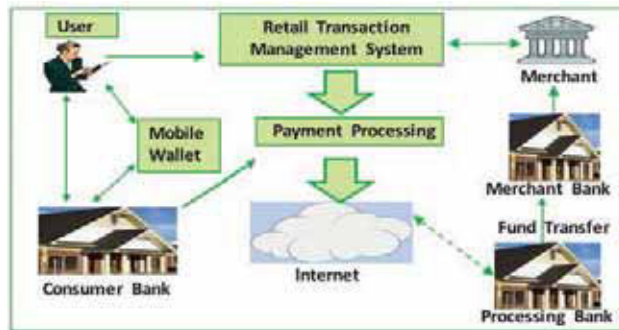
Digital Payment

Digital Payment is a way of payment which is made through digital modes. In digital payments, payer and payee both use digital modes to send and receive money. It is also called electronic payment. No hard cash is involved in the digital payments.

Advantages of Digital Payments	Drawbacks of Digital Payments
<ul style="list-style-type: none"> • Easy and convenient • Pay or send money from anywhere • Discounts from taxes • Written record • Less Risk 	<ul style="list-style-type: none"> • Difficult for a Non-technical person • Risk of data theft • Overspending

E-Commerce Architecture Vide Mobile Apps

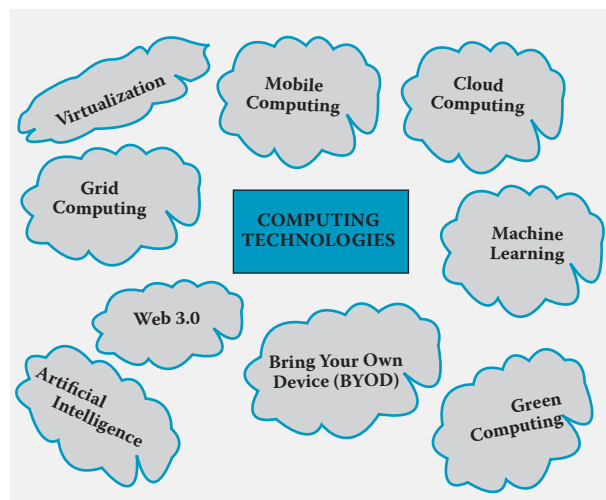
M-Commerce (Mobile Commerce): M-commerce is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). M-commerce enables users to access the Internet without needing to find a place to plug in.



Digital Payment (contd..)

All the transactions in digital payments are completed online. It is an instant and convenient way to make payment; resulting in absolute transparency and involvement of minimal processes.

New Methods of Digital Payment	Traditional Methods of Digital Payment
<ul style="list-style-type: none"> • Unified Payment Interface (UPI) Apps • Immediate Payment Service (IMPS) • Mobile Apps - BHIM (Bharat Interface for Money) • Mobile Wallets • Aadhar Enabled Payment Service (AEPS) • Un-structure Supplementary Service Data (USSD) 	<ul style="list-style-type: none"> • E-Wallet • Cards - Credit Cards, Debits Cards • Net Banking



ENTERPRISE INFORMATION SYSTEMS ||

I. Virtualization		
Virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. This refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them.		Application Areas <ul style="list-style-type: none"> • Server Consolidation • Disaster Recovery • Testing and Training • Portable Applications • Portable Workspaces
Types of Virtualization		
Hardware Virtualization	Network Virtualization	Storage Virtualization
This refers to the creation of a virtual machine that acts like a real computer with an operating system. The basic idea of Hardware virtualization is to consolidate many small physical servers into one large physical server so that the processor can be used more effectively. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Linux operating system; based software that can be run on the virtual machine.	It is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. It is intended to optimize network speed, reliability, flexibility, scalability, and security.	It is the apparent pooling of data from multiple storage devices, even different types of storage devices, into what appears to be a single device that is managed from a central console. It helps the storage administrator perform the tasks of backup, archiving, and recovery more easily and in less time by disguising the actual complexity of a Storage Area Network (SAN).
II. Grid Computing: It is a computer network in which each computer's resources are shared with every other computer in the system. It is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks.		
Benefits	Types of Resources	Security
<ul style="list-style-type: none"> ❖ Making use of Underutilized Resources. ❖ Resource Balancing. ❖ Parallel CPU Capacity. ❖ Access to additional resources. ❖ Virtual resources and virtual organizations for collaboration. ❖ Reliability. ❖ Management. 	<ul style="list-style-type: none"> ❖ Computation. ❖ Storage. ❖ Communications. ❖ Software and Licenses. ❖ Special equipment, capacities, architectures, and policies. 	<ul style="list-style-type: none"> ❖ Single Sign-on. ❖ Protection of Credentials. ❖ Interoperability with local security solutions. ❖ Exportability ❖ Support for secure group communication. ❖ Support for multiple implementations.
III. Cloud Computing: Cloud Computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT enabled services enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser, and thus enabling users to access the resources from any client device including notebooks, desktops and mobile devices.		
Characteristics <ul style="list-style-type: none"> ❖ Elasticity & Scalability ❖ Pay-Per-Use ❖ On-demand ❖ Resiliency ❖ Multi-Tenancy ❖ Workload Movement 	Advantages <ul style="list-style-type: none"> ❖ Achieve economies of scale ❖ Reduce spending on technology infrastructure ❖ Globalize the workforce ❖ Streamline business processes ❖ Reduce capital costs ❖ Pervasive accessibility ❖ Monitor projects more effectively ❖ Less personnel training is needed ❖ Minimize maintenance & licensing software ❖ Improved flexibility 	

|| ENTERPRISE INFORMATION SYSTEMS

Types of Cloud			
Private Cloud	Public Cloud	Community Cloud	Hybrid Cloud
It resides within the boundaries of an organization and is used exclusively for the organization's benefits. Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).	It is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.	It is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises.	This is a combination of both, at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used.
Characteristics of Cloud Computing			
<ul style="list-style-type: none">❖ Secure❖ Central Control❖ Weak Service Level Agreements (SLAs)	<ul style="list-style-type: none">❖ Highly Scalable❖ Affordable❖ Less Secure❖ Highly available❖ Stringent SLAs	<ul style="list-style-type: none">❖ Collaborative & Distributive maintenance❖ Partially secure❖ Cost effective	<ul style="list-style-type: none">❖ Scalable❖ Partially Secure❖ Stringent SLAs❖ Complex Cloud Management
Cloud Computing Service Models			
Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	
IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand.	PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider.	SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.	
This allows users to maximize the utilization of computing capacities without having to own and manage their own resources.	PaaS changes the application development from local machine to online.	SaaS is delivered as an on-demand service over the Internet, there is no need to install the software to the end-user's devices.	
Different instances are - Network as a Service (NaaS), Storage as a Service (STaaS), Database as a Service (DBaaS), Backend as a Service (BaaS), and Desktop as a Service (DTaaS).	PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.	Different instances of SaaS include Testing as a Service (TaaS), API as a Service (APIaaS), Email as a Service (EaaS), Communication as a Service (CaaS), Data as a Service (DaaS), Security as a Service (SECaaS), and Identity as a Service (IDaaS).	
IV. Mobile Computing: This refers to technology that allows transmission of data via a computer without having to be connected to a fixed physical link.			
Components	Limitations	Benefits	
<ul style="list-style-type: none">❖ Mobile Communication: Refers to infrastructure put in place to ensure that seamless and reliable communication goes on.❖ Mobile Hardware: This includes mobile devices/device components that range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA).❖ Mobile Software: It is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications.	<ul style="list-style-type: none">❖ Insufficient Bandwidth❖ Security Standards❖ Power consumption❖ Transmission interferences❖ Potential health hazards❖ Human interface with device.	<ul style="list-style-type: none">❖ Mobile workforce with remote access to work order details.❖ Enables mobile sales personnel to update work order status in real-time.❖ Facilitates access to corporate services and information at any time.❖ Provides remote access to the corporate knowledge base at job location.❖ Enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.	

ENTERPRISE INFORMATION SYSTEMS ||

IV. Green Computing: **Green Computing** or **Green IT** refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way.

Best Practices

- ❖ Develop a sustainable Green Computing plan
- ❖ Recycle
- ❖ Make environmentally sound purchase decisions
- ❖ Reduce Paper Consumption
- ❖ Conserve Energy

V. BYOD (Bring Your Own Device): This refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application.

Advantages

- ❖ Happy Employees
- ❖ Lower IT budgets
- ❖ IT reduces support requirement
- ❖ Early adoption of new Technologies
- ❖ Increased employee efficiency

Emerging BYOD Threats

- ❖ **Network Risks:** It is normally exemplified and hidden in '**Lack of Device Visibility**'. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous.
- ❖ **Device Risks:** It is normally exemplified and hidden in '**Loss of Devices**'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- ❖ **Application Risks:** It is normally exemplified and hidden in '**Application Viruses and Malware**'. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user.'
- ❖ **Implementation Risks:** It is normally exemplified and hidden in '**Weak BYOD Policy**'. The effective implementation of the BYOD program should not only cover technical issues mentioned above but also mandate the development of a robust implementation policy.

VI. Web 3.0 Technology

- ❖ Known as the **Semantic Web**, this describes sites wherein the computers will generate raw data on their own without direct user interaction.
- ❖ Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behaviour, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users.
- ❖ Web 3.0 Technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

Web 3.0 Components

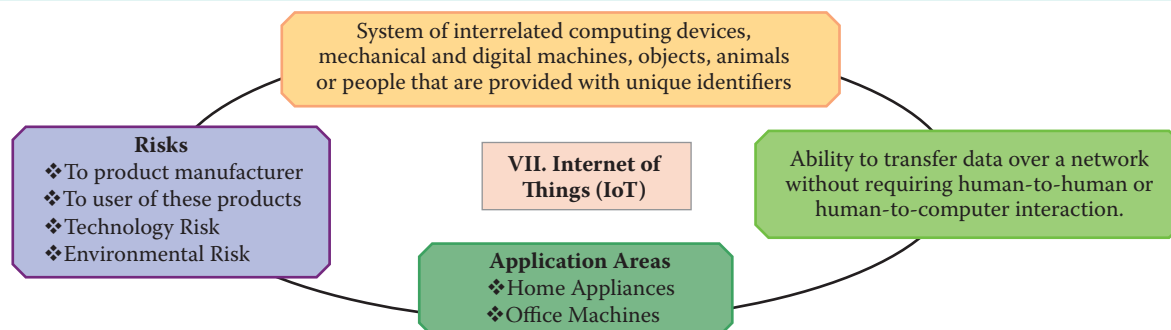
Semantic Web

This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries.

Web Services

It is a software system that supports computer - to - computer interaction over the Internet. For example – photo sharing website.

Example: The application that uses content management systems along with artificial intelligence. This helps to achieve a more connected open and intelligent web applications using concepts of natural language processing machine learning, machine reasoning and autonomous agents.



VIII. Artificial Intelligence may be defined as the ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgement to solve problems and adapt to new situations. Applications Areas include Medical diagnosis; in cancer research; Predicting the chances of an individual getting ill by a disease; Creating art such as poetry; Proving mathematical theorems; Playing games (such as Chess or Go) and predicting the outcomes etc.

IX. Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data. The process of machine learning is similar to that of data mining. For example: Machine learning has been used for image, video, and text recognition, as well as serving as the power behind recommendation engines.

CHAPTER 5: CORE BANKING SYSTEMS

This chapter deals with components and architecture of Core Banking Systems (CBS) and impact of related risks and controls, discusses the functioning of core module of banking and business process flow. The chapter also provides a detailed understanding on the regulatory and compliance requirements applicable to CBS such as Banking Regulations Act, RBI regulations, Prevention of Money Laundering Act and Information Technology Act.

Banking is the engine of economic growth specifically in a rapidly developing country like India with its diverse background, practices, cultures and large geographic dispersion of citizens. The core of banking functions is acceptance of deposits and lending of money. Further, specific services such as demand drafts, bank guarantees, letter of credits, etc. are also provided. The key features of a banking business are as follows:

- The custody of large volumes of monetary items, including cash and negotiable instruments, whose physical security should be ensured.
- Dealing in large volume (in number, value and variety) of transactions.
- Operating through a wide network of branches and departments, which are geographically dispersed.
- Increased possibility of frauds as banks directly deal with money making it mandatory for banks to provide multi-point authentication checks and the highest level of information security.

PRODUCTS & SERVICES RENDERED BY COMMERCIAL BANKS

I. Acceptance of Deposits

Commercial banks accept deposits in various forms such as term deposits, savings bank deposits, current account deposits, recurring deposit, saving-cum-term deposit and various others innovative products.

II. Granting of Advances

Advances constitute a major source of lending by commercial banks. The type of advances granted by commercial banks take various forms such as cash credit, overdrafts, purchase/discounting of bills, term loans, etc.

III. Remittances

Involves transfer of funds from one place to another. Two of most common modes of remittance of funds are demand drafts & Telegraphic/ Mail Transfers (TT/ MT).

IV. Collections

Collections involve collecting proceeds on behalf of the customer. Customers can lodge various instruments such as cheques, drafts, pay orders, travelers' cheques, dividend and interest warrants, tax refund orders, etc.

V. Clearing

This involves collecting instruments on behalf of customers of bank.

VI. Letters of Credit (LC)

It is an undertaking by a bank to the payee to pay to him, on behalf of the applicant any amount up to the limit specified in the LC, provided the terms and conditions mentioned in the LC are complied with.

VII. Guarantees

These are required by the customers of banks for submission to the buyers of their goods/services to guarantee performance of contractual obligations undertaken by them or satisfactory performance of goods supplied by them, or for submission to certain departments like excise and customs, electricity boards, or to suppliers of goods, etc. in lieu of the stipulated security deposit.

VIII. Credit Cards

Most credit cards issued by banks are linked to one of the international credit card networks like VISA, Master etc.

IX. Debit Cards

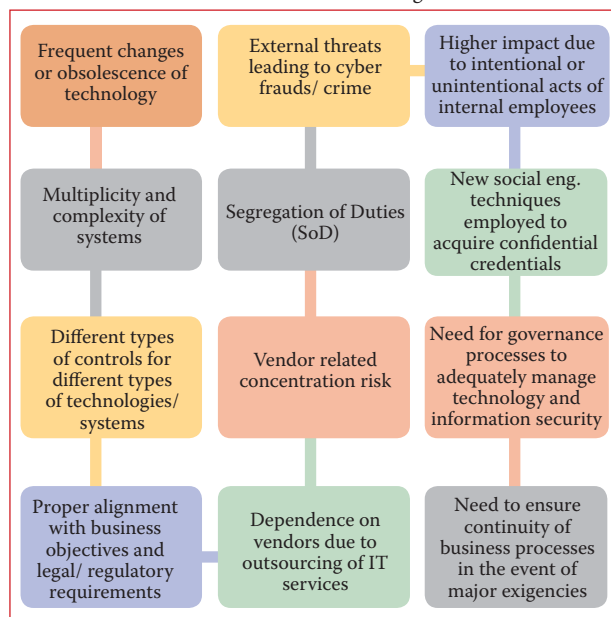
Debit Cards facilitates customers to pay at any authorized outlet as well as to withdraw money from an ATM from their account.

X. Other Banking Services

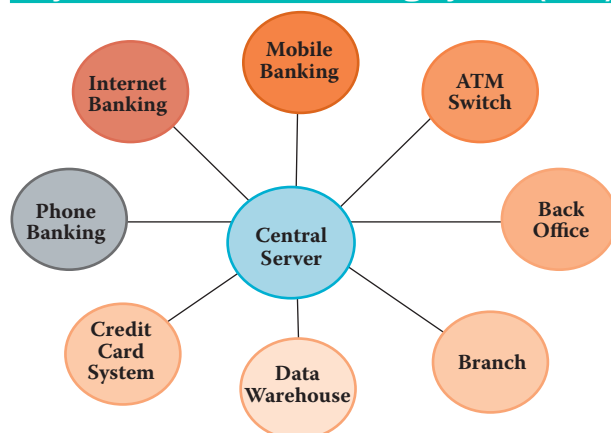
These include Back operations, Retail Banking, High Net-worth Individuals (HNI), Risk Management and Specialized Services such as insurance broking, claims, underwriting, life insurance, non-life insurance, etc.

ENTERPRISE INFORMATION SYSTEMS ||

The business processes and standards adapted by Banks should consider these new set of IT risks and challenges:



Key Modules of Core Banking System (CBS)



RISKS AND CONTROLS

- **Risk** can be defined as “the potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset.”
- **Risk Analysis** is defined as the process of identifying security risks and determining their magnitude and impact on an organization.

IT Risk Management is as follows:

- **Avoid:** Eliminate the risk by not taking up or avoiding the specific business process which involves risk.
- **Mitigate:** Implement controls (e.g. acquire and deploy security technology to protect the IT infrastructure).
- **Transfer:** Share risk with partners or transfer to insurance coverage.
- **Accept:** Formally acknowledge that the risk exists and monitor it.

Control refers to the policies, procedures, practices and organization structures that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented, detected or corrected.

General Controls: Also, known as Infrastructure Controls, these are pervasive controls and apply to all systems components, processes, and data for a given enterprise or systems environment.

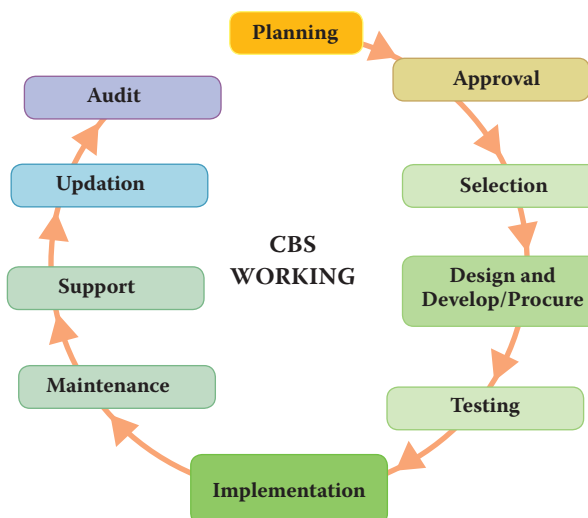
Application Controls: These are implemented in an application to prevent or detect and correct errors. Application controls ensure that all transactions are authorized, complete and accurate.

General Controls include, but are not limited to:

- Information Security Policy
- Administration, Access, and Authentication;
- Separation of key IT functions;
- Management of Systems Acquisition and Implementation;
- Change Management;
- Backup, Recovery & Business Continuity;
- Proper Development and Implementation of Application S/w;
- Confidentiality, Integrity & Availability of Software & data files; and
- Incident response and management.

Some examples of Application controls are as follows:

- Data edits (editing of data is allowed only for permissible fields);
- Separation of business functions (e.g., transaction initiation versus authorization);
- Balancing of processing totals (debit and credit of all transactions are tallied);
- Transaction logging (all transactions are identified with unique id and logged);
- Error reporting (errors in processing are reported); and
- Exception Reporting (all exceptions are reported).



|| ENTERPRISE INFORMATION SYSTEMS

Planning

Implementation of CBS should be done as per strategic and business objectives of bank.

Approval

The decision to implement CBS must be approved by the Board of Directors as high investment and recurring costs are involved.

Selection

Bank should select the right solution considering various parameters as defined by the bank to meet their specific requirements and business objectives.

Design/Develop or Procured

Currently, most of the CBS deployment are procured. There should be appropriate controls covering the design or development or procurement of CBS for the bank.

Testing

The testing is to be done at different phases at procurement stage to test suitability to data migration to ensure all existing data is correctly migrated and testing to confirm processing of various types of transactions of all modules produces the correct results.

Implementation

CBS must be implemented as per pre-defined and agreed plan with specific project milestones to ensure successful implementation.

Maintenance

CBS must be maintained as required. E.g. program bugs fixed, version changes implemented, etc.

Support

CBS must be supported to ensure that it is working effectively.

Updation

CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements.

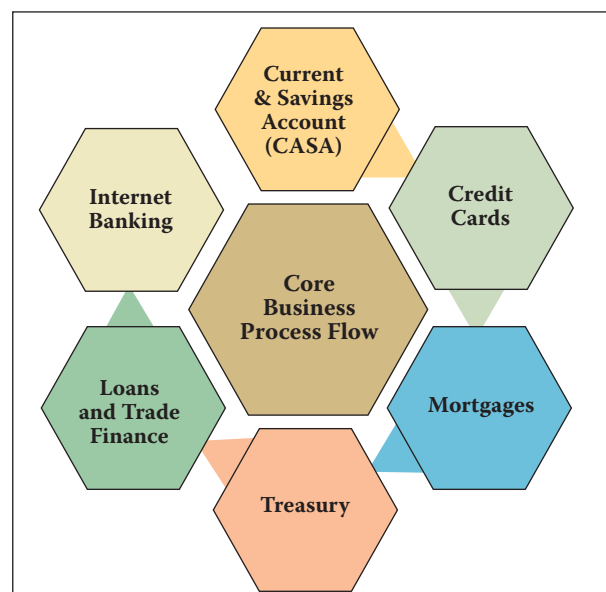
Audit

Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

CBS IT ENVIRONMENT

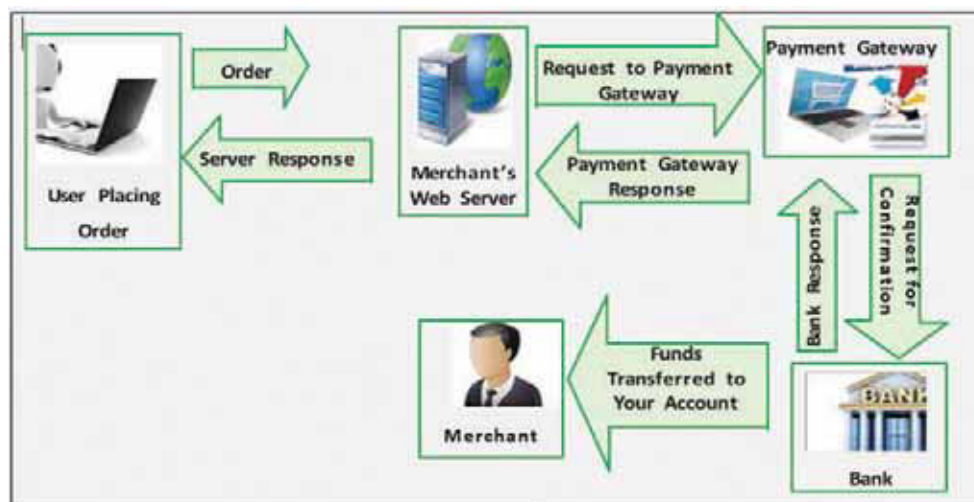
The CBS facilities providing banking services for branches of a bank which are networked and connected to common data center. This facilitates staff to process transactions of customers of any branch. The Server is a sophisticated computer that accepts service requests from different machines called clients. The requests are processed by the server and sent back to the clients. There are different types of servers used in deploying CBS which are as follows:

CBS SERVERS	FUNCTIONING
Application Server	The application software, resides in the application server and is always the latest version as accepted after adequate testing.
Database Server	The Database Server of Bank contains entire data of Bank which would consist of various accounts of customers & master data.
ATM Channel Server	This server contains the details of ATM account holders. Soon after the facility of using the ATM is created by the Bank, the details of such customers are loaded on to the ATM server.
Internet Banking Channel Server (IBCS)	IBCS software stores the name and password of the entire internet banking customers. IBCS server also contains the details about the branch to which the customer belongs.
Internet Banking Application Server (IBAS)	The Internet Banking Software which is stored in IBAS authenticates customer with the login details stored in IBCS.
Web Server	The Web Server is used to host all web services and internet related software. Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.
Proxy Server	A Proxy Server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services.
Anti-Virus Software Server	The Anti-Virus Server is used to host anti-virus s/w which is deployed for ensuring all the s/w deployed are first scanned to ensure that appropriate virus/ malware scans are performed.



ENTERPRISE INFORMATION SYSTEMS ||

e-Commerce Transaction flow for approval of payments



RISKS ASSOCIATED WITH CBS

Ownership of Data/ Process

Data resides at the Data Centre. Establish clear ownership.

Authorization Process

Anybody with access to the CBS, including the customer himself, can enter data directly. What is the authorization process?

Authentication Procedures

These may be inadequate and hence the user entering the transaction may not be determinable or traceable.

Several software interfaces across diverse networks

A Data Centre can have as many as 75-100 different interface and application software.

Maintaining Response Time

Maintaining the interfacing software and ensuring optimum response time and up time can be challenging

User Identity Management

This could be a serious issue. Some Banks may have more than 5000 users interacting with the CBS at once.

Access Controls

Designing and monitoring access control is an extremely challenging task.

Incident handling procedures

These may not be adequate considering the need for real-time risk management.

Change Management

At application level and data level – Master files, Transaction files and Reporting software.

IT Related Risks

From a business perspective, the risks that can be classified based on following Information criteria are as follows:

Efficiency

Response is delayed resulting in dissatisfied stakeholder.

Effectiveness

Process is ineffective and multiple runs consume time.

Reliability

Users lose confidence in information system.

Confidentiality

Due to loss of critical data.

Integrity

Incomplete or inaccurate data due to errors in input or processing.

Availability

Information system is not available when required.

Compliance

The information system does not comply with legal, regulatory, contractual or internal compliance requirements.

Applicable Regulatory and Compliance Requirements

Negotiable Instruments Act-1881 (NI Act) Under NI Act, Cheque includes electronic image of truncated cheque and a cheque in the electronic form. The truncation of cheques in clearing has been given effect to and appropriate safeguards in this regard have been set forth in the guidelines issued by RBI from time to time.

|| ENTERPRISE INFORMATION SYSTEMS

I. The Reserve Bank of India (RBI) was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. The basic functions of the Reserve Bank as: “to regulate the issue of Bank Notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its advantage.”

II. Money Laundering is the process by which the proceeds of the crime and the true ownership of those proceeds are concealed or made opaque so that the proceeds appear to come from a legitimate source.

- **Prevention of Money Laundering Act (PMLA)**

- **Three stages of Money Laundering**

- ❖ **Placement:** Involves the Placement of proceeds derived from illegal activities – the movement of proceeds, frequently currency, from the scene of the crime to a place, or into a form, less suspicious and more convenient for the criminal.

- ❖ **Layering:** Involves the separation of proceeds from illegal source using complex transactions designed to obscure the audit trail and hide the proceeds.

- ❖ **Integration:** Involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations.

- **Anti-Money Laundering (AML) using Technology**

- **Financing of Terrorism**

Information Technology (IT) Act

The Information Technology Act was passed in 2000, amended in 2008 and the Rules were passed in 2011.

- ♦ The Act provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government.
- ♦ The Act provides the legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also deals with cybercrime and facilitates electronic commerce. It also defined cyber-crimes and prescribed penalties for them.
- ♦ The Amendment Act 2008 provides stronger privacy data protection measures as well as implementing reasonable information security by implementing ISO 27001 or equivalent certifiable standards to protect against cyber-crimes.
- ♦ **Cyber Crimes:** Also known as computer crime, it is defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones”.

Some examples of offences in IT Act which could impact Banks

Section 43 provides for Penalty and compensation for damage to computer, computer system, etc.

Section 65: Tampering with Computer Source Documents

Section 66: Computer Related Offences

Section 66-B: Punishment for dishonestly receiving stolen computer resource or communication device

Section 66-C: Punishment for identity theft

Section 66-D: Punishment for cheating by personation by using computer resource

Section 66-E: Punishment for violation of privacy

Sensitive Personal Data Information (SPDI)

The IT Act has a specific category, “Sensitive Personal Data or Information,” which consists of password, financial information (including bank account, credit card, debit card or other payment details), physical, physiological and mental health conditions, sexual orientation, medical records, and biometric information. This legally obligates all stakeholders (i.e., any individual or organization that collects, processes, transmits, transfers, stores or deals with sensitive personal data) to adhere to its requirements.