Sanjay Khemka Classes

Moulding Lives....

CA INTER

EIS

AMENDMENT

NOTES

Compiled By CA Sanjay Khemka

For more information, Please contact
(9830513015 / 7003063447)
Visit www.sanjaykhemkaclasses.com

CHAPTER 1

AUTOMATED BUSINESS PROCESSES

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Build an understanding on the concepts of Business Process, its automation and implementation.
- Understand concepts, flow and relationship of internal and automated controls.
- Acknowledge risks and controls of various business processes.
- Grasp the understanding on the structure and flow of business processes, related risks and controls.
- Comprehend the specific regulatory and compliance requirements of The Companies Act, 2013 and The Information Technology Act, 2000 as applicable to Computer related offences.

1.1 INTRODUCTION

In today's connected world where information flows at speed of light, success of any organization depends on its ability to respond to fast changing environment. The capability of any organization depends on its ability to take fast decisions. A large organization typically has several different kinds of Information systems built around diverse functions, organizational levels, and business processes that can automatically exchange information. All these information systems have fragmentation of data in hundreds of separate systems that degrade organizational efficiency and business performance. For instance – sales personnel might not be able to tell at the time they place an order whether the ordered items are in inventory, and manufacturing cannot easily use sales data to plan for next production.

The solution to this problem is provided by Enterprise Information Systems, by collecting data from numerous crucial business processes like manufacturing and production, finance and accounting, sales and marketing, and human resources and storing the data in single central data repository. 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.

An EIS provides a technology platform that enables organizations to integrate and coordinate their business processes on a robust foundation. An EIS provides a single system that is central to the organization that ensures information can be shared across all functional levels and management hierarchies. It may be used to amalgamate existing applications. An EIS can be used to increase business productivity and reduce service cycles, product development cycles and marketing life cycles. Other outcomes include higher operational efficiency and cost savings.

Example 1.1: When a customer places an order, the data flows automatically to other fractions of the company that are affected by placing the order, thus, leading to an enhanced coordination between these different parts of the business which in turn lowers costs and increases customer satisfaction. Refer to the Fig. 1.1.1.

- The order transaction triggers the warehouse to pick the ordered products and schedule shipment.
- The warehouse informs the factory to replenish whatever has depleted.

II. Supporting Processes (or Secondary Processes)

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. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

Example 1.2: Human Resource Management

The main HR Process areas are grouped into logical functional areas that include Recruitment and Staffing; Goal Setting; Training and Development; Compensation and Benefits; Performance Management; Career Development and Leadership Development.

III. Management Processes

Management Processes measure, monitor and control the activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting, and infrastructure or capacity management. Like supporting processes, management processes do not provide value directly to the customers. However, it has a direct impact on the efficiency of the enterprise.

Example 1.3: Process of Budgeting

Referring to the Fig. 1.2.3, in any enterprise, budgeting needs to be driven by the vision (what enterprise plans to accomplish) and the strategic plan (the steps to get there). Having a formal and structured budgeting process is the foundation for good business management, growth and development.

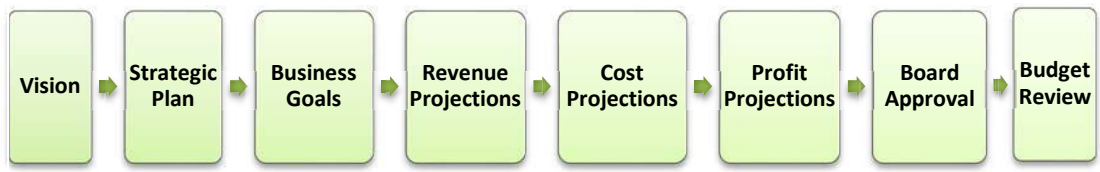


Fig. 1.2.3: Budgeting Process

Table 1.2.1 summarises various categories of business processes through an example.

Table 1.2.1: Examples representing all categories of Business Processes

S. No.	Nature of Business Decision	Description of decision
1	**Vision and Mission**	One of Asia's largest dairy product companies decided in 2005 to increase its turnover by 2x in next ten years. The present turnover is ₹ 10,000/- Crores.
2	**Management Process**	The top management sits down and lists down activities to be done to achieve the said turnover. This included: - Enter into new markets. It was decided to have an all India presence. At present, the company products are being sold across 20 out of 29 states including the four metros, namely Delhi, Mumbai, Chennai and Kolkata. - Launch new products. Presently, the company is mainly selling milk products. Few new products that are decided to be sold in future included Biscuits, Toast, Flour, Packaged Drinking Water. - Acquire existing dairies in markets where company has no presence.
3	**Support Process**	For all activities to be done as envisioned by top management, a huge effort is needed on human resources front. This includes- - Defining and creating a new management structure. - Performing all human resource activities as per activities listed above in management process.
4	**Operational Process**	Post the management processes, it is on the operational managers to implement the decisions in actual working form. It is here, where the whole hard job is done.

1.3 AUTOMATED BUSINESS PROCESSES

Today technology innovations are increasing day by day, technology is becoming easily available, cost of accessing and using technology is going down, internet connectivity in terms of speed and geographical spread is increasing day by day. All these factors are having a profound impact on the business processes being used by entity.

details can be used to demonstrate compliance during audits. For example- invoice issue to vendors.

- **Processes having significant impact on other processes and systems:** Some processes are cross-functional and have significant impact on other processes and systems. In cross functional processes, different departments within the same company work hand in hand to achieve a common goal. For example - the marketing department may work with sales department. Automating these processes results in sharing information resources and improving the efficiency and effectiveness of business processes.

1.3.4 Challenges involved in Business Process Automation

Automated processes are susceptible to many challenges, some of them are discussed below:

- **Automating Redundant Processes:** Sometimes organizations start off an automation project by automating the processes they find suitable for automation without considering whether such processes are necessary and create value or not. In other cases, some business processes and tasks require high amount of tacit knowledge that cannot be documented and transferred from one person to another and therefore seek employees to use their personal judgment. These processes are generally not good candidates for automation as these processes are hard to encode and automate.
- **Defining Complex Processes:** BPA requires reengineering of some business processes that requires significant amount of time to be allocated and spent at this stage. This requires a detailed understanding of the underlying business processes to develop an automated process.
- **Staff Resistance:** In most cases, human factor issues are the main obstacle to the acceptance of automated processes. Staff may see automation process as a way of reducing their decision-making power. This is due to the reason that with automated processes, the management has a greater visibility of the process and can make decisions that used to be made by the staff earlier. Moreover, the staff may perceive automated processes as threat to their jobs.
- **Implementation Cost:** The implementation of automated processes may be an expensive proposition in terms of acquisition/development cost of

automated systems and special skills required to operate and maintain these systems.

1.3.5 BPA Implementation

Business needs a reason to go for any new system. Benefits outlined in Table 1.3.1 are good indicators why any business shall go for automation for business process. Of all good reasons discussed above, one factor needs additional consideration that is global competition. Today the connected world has opened huge opportunities as well as brought new threats to any business. The increased availability of choice to customers about products/services makes it very important for businesses to keep themselves updated to new technology and delivery mechanisms. All these factors are forcing businesses to adopt BPA.

The steps to go about implementing Business Process Automation are depicted in Table 1.3.2. One important point to remember is that not all processes can be automated at a time. The best way to go about automation is to first understand the criticality of the business process to the enterprise. Let us discuss the key steps in detail.

(i) Step 1: Define why we plan to implement a BPA?

The primary purpose for which an enterprise implements automation may vary from enterprise to enterprise. A list of generic reasons for going for BPA may include any or combination of the following:

- Errors in manual processes leading to higher costs.
- Payment processes not streamlined, due to duplicate or late payments, missing early pay discounts, and losing revenue.
- Paying for goods and services not received.
- Poor debtor management leading to high invoice aging and poor cash flow.
- Not being able to find documents quickly during an audit or lawsuit or not being able to find all documents.
- Lengthy or incomplete information of new employee or new account on-boarding.
- Unable to recruit and train new employees, but where employees are urgently required.
- Lack of management understanding of business processes.
- Poor customer service.

(vi) Step 6: Calculate the RoI (Return on Investment) for project

The right stakeholders need to be engaged and involved to ensure that the benefits of BPA are clearly communicated, and implementation becomes successful. Hence, the required business process owners have to be convinced so as to justify the benefits of BPA and get approval from senior management. A lot of meticulous effort would be required to convince the senior management about need to implement the right solution for BPA. The right business case must be made covering technical and financial feasibility so as to justify and get approval for implementing the BPA. The best way to convince would be to generate a proposition that communicates to the stakeholders that BPA shall lead to not only cost savings for the enterprise but also improves efficiency and effectiveness of service offerings.

Some of the methods for justification of a BPA proposal may include:

- Cost Savings, being clearly computed and demonstrated.
- How BPA could lead to reduction in required manpower leading to no new recruits need to be hired and how existing employees can be re-deployed or used for further expansion.
- Savings in employee salary by not having to replace those due to attrition.
- The cost of space regained from paper, file cabinets, etc. is reduced.
- Eliminating fines to be paid by entity due to delays being avoided.
- Reducing the cost of audits and lawsuits.
- Taking advantage of early payment discounts and eliminating duplicate payments.
- Ensuring complete documentation for all new accounts.
- New revenue generation opportunities.
- Collecting accounts receivable faster and improving cash flow.
- Building business reputation by providing superior levels of customer service.
- Instant access to records (e.g. public information, student transcripts, medical records).

The above can be very well presented to justify the proposal and convince management to go ahead with the project of BPA implementation as required for the enterprise.

Step 4: Define the objectives/goals to be achieved by implementing BPA.

The objective behind the present exercise is to ensure that there are no production losses due to non-availability of critical items of inventory. This shall automatically ensure timely delivery of goods to customer.

Step 5: Engage the business process consultant.

ABC Limited, a consultant of repute, has been engaged for the same. The consultant has prior experience and knowledge about entity's business.

Step 6: Calculate the ROI for project.

The opportunity loss for the project comes to around ₹ 100/- lakhs per year. The cost of implementing the whole BPA shall be around ₹ 50/- lakhs. It is expected that the opportunity loss after BPA shall reduce to ₹ 50 lakhs in year one, ₹ 25/- lakhs in later years for the next five years.

Step 7: Developing the BPA.

Once the top management says 'Yes', the consultant develops the necessary BPA. The BPA is to generate purchase orders as soon as an item of inventory reaches its re-order level. To ensure accuracy, all data in the new system need to be checked and validated before being put the same into system:

- Item's inventory was physically counted before uploading to new system.
- Item's re-order levels were recalculated.
- All items issued for consumption were timely updated in system.
- All Purchase orders automatically generated are made available to Purchase manager at the end of day for authorizations.

Step 8: Testing the BPA.

Before making the process live, it should be thoroughly tested.

Case 2: Automation of Employees' Attendance System

Various steps of automation are given as follows:

Step 1: Define why we plan to go for a BPA?

The system of recording of attendance being followed is not generating confidence in employees about the accuracy. There have been complaints that salary pay-outs are not as per actual attendance. It has also created friction and differences between employees, as some may feel that other employees have been paid more for their salary has not been deducted for being absent.

Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.
- Their data classification would normally be Proprietary, highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. It is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets. A good example of potential threats involves malware, ransomware, and viruses. Attackers often focus on the total destruction of an asset, Distributed Denial of Services (DDoS), or social engineering to accomplish their goals.

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (example - system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example - vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Some examples of vulnerabilities are as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.

- Passwords should not be stored in configuration files instead some secure mechanism should be used.

Similarly, for other vulnerabilities, different counter measures may be used.

Risk: Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence. The planned objective could be any aspect of an enterprise's strategic, financial, regulatory and operational processes, products or services. The degree of risk associated with an event is determined by the likelihood (uncertainty, probability) of the event occurring, the consequences (impact) if the event were to occur and it's timing.

Example 1.5: Fig. 1.4.1 depicts the relationship and different activities among the aforementioned terms.

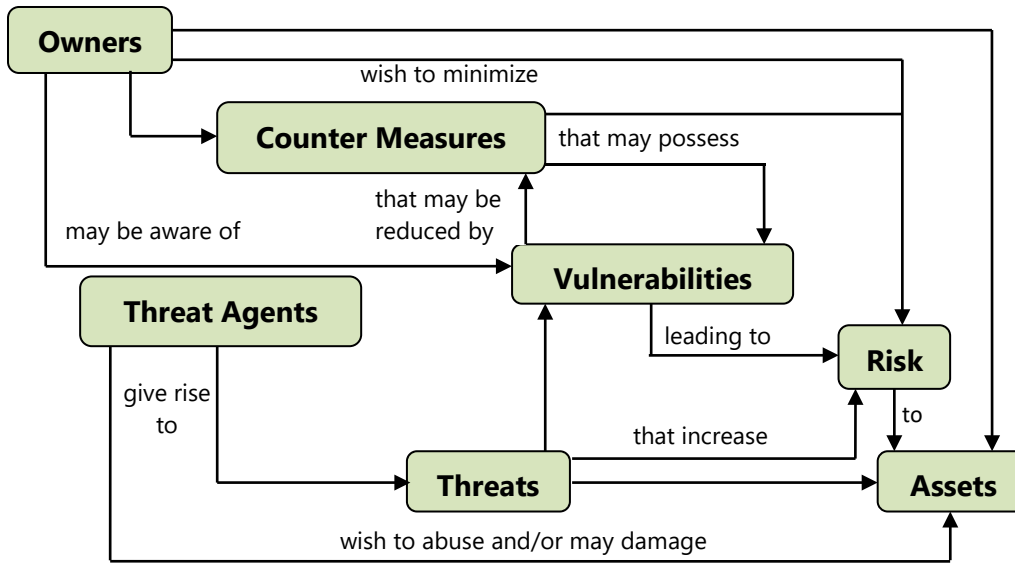


Fig. 1.4.1: Risk and Related Terms

1.4.2 Sources of Risk

When an enterprise adopts automation to support its critical business processes, it exposes itself to several risks, such as downtime due to failure of technology. The most important step in risk management process is to identify the sources of risk, the areas from where risks can occur. This will give information about the possible threats, vulnerabilities and accordingly appropriate risk mitigation strategy can be adapted. Some of the common sources of risk are commercial and legal relationships, economic circumstances, human behavior, natural events,

global data protection requirements and local tax or statutory laws. New and emerging regulations can have a wide-ranging impact on management's strategic direction, business model and compliance system. It is, therefore, important to consider regulatory requirements while evaluating business risks.

- **Operational Risks:** Operational risks include those risks that could prevent an organization from operating in the most effective and efficient manner or be disruptive to other operations due to inefficiencies or breakdown in internal processes, people and systems. Examples include risk of loss resulting from inadequate or failed internal processes, fraud or any criminal activity by an employee, business continuity, channel effectiveness, customer satisfaction and product/service failure, efficiency, capacity, and change integration.
- **Hazard Risks:** Hazard risks include risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.
- **Residual Risks:** This includes any risk remaining even after the counter measures are analyzed and implemented. An organization's management of risk should consider these two areas - Acceptance of residual risk and Selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimized, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed.

B. Technology Risks: Automated processes are technology driven. The dependence on technology in BPA for most of the key business processes has led to various challenges. All risks related to the technology equally applicable to BPA. As technology is taking new forms and transforming as well, the business processes and standards adapted by enterprises should consider these new set of IT risks and challenges which are described below:

(i) **Downtime due to technology failure:** Information system facilities may become unavailable due to technical problems or equipment failure. A common example of this type of failure is non-availability of system due to server failure.

(ix) **External threats leading to cyber frauds/ crime:** The system environment provides access to customers anytime, anywhere using internet. Hence, information system which was earlier accessible only within and to the employees is now exposed as it's open to be accessed by anyone from anywhere. Making the information available is business imperative but this is also fraught with risks of increased threats from hackers and others who could access the software to commit frauds/crime.

(x) **Higher impact due to intentional or unintentional acts of internal employees:** Employees in a technology environment are the weakest link in an enterprise. Employees are expected to be trusted individuals that are granted extended privileges, which can easily be abused.

(xi) **New social engineering techniques employed to acquire confidential credentials:** Fraudsters use new social engineering techniques such as socializing with employees and extracting information which is used to commit frauds. For example: extracting information about passwords from staff acting as genuine customer and using it to commit frauds.

(xii) **Need for governance processes to adequately manage technology and information security:** Controls in system should be implemented from macro and business perspective and not just from function and technology perspective. With BPA, technology becomes the key enabler for the organization and is implemented across the organization. The senior management should be involved in directing how technology is deployed in and approve appropriate policies. This requires governance process to implement security as required.

(xiii) **Need to ensure continuity of business processes in the event of major exigencies:** The high dependence on technology makes it imperative to ensure resilience to ensure that failure does not impact the organization's services. Hence, a documented business continuity plan with adequate technology and information systems should be planned, implemented and monitored.

C. Data related risks: The primary concern of any organization should be its data, because it is often a unique resource. All data and applications are susceptible to disruption, damage and theft. Data related risks include unauthorized implementation or modification of data and software and are discussed below:

(i) **Data Diddling:** This involves the change of data before or after they entered the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.

(ii) **Bomb:** Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.

(iii) **Christmas Card:** It is a well-known example of Trojan and was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half-finished work.

(iv) **Worm:** A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses. Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

(v) **Rounding Down:** This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

(vi) **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, ₹ 21,23,456.39 becomes ₹ 21,23,456.40, while in the Salami technique the transaction amount ₹ 21,23,456.39 is truncated to either ₹ 21,23,456.30 or ₹ 21,23,456.00, depending on the logic.

(vii) **Trap Doors:** Trap doors allow insertion of specific logic such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

(viii) **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes user login again.

(ix) **Asynchronous Attacks:** They occur in many environments where data can be moved synchronously across telecommunication lines. These kind of attacks make use of the timing difference between the time when the data is inputted to the system and the time when it gets processed by the system. Data that is waiting to be transmitted are liable to unauthorized access called **Asynchronous Attack**. These attacks are hard to detect because they are usually very small pin like insertions and are of following types:

- **Data Leakage:** This involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- **Subversive Attacks:** These can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.
- **Wire-Tapping:** This involves spying on information being transmitted over communication network.
- **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.

1.4.4 Risk Management Strategies

Risk Analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Effective risk management begins with a clear understanding of an enterprise's risk appetite and identifying high-level risk exposures. The unacceptable high levels of risks can be controlled by designing and implementing adequate proactive controls.

Risk Management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.

But it is not always appropriate to counter risks by implementing controls because controls involve cost. After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Based on the type of risk, project and its significance to the business; Board and Senior Management may choose to take up any of the following risk management strategy in isolation or combination as required:

- ***Tolerate/Accept the risk. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate. The risks should be reviewed periodically to ensure that their impact remains low. A common example of risk acceptance is planning for potential production delays (within a reasonable time range) since it's often difficult to predict a precise delivery schedule in advance.***
- ***Terminate/Eliminate the risk. Especially in the case of risks that have high probability and impact values, it may be best to modify any project strategy to avoid them altogether. For example - it is possible for a risk to be associated with the use of a technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.***
- ***Transfer/Share the risk. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.***
- ***Treat/mitigate the risk. Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects. A good example of risk mitigation is planning for the eventuality in case an enterprise won't have sufficient capacity or supplies to deal with a very high demand. In that case, enterprise shall have a mitigation strategy in place that allows them to rapidly scale their capacity, or to subcontract some of the work to other parties to meet the high demand.***

communication also should occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

(viii) Monitoring: The entire ERM process should be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of the ERM processes or a combination of both.

1.6 CONTROLS

Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected. The main objectives of information controls are safeguarding of assets, maintenance of data integrity, effectiveness in achieving organizational objectives, and efficient consumption of resources. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

Example 1.6: Purchase to Pay (P2P)-Given below is a simple example of controls for the Purchase to Pay cycle, which is broken down to four main components as shown in the Fig. 1.6.1 *(P2P cycle is explained in later part of chapter)*.

- **Purchases:** When an employee working in a specific department (e.g., marketing, operations, sales, etc.) wants to purchase something required for carrying out the job, he/she will submit a Purchase Requisition (PR) to a manager for approval. Based on the approved PR, a Purchase Order (PO) is raised. The PO may be raised manually and then input into the computer system or raised directly by the computer system.
- **Goods Receipt:** The PO is then sent to the vendor, who will deliver the goods as per the specifications mentioned in the PO. When the goods are received at the warehouse, the receiving staff checks the delivery note, PO number etc. and acknowledges the receipt of the material. Quantity and quality are checked and any unfit items are rejected and sent back to the vendor. A Goods Receipt Note (GRN) is raised indicating the quantity

received. The GRN may be raised manually and then input into the computer system or raised directly by computer system.

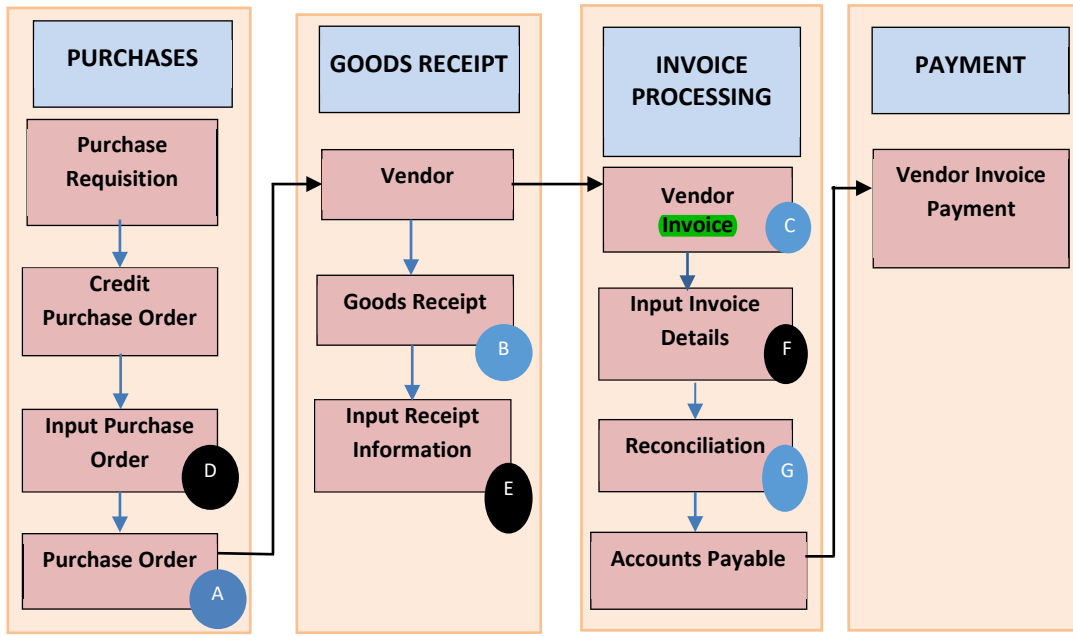


Fig. 1.6.1: Purchase Cycle – Sample Controls

- **Invoice Processing:** The vendor sends the invoice to the accounts payable department who will input the details into the computer system. The vendor invoice is checked with the PO to ensure that only the goods ordered have been invoiced and at the negotiated price. Further the vendor invoice is checked with the GRN to ensure that the quantity ordered has been received.
- **Payment:** If there is no mismatch between the PO, GRN and vendor invoice; the payment is released to the vendor based on the credit period negotiated with the vendor.

Based on the mode of implementation, these controls can be Manual, Automated or Semi-Automated (partially manual and partially automated). The objective of a control is to mitigate the risk.

- **Manual Control:** Manually verify that the goods ordered in PO (A) are received (B) in good quality and the vendor invoice (C) reflects the quantity and price that are as per the PO (A).

(a) Information Technology General Controls (ITGC)

ITGC also known as Infrastructure Controls pervade across different layers of IT environment and information systems and apply to all systems, components, processes, and data for a given enterprise or systems environment. ITG controls are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions.

General controls include, but are not limited to:

- **Information Security Policy:** An Information Security policy is the statement of intent by the senior management about how to protect a company's information assets. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization. The security policy is approved by the senior management and encompasses all areas of operations and drives access to information across the enterprise and other stakeholders.
- **Administration, Access, and Authentication:** Access controls are measures taken to ensure that only the authorized persons have access to the system and the actions they can take. IT should be administered with appropriate policies and procedures clearly defining the levels of access to information and authentication of users.
- **Separation of key IT functions:** Secure deployment of IT requires the organization to have separate IT organization structure with key demarcation of duties for different personnel within IT department and to ensure that there are no Segregation of Duties (SoD) conflicts.
- **Management of Systems Acquisition and Implementation:** Management should establish acquisition standards that address the security, functionality, and reliability issues related to systems acquisition. Hence, process of acquisition and implementation of systems should be properly controlled.
- **Change Management:** Deployed IT solutions and its various components must be changed in tune with changing needs as per changes in technology environment, business processes, regulatory, compliance requirements and changing needs of the users. These changes impact the live environment of the organization. Hence, change management process should be

implemented to ensure smooth transition to new environments covering all key changes including hardware, software and business processes. All changes must be properly approved by the management and tested before implementation.

- **Backup, Recovery and Business Continuity:** Heavy dependence on IT and criticality makes it imperative that resilience of the organization operations should be ensured by having appropriate business continuity including backup, recovery and off-site data center. Business continuity controls ensure that an organization can prevent interruptions (violations) and processing can be resumed in an acceptable period of time.
- **Proper Development and Implementation of Application Software:** Application software drives the business processes of the organizations. These solutions in case developed and implemented must be properly controlled by using standard software development process. Controls over software development and implementation ensure that the software is developed according to the established policies and procedures of the organization. These controls also ensure that the systems are developed within budgets, within budgeted time, security measures are duly incorporated, and quality and documentation requirements are maintained.
- **Confidentiality, Integrity and Availability of Software and data files:** Security is implemented to ensure Confidentiality, Integrity and Availability (CIA) of information. **Confidentiality** refers to protection of critical information to ensure that information is only available to persons who have right to see the same. **Integrity** refers to ensuring that no unauthorized amendments can be made in data in all stages of processing. **Availability** refers to ensuring availability of information to users when required.
- **Incident response and management:** There may be various incidents created due to failure of IT. These incidents need to be appropriately responded and managed as per pre-defined policies and procedures.
- **Monitoring of Applications and supporting Servers:** The Servers and applications running on them are monitored to ensure that servers, network connections and application software along with the interfaces are working continuously.
- **Value Added areas of Service Level Agreements (SLA):** SLA with vendors is regularly reviewed to ensure that the services are delivered as per specified performance parameters.

its governance responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

II. Risk Assessment

Every entity faces a variety of risks from external and internal resources. Risk may be defined as the possibility that an event will occur and adversely affect the achievement of objectives. **Risk Assessment** involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances.

Thus, Risk Assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives linked at different levels of the entity. Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives. Because economic, industry, regulatory and operating conditions will continue to change; risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Risk Assessment includes the following:

- ♦ Identification of threats and vulnerabilities in the system;
- ♦ Potential impact or magnitude of harm that a loss of CIA would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and

New technology provides the potential for dramatically enhanced business performance, improved and demonstrated information risk reduction and security measures. Technology can also add real value to the organization by contributing to interactions with the trading partners, closer customer relations, improved competitive advantage and protected reputation.

III. Control Activities

Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all

1.8.2 Data Flow Diagrams (DFDs)

Data Flow Diagrams are used to graphically represent the flow of data in a business information system from one place to another. DFD describes the processes that are involved in a system to transfer data from the input to the file storage and reports generation. DFD uses few simple symbols to illustrate the flow of data among external entities such as people or organizations, etc.. DFDs describe the processes showing how these processes link together through data stores and how the processes relate to the users and the outside world. The limitation of this diagram is that processes are not identified to functional departments.

Example 1.14: The Fig. 1.8.8 depicts a simple business process (traditional method) flow.

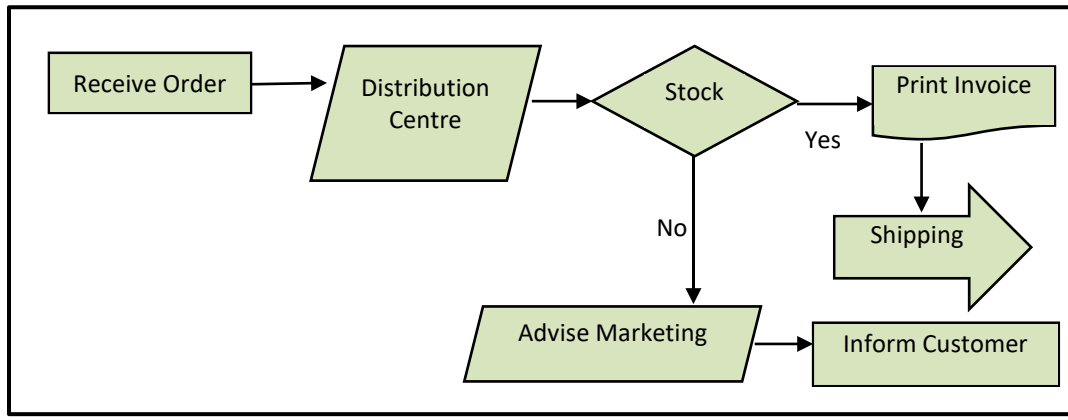


Fig. 1.8.8: Simple Flow chart of Sales (Example: 1.14)

DFD basically provides an overview of:

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

Example 1.15: In the simple DFD shown in Fig. 1.8.9, please note that the processes are specifically identified to the function using "swimlanes". Each lane represents a specific department where the business process owner can be identified. The business process owner is responsible for ensuring that adequate controls are implemented to mitigate any perceived business process risks.

the responsibilities are clearly defined. Let us understand flow from the perspective of each department/entity.

(i) User Department

- A user in an enterprise may require some material or service. Based on the need and justification, the user raises a Purchase Request (PR) to the Procurement Department (PD).

(ii) Procurement Department (PD)

- PD receives the PR and prioritizes the request based on the need and urgency of the user.
- It is then the responsibility of the PD to find the best source of supply, for the specific material/service. PD will then request the potential vendors to submit their quotes, based on which negotiations on price, quality and payment terms, will take place.
- The Purchase Order (PO) will then be released to the selected vendor.

(iii) Vendor

- The vendor receives the PO and carries out his own internal checks.
- Matches the PO with the quotation sent and in the event of any discrepancy, will seek clarification from the enterprise.
- If there are no discrepancies, the vendor will raise an internal sales order within the enterprise.
- The material is then shipped to the address indicated in the PO.
- The Vendor Invoice (VI) is sent to the Accounts Payable department, based on the address indicated in the PO.

(iv) Stores

- Receives the material.
- Checks the quantity received with the PO and quality with the users. If there is any discrepancy the vendor is immediately informed.
- The Goods Received Note (GRN) is prepared based on the actual receipt of material and the stores stock updated. The GRN is then sent to the Accounts Payable department for processing the payment.
- A Material Issue Note is created, and the material is sent to the concerned user.

transactions over the internet without fear of misuse. Some advantages of Cyber laws are discussed below:

- The Act offers the crucial legal framework so that any information which is in the form of electronic records shall not be denied legal effect, validity or enforceability. This legal framework allows for the authentication and origin of electronic records/communications through digital signature.
- Considering the growth in electronic transactions and communications, the Act seeks to empower government departments to encourage digital data format in terms of accepting filing, creating and retention of official documents.
- The Act allows the emails to be a valid and legal form of communication in India that can be duly produced and approved in a court of law; thus providing boon to e-businesses in India.
- As the Act sanctions and gives legal validity to Digital signatures, many corporate companies have entered into the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Government can issue notification on the web thus heralding e-governance under the Act.
- The Act enables the companies to approach any office, authority, body or agency owned or controlled by the appropriate Government to file any form, application or any other document in electronic form as prescribed by them.
- The corporates get statutory remedy in case their computer systems, data or network get damaged by intruders. The Act allows remedy in the form of monetary damages not exceeding ₹ 1 crore.

III. Privacy of Online Data

When people access the Web, they often entrust vital personal information such as their name, address, credit card number, etc. to their Internet Service Providers and to the websites they accessed. This information may fall into wrong hands and may be used for illegitimate purposes. The organizations that collect and manage the personal information of people must also protect it against misuse. The collection of personal information by an organization is an important issue related to the privacy of online data. Privacy laws vary in different countries. Multi-national companies often receive information in one country and process this information in some other country where privacy laws are altogether

manual processes. The customers of the company are becoming more demanding with respect to higher quality of products and delivery time.

To remain competitive in the market and to overcome the issues faced by its customers, the company decided to optimize and streamline its essential business processes using the latest technology to automate the functions involved in carrying out these essential processes. The management of the company is very optimistic that with automation of business processes, it will be able to extract maximum benefit by using the available resources to their best advantage. Moreover, with automation the company will be able to integrate various processes and serve its customers better and faster. The management is aware that the automation of business processes will lead to new types of risks in the company's business. The failure or malfunction of any critical business process will cause significant operational disruptions and materially impact its ability to provide timely services to its customers. The management of ABC Ltd. adopted different Enterprise Risk Management (ERM) strategies to operate more effectively in environment filled with risks. To reduce the impact of these risks, the company also decided to implement necessary internal controls.

Answer the following Questions:

1. The processes automated by ABC Ltd. are susceptible to many direct and indirect challenges. Which of the following factor cannot be considered valid in case the company fails to achieve the desired results?

   (a) The business processes are not well thought or executed to align with business objectives.

   (b) The staff may perceive automated processes as threat to their jobs.

   (c) The documentation of all the automated business processes is not done properly.

   (d) The implementation of automated processes in the company may be an expensive proposition.

2. The processes automated by ABC Ltd. are technology driven. The dependence on technology in key business processes exposed the company to various internal as well as external threats. According to you, external threats leading to cyber-crime in BPA is because:

   (a) Organizations may have a highly-defined organization structure with clearly defined roles, authority and responsibility.

- Hence every ledger is classified in one of the four categories, i.e. **Assets, Expense, Income** or **Liability**. It cannot be categorized in more than one category. The examples of Ledger account are as follows:

  (a) **Assets** includes Cash, property plant and equipment, accounts receivable etc.

  (b) **Expense** includes salary, insurance, utilities etc.

  (c) **Income** includes sales, interest income, rent income and other operating income etc.

  (d) **Liabilities** includes Debt/loans, accounts payable, outstanding expenses etc.

- Difference between Total Income and Total Expenses, i.e. Profit & Loss, as the case may be, is taken to Balance Sheet. So, everything in accounting software boils down to Balance Sheet. Balance Sheet is the last point in accounting process.

- **Income** and **Expense** ledgers are considered in **Profit and Loss Account** and **Asset** and **Liability** ledgers are considered in **Balance Sheet**.

- Accounting software does not recognize any ledger as Personal, Real or Nominal; instead it recognizes it as an Asset, Liability, Income or Expense Ledger.

VI. Grouping of Ledgers

At the time of creation of any new ledger, it must be placed under a particular group. There are four basic groups in Accounting, i.e. **Income**, **Expense**, **Asset**, **Liability**. There may be any number of sub groups under these four basic groups. Grouping is important as this is way to tell software about the nature of the ledger and where it is to be shown at the time of reporting.

For example- Cash ledger is an asset ledger and should be shown under current assets in Balance Sheet. If we group cash ledger under indirect expenses, it shall be displayed in profit and loss account as expenditure. Liabilities are recorded on the balance sheet and measure the obligations that a company needs to make. Liabilities include loans, accounts payable, deferred revenues, and accrued expenses. In the similar way, Income includes Direct income and Indirect income. The direct income can include Apprentice Premium, factory income and indirect incomes include Bad Debts and Commission Received by company. Software cannot prevent incorrect grouping of ledger.

2.3.2 Risks and Controls related to ERP Implementation

ERP system implementation is a huge task and requires lot of time, money and above all patience. The success or failure of any ERP or saying it in terms of payback or ROI of an ERP, is dependent on its successful implementation and once implemented proper usage.

Tables 2.3.1(A,B,C,D,E) provide extensive discussion on the risks related to various aspects including – **People**, **Process**, **Technological**, **Implementation** and **Post implementation issues** that arise during implementation and related controls respectively.

1. People Aspect: Employees, Management, implementation team, consultants and vendors are the most crucial factor that decides the success or failure of an ERP System.

Table 2.3.1(A): Risks and corresponding Controls related to People

Aspect	Risk Associated	Control Required
Change Management	Change will occur in the employee's job profile in terms of some jobs becoming irrelevant and some new jobs created.	Proper training of the users with well documented manuals. Practical hands on training of the ERP System should be provided so that the transition from old system to ERP system is smooth and hassle free.
	The way in which organization functions will change, the planning, forecasting and decision-making capabilities will improve, information integration happening etc.	It requires ensuring that a project charter or mission statement exists. The project requirements are to be properly documented and signed by the users and senior management.
	Changing the scope of the project is another problem.	This requires clear defining of change control procedures and holds everyone to them.
Training	Since the greater part of the training takes place towards the end of the ERP implementation cycle, management may curtail the	Training is a project-managed activity and shall be imparted to the users in an organization by the skilled consultants and representatives of the hardware

	and the tools are underutilised.	
Application Portfolio Management	These processes focus on the selection of new business applications and the projects required in delivering them.	By bringing to the light the sheer number of applications in the current portfolio, IT organizations can begin to reduce duplication and complexity.

4. Implementation Aspect: Many times, ERP implementations are withdrawn because of the following factors.

Table 2.3.1(D): Risks and corresponding Controls related to Implementation Aspect

Aspect	Risk Associated	Control Required
Lengthy implementation time	ERP projects are lengthy that takes anywhere between 1 to 4 years depending upon the size of the organization. Due to technological developments happening every day, the business and technological environment during the start and completion of the project will never be the same. Employee turnover is another problem.	Care must be taken to keep the momentum high and enthusiasm live amongst the employees, so as to minimize the risk.
Insufficient Funding	The budget for ERP implementation is generally allocated without consulting experts and then implementation is stopped along the way, due to lack of funds.	It is necessary to allocate necessary funds for the ERP implementation project and then allocate some more for contingencies.
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	This can be controlled by removing redundant data, using

Table 2.3.2: Users Database of Indradhanu Consulting Private Limited (Illustrative)

S. No.	Employee Name	Designation	Allow Access To	Dis-allow access to
1	Swapnil Ghate	Director	Complete access to all the reports, masters and transactions but limited to viewing purpose only. No need to give any alteration or creation access.	Creation / Alteration
2	CA. Pankaj Deshpande	CFO	Same as Director but in some cases, creation or alteration access to masters and transactions may be given.	Creation / Alteration (with few exceptions)
3	Mayura Rahane	Head HR	Full access to all HR related masters and transactions, e.g. Creation and alteration of employees, pay heads, salary structures, leave types etc. Creation and alteration of leave and salary calculations etc.	All non-related masters, transactions and reports.
4	Amit Shriwas	Head-Accounts	Full access to all accounting masters, transactions and reports.	All non-related masters, transactions and reports.
5	Sachi Dongre	Accountant	Only voucher entry and viewing accounting master data.	Reports like Balance Sheet, Profit & Loss access to ledger creation or alteration.

the process throughout the organization. Assigning enterprise process owners and aligning employees' performance reviews and compensation to the value creation of the processes could accomplish this.

Process management is based on a view of an organization as a system of interlinked processes which involves concerted efforts to map, improve and adhere to organizational processes; whereas traditional organizations are composed of departments and functional stages, this definition views organization as networks or systems of processes. Process orientation is at the core of BPM. Hence, It is important to get understand clearly that distinction of the traditional functional organizations and process organization.

2.6.2 Business Process Flow

As discussed earlier, a **Business Process** is a prescribed sequence of work steps performed to produce a desired result for an organization. A business process is initiated by a kind of event, has a well-defined beginning and end, and is usually completed in a relatively short period. Organizations have many different business processes such as completing a sale, purchasing raw materials, paying employees and vendors, etc. Each of the business processes has either a direct or indirect effect on the financial status of the organization. The number and type of business processes and how the processes are performed would vary across enterprises and is also impacted by automation. However, most of the common processes would flow a generic life cycle.

Example 2.6: Accounting Process Flow

Accounting or Book-keeping cycle covers the business processes involved in recording and processing accounting events of a company. It begins when a transaction or financial event occurs and ends with its inclusion in the financial statements. A typical life cycle of an accounting transaction may include the following transactions as depicted in Fig. 2.6.1:

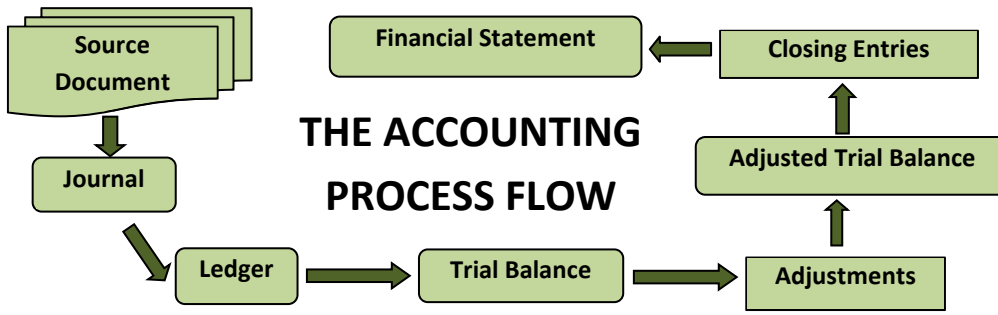


Fig. 2.6.1: Accounting Process Flow

B. Functional Modules of ERP

Business process may change as per type of business. There may be different business units within a business. Hence, different modules are possible in an integrated system. There may be modules defined as under. Fig. 2.6.2 shows different business process modules in ERP System. There may be some other modules also. Different types of industries require different modules.

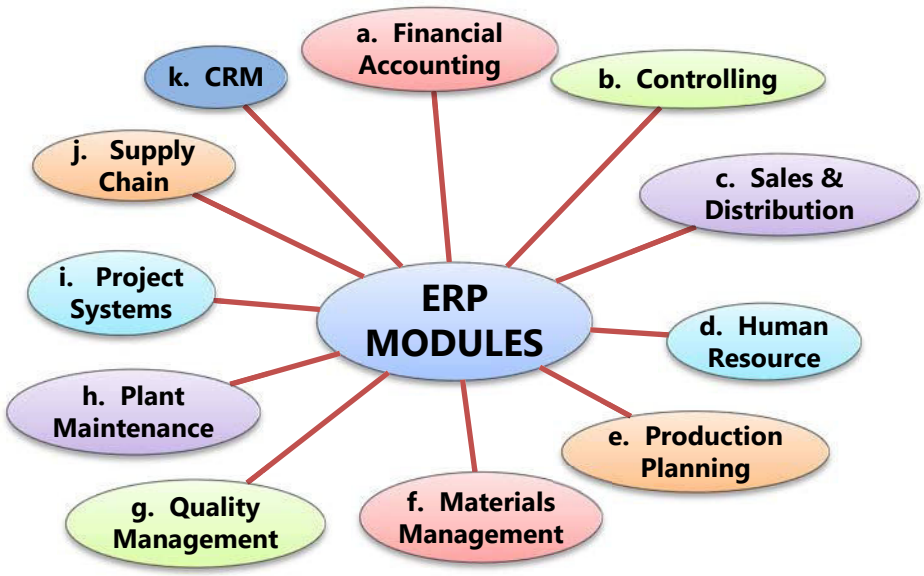


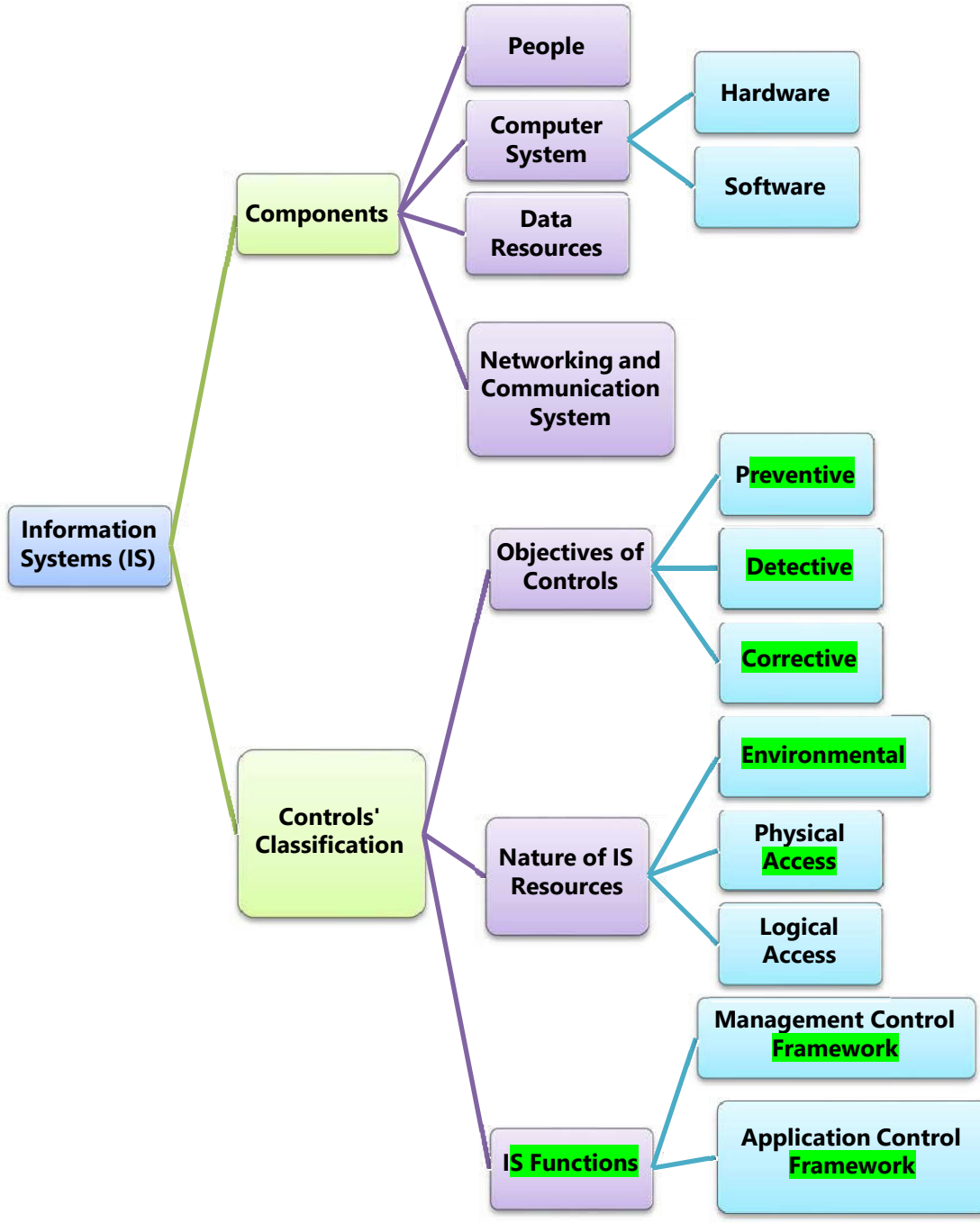
Fig. 2.6.2: ERP Modules

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. Every module is somehow connected with this module.
The key features of this module are as under:

- Tracking of flow of financial data across the organization in a controlled manner and integrating all the information for effective strategic decision making.
- Creation of Organizational Structure (Defining Company, Company Codes, business Areas, Functional Areas, Credit Control, Assignment of Company Codes to Credit Controls).

CHAPTER OVERVIEW



- **Processing:** A process is a series of steps undertaken to achieve desired outcome or goal. Information Systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes.
- **Output:** The system processes the data by applying the appropriate procedure on it and the information thus produced is stored for future use or communicated to user.
- ***Storage:*** ***The storage of data shall be done at the most detailed level possible. Regular backups should be stored in a geographically different locations to avoid impact on both the original data storage and the backup data storage due to any major disasters such as flooding or fires etc.***

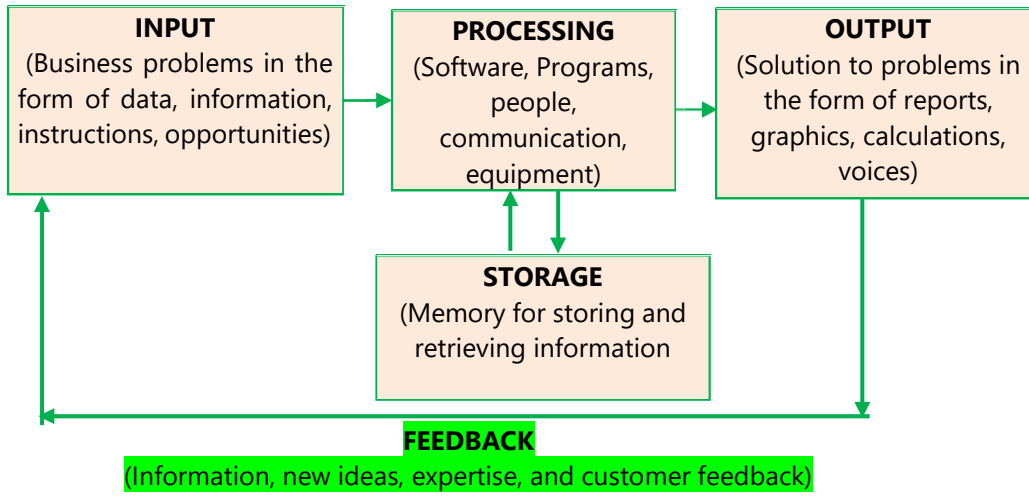


Fig. 3.2.1: Functions of Information Systems

- **Feedback:** Apart from these activities, information system also needs feedback that is returned to appropriate members of the enterprises to help them to evaluate at the input stage.

These basic activities of an information system that are defined above, helps enterprise in making decisions, control operations, analyze problems and creates new products or services as an output.

3.3 COMPONENTS OF INFORMATION SYSTEMS

With the help of information systems enterprises and individuals can use computers to collect, store, and process, analyze, and distribute information. There are different types of information systems, i.e. Manual (paper and pencil) information

Capacity	RAM memory is large and high capacity.	ROM is generally small and of low capacity.

To bridge the huge differences of speed between the Registers and Primary memory, the Cache Memory is introduced.

Cache memory is a smaller, extremely fast memory type built into a computer's Central Processing Unit (CPU) and that acts as a buffer between RAM and the CPU. Cache Memory stores copies of the data from the most frequently used main memory locations so that CPU can access it more rapidly than main memory.

The differences between Processor Registers and Cache Memory are provided below in the Table 3.3.2.

Table 3.3.2: Processor Registers vs Cache Memory

Processor Registers	Cache Memory
These are high speed memory units within CPU for storing small amount of data (mostly 32 or 64 bits).	It is fast memory built into a computer's CPU and is used to reduce the average time to access data from the main memory. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere.
The registers are the only Memory Units most processors can operate on directly.	Cache memory is an interface between CPU and Main storage. It is not directly accessible for operations.

(b) **Secondary Memory:** Secondary memory devices are non-volatile, have greater capacity (they are available in large size), greater economy (the cost of these is lesser compared to register and RAM) and slow speed (slower in speed compared to registers or primary storage). Examples include Hard disk, Pen drive, Memory card etc. Table 3.3.3 provides the key differences between Primary Memory and Secondary Memory.

Table 3.3.3: Primary Memory vs Secondary Memory

Aspect	Primary/Main Memory	Secondary Memory
Basic	Primary memory is directly accessible by Processor/CPU.	Secondary memory is not directly accessible by CPU.

Data	Instructions or data to be currently executed are copied to main memory.	Data to be permanently stored is kept in secondary memory.
Volatility	Primary memory is usually volatile.	Secondary memory is non-volatile.
Formation	Primary memories are made of semiconductors.	Secondary memories are made of magnetic and optical material.
Access Speed	Accessing data from primary memory is faster.	Accessing data from secondary memory is slower.
Access	Primary memory is accessed by the data bus.	Secondary memory is accessed by input-output channels.
Size	The computer has a small primary memory.	The computer has a larger secondary memory.
Expense	Primary memory is costlier than secondary memory.	Secondary memory is cheaper than primary memory.
Memory	Primary memory is an internal memory.	Secondary memory is an external memory.

With respect to CPU, the memory is organized as follows (as shown in the Fig. 3.3.4):

- Registers that have small capacity, high cost, very high speed are placed inside the CPU.
- Cache memory is placed next in the hierarchy followed by Primary memory.
- Secondary memory is the farthest from CPU (large capacity, low cost, low speed).

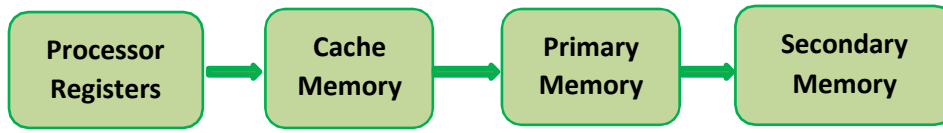


Fig. 3.3.4: Computer Memory hierarchy

(iv) Output Devices: Computer systems provide output to decision makers at all levels in an enterprise to solve business problems, the desired output may be in

visual, audio or digital forms. Output devices are devices through which system responds. Visual output devices like - a display device visually conveys text, graphics, and video information. Information shown on a display device is called soft copy because the information exists electronically and is displayed for a temporary period. Display devices include CRT monitors, LCD monitors and displays, gas plasma monitors, and televisions. Some types of output are textual, graphical, tactile, audio, and video.

- **Textual output** comprises of characters that are used to create words, sentences, and paragraphs.
- **Graphical outputs** are digital representations of non-text information such as drawings, charts, photographs, and animation.
- **Tactile output** such as raised line drawings may be useful for some individuals who are blind.
- **Audio output** is any music, speech, or any other sound.
- **Video output** consists of images played back at speeds to provide the appearance of full motion.

Most common examples of output devices are Speakers, Headphones, Screen (Monitor), Printer, Voice output communication aid, Automotive navigation system, Video, Plotter, Wireless etc.

II. Software

Software is defined as a set of instructions that tell the hardware what to do. Software is not tangible; it cannot be touched. Software is created through the process of programming. When programmers create software, what they are really doing is simply typing out lists of instructions that tell the hardware what to execute. Without software, the hardware would not be functional. Software can be broadly divided into two categories: **Operating System Software** and **Application Software** as shown in the Fig. 3.3.2.

(a) Operating System Software

An **Operating System (OS)** is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs. The operating system is a vital component of the system software in a computer system. Operating systems make the hardware usable and manage them by creating an interface between the hardware and the user. Application programs usually require an operating system to function that provides a convenient environment to users for executing their programs. Computer hardware with

Internet but are instead installed on a device and work with a single user at a time. Various operations that can be performed on these files include adding new files to database, deleting existing files from database, inserting data in existing files, modifying data in existing files, deleting data in existing files, and retrieving or querying data from existing files. DBMS packages generally provide an interface to view and change the design of the database, create queries, and develop reports. Commercially available DataBase Management Systems are Oracle, MySQL, SQL Servers and DB2 etc. whereas Microsoft Access and Open Office Base are examples of personal DBMS.

Advantages of DBMS

- **Permitting Data Sharing:** One of the major advantages of a DBMS is that the same information can be made available to different users.
- **Minimizing Data Redundancy:** In a DBMS, duplication of information or redundancy is, if not eliminated, carefully controlled or reduced i.e. there is no need to repeat the same data repeatedly. Minimizing redundancy significantly reduce the cost of storing information on storage devices.
- **Integrity can be maintained:** Data integrity is maintained by having accurate, consistent, and up-to-date data. Updates and changes to the data only must be made in one place in DBMS ensuring Integrity.
- **Program and File consistency:** Using a DBMS, file formats and programs are standardized. The level of consistency across files and programs makes it easier to manage data when multiple programmers are involved as the same rules and guidelines apply across all types of data.
- **User-friendly:** DBMS makes the data access and manipulation easier for the user. DBMS also reduces the reliance of users on computer experts to meet their data needs.
- **Improved security:** DBMS allows multiple users to access the same data resources in a controlled manner by defining the security constraints. Some sources of information should be protected or secured and only viewed by select individuals. Using passwords, DBMS can be used to restrict data access to only those who should see it. Security will only be improved in a database when appropriate access privileges are allotted to prohibit unauthorized modification of data.
- **Achieving program/data independence:** In a DBMS, data does not reside in applications, but database program and data are independent of each other.

- **Faster Application Development:** In the case of deployment of DBMS, application development becomes fast. The data is already therein databases, application developer must think of only the logic required to retrieve the data in the way a user needs.

Disadvantages of DBMS

- **Cost:** Implementing a DBMS in terms of both system and user-training can be expensive and time-consuming, especially in large enterprises. Training requirements alone can be quite costly.
- **Security:** Even with safeguards in place, it may be possible for some unauthorized users to access the database. If one gets access to database, then it could be an all or nothing proposition.

3.3.4 Networking and Communication Systems

In today's high-speed world, we cannot imagine an information system without an effective and efficient communication system, which is a valuable resource which helps in good management. Telecommunication networks give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees, customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application. All of this offers firm important opportunities to restructure its business processes and to capture highly competitive ground in the marketplace. Through telecommunications, this value may be:

(i) an increase in the efficiency of operations;

(ii) improvements in the effectiveness of management; and

(iii) innovations in the marketplace.

A network is a group of devices connected to each other and a **Computer Network** is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Where atleast one process in one device can send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network.

Network and Communication System: These consist of both physical devices and software that 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. A network links two or more computers to share data or resources such as a printer.

Banking Company, accounting information of various customers could be distributed across various branches but to make Consolidated Balance Sheet at the year-end, it would need networking to access information from all its branches.

- **Resource Sharing:** Data could be stored at a central location and can be shared across different systems. Even resource sharing could be in terms of sharing peripherals like printers, which are normally shared by many systems. For example- In the case of a Core Banking System, Bank data is stored at a Central Data Centre and could be accessed by all branches as well as ATMs.
- **Computational Power:** The computational power of most of the applications would increase drastically through load balancing when the processing is distributed amongst computer systems. For example: processing in an ATM machine in a bank is distributed between ATM machine and the central Computer System in a Bank, thus reducing load on both.
- **Reliability:** Many critical applications should be available 24x7, if such applications are run across different systems which are distributed across network, then the reliability of the applications would be high. For example- In a city, there could be multiple ATM machines so that if one ATM fails, one could withdraw money from another ATM.
- **User communication:** Networks allow users to communicate using e-mail, newsgroups, video conferencing, etc.

Telecommunications may provide these values through the following impacts:

(a) **Time compression:** Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

(b) **Overcoming geographical dispersion:** Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

(c) **Restructuring business relationships:** Telecommunications make it possible to create systems which restructure the interactions of people within a firm as well as a firm's relationships with its customers. Operational efficiency may be raised by eliminating intermediaries from various business processes.

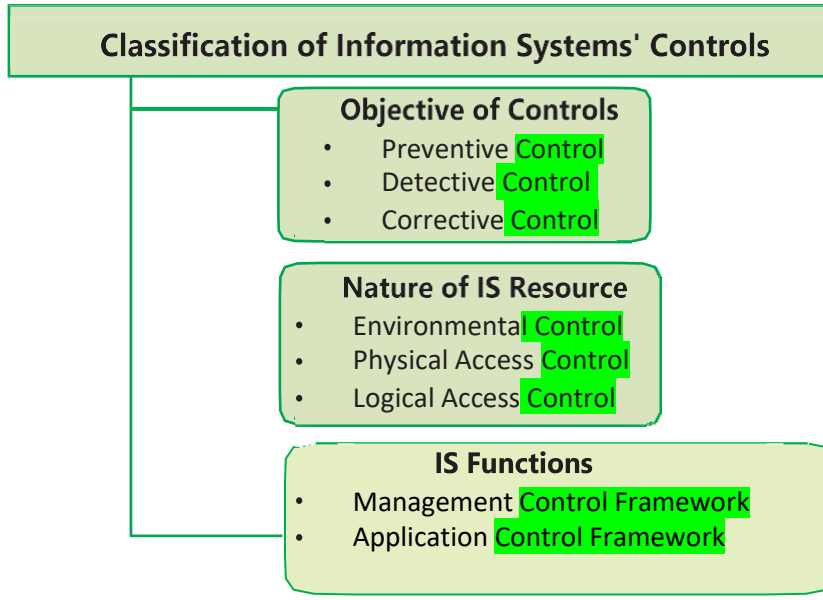


Fig. 3.4.1: Classification of IS Controls

3.4.1 Classification based on "Objective of Controls"

The controls as per the time that they act, relative to a security incident can be classified as under:

(A) Preventive Controls: These controls prevent errors, omissions, or security and malicious incidents from occurring. They are basically proactive in nature. 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 unauthorized people, and complex and dynamic technical controls such as anti-virus software, firewalls, and intrusion prevention systems. Preventive controls can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other.

Example 3.2: Some examples of preventive controls are as follows:

Employing qualified personnel; Segregation of duties; Access control; Vaccination against diseases; Documentation; Prescribing appropriate books for a course; Training and retraining of staff; Authorization of transaction; Validation, edit checks in the application; Firewalls; Anti-virus software (sometimes this act like a corrective control also) etc. and Passwords. The above list contains both of manual and computerized preventive controls.

The main characteristics of Preventive controls are given as follows:

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats;
- Provision of necessary controls for probable threats from materializing.

Example 3.3: The following Table 3.4.1 shows how the purpose of preventive controls is achieved by using manual and computerized controls.

Table 3.4.1: Preventive Controls

Purpose	Manual Control	Computerized Control
Restrict unauthorized entry into the premises.	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restrict unauthorized entry into the software applications.	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

(B) **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. In other words, Detective Controls detect errors or incidents that elude preventive controls. They are basically investigative in nature. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls indicate that a message has been corrupted or the sender's secure identification cannot be authenticated.

The main characteristics of Detective controls are given as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
- An established mechanism to refer the reported unlawful activities to the appropriate person or group, whistle blower mechanism;
- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

Example 3.4: Some examples of Detective Controls are as follows:

Review of payroll reports; Compare transactions on reports to source documents; Monitor actual expenditures against budget; Use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend; Hash totals; Check points in production jobs; Echo control in telecommunications; Duplicate checking of calculations; Past-due accounts report, the Internal Audit functions; Intrusion Detection System; Cash counts and Bank reconciliation and Monitoring expenditures against budgeted amount.

(C) Corrective Controls: It is desirable to correct errors, omissions, or incidents once they have been detected. These controls are reactive in nature. These vary from simple correction of data-entry errors, to identifying and removing unauthorized users or software from systems or networks to recovery from incidents, disruptions, or disasters. Generally, it is most efficient to prevent errors or detect them as close as possible to their source to simplify correction. These corrective processes also should be subject to preventive and detective controls because they represent another opportunity for errors, omissions, or falsification. Corrective controls are designed to reduce the impact or correct an error once it has been detected.

The main characteristics of the corrective controls are as follows:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing Remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying the processing systems to minimize future occurrences of the incidents.

Example 3.5: Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. For example- "Complete changes to IT access lists if individual's role changes" is an example of corrective control. If an accounts clerk is transferred to the sales department as a salesman, his/her access rights to the general ledger and other finance functions should be removed and he/she should be given access only to functions required to perform his sales job.

Some other examples of Corrective Controls are submitting corrective journal entries after discovering an error; a Business Continuity Plan (BCP); Contingency planning; Backup procedure; Rerun procedures; System reboot; Change input value to an application system; and Investigate budget variance and report violations.

3.4.2 Classification based on "Nature of Information System Resources"

These are as follows:

(A) Environmental Controls: These are the controls relating to IT environment such as power air-conditioner, Uninterrupted Power Supply (UPS), smoke detector, fire-extinguishers, dehumidifiers etc. Tables 3.4.2 (A,B,C,D) enlist all the controls against the environmental exposures like Fire, Electrical Exposures, Water Damage, and Pollution damage and others with their corresponding controls respectively.

I. Fire: It is a major threat to the physical security of a computer installation.

Table 3.4.2(A): Controls for Fire Exposure

♦ ***Smoke Detectors: Smoke detectors should be positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).***
♦ ***Norms to reduce Electric Firing: To reduce the risk of electric firing, the location of the computer room should be strategically planned and should not be in the basement or ground floor of a multi-storey building. Less wood and plastic material should be used in computer rooms. To reduce the risk of electric fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room. Fireproof Walls, Floors and Ceilings surrounding the Computer Room and Fire-resistant office materials such as waste baskets, curtains, desks, and cabinets should be used.***
♦ ***Fire Extinguishers: Manual fire extinguishers can be placed at strategic locations. Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon-dioxide based fire extinguishers should be well placed and maintained.***
♦ ***Fire Alarms: Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly***

indicate this. Besides the control panel, master switches may be installed for power and automatic fire suppression system. A gas-based fire suppression system is preferable, however, depending upon the situation, different fire suppression techniques like Dry-pipe sprinkling systems, water-based systems, halon etc., may be used. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.

- ***Regular Inspection and Raising awareness: Regular inspection by Fire Department Officials should be conducted. The procedures to be followed during an emergency should be properly documented. Fire exits should be clearly marked, and all the staff members should know how to use the system in case of emergency.***
- **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency. In all circumstances, saving human life should be given paramount importance.

II. Electrical Exposures: These include risk of damages that may be caused due electrical faults which may occur due to very short pulse of energy in a power line. These include non-availability of electricity, spikes (temporary very high voltages), fluctuations of voltage and other such risk.

Table 3.4.2(B): Controls for Electrical Exposure

- **Electrical Surge Protectors:** The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically built into the Uninterrupted Power System (UPS).
- **Un-interruptible Power System/Generator:** In case of a power failure, the UPS provides the backup by providing electrical power from the battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown.
- **Voltage regulators and circuit breakers:** These protect the hardware from temporary increase or decrease of power.
- **Emergency Power-Off Switch:** When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic

locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

III. Water Damage: Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc.

Table 3.4.2(C): Controls for Water Exposure

- ***Water Detectors: These should be placed under the raised floor, near drain holes and near any unattended equipment storage facilities.***
- ***Strategically locating the computer room: To reduce the risk of flooding, the computer room should not be located in the basement of ground floor of a multi-storey building.***
- Some of the major ways of protecting the installation against water damage are as follows:
  - Wherever possible have waterproof ceilings, walls and floors;
  - Ensure an adequate positive drainage system exists;
  - Install alarms at strategic points within the installation;
  - In flood-prone areas, have the installation above the upper floors but not at the top floor;
  - Water proofing; and
  - Water leakage Alarms.

IV. Pollution Damage and others: The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read / write errors.

Table 3.4.2(D): Controls for Pollution Damage Exposure

- **Power Leads from Two Substations:** Electrical power lines are exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility so that interruption of one power supply does not adversely affect electrical supply.

are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Table 3.4.4 provides the controls for Technical Exposures.

Table 3.4.4: Controls for Technical Exposures

I.	**User Access Management:** This involves the administration within a system for giving individual users the access to the tools they require at the right time. This is an important factor that involves following:
	• **User Registration:** Information about every user is documented. Some questions like why and who is the user granted the access; has the data owner approved the access, and has the user accepted the responsibility? etc. are answered. The de-registration process is also equally important.
	• **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities are to be minimal w.r.t. their job functions. For example, an operator at the order counter shall have direct access to order processing activity of the application system. Similarly, a business analyst could be granted the access to view the report but not modify which would be done by the developer.
	• **User password management:** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords and making them responsible for their password.
	• **Review of user access rights:** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.
II.	**User Responsibilities:** User awareness and responsibility are also important factors discussed below:
	• **Password use:** This includes mandatory use of strong passwords to maintain confidentiality.
	• **Unattended user equipment:** Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password and should not leave it

accessible to others. While leaving the premises from work, care should be taken to always lock the system.

III. **Network Access Control:** Network Access controls refers to the process of managing access for use of network based services like shared resources, access to cloud based services, remote login, network and internet access. The protection can be achieved through the following means:

- **Policy on use of network services:** An enterprise-wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.
- **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks e.g. internet access by employees will be routed through a firewall and proxy.
- **Segregation of networks:** Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service thereby providing a secure remote connection.
- **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.
- **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.
- **Firewall:** A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall that will allow only authorized traffic between the organization and the outside to pass through it. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also as per the organizations network usage policy.

- **Network Encryption:** Network encryption is defined as the process of encrypting data and messages transmitted or communicated over a computer network. Encrypting date means the conversion of data into a secret code for storage in databases and transmission over networks. Two general approaches - Private key and Public key encryption are used for encryption.
- **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits the access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

IV. Operating System Access Control: Operating System (O/S) is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database, and printers. Major tasks of O/S are Job Scheduling; Managing Hardware and Software Resources; Maintaining System Security; Enabling Multiple User Resource Sharing; Handling Interrupts and Maintaining Usage Records. Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'. Hence, protecting operating system access is extremely crucial and can be achieved using following steps.

- **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access as it does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.

- **Access Token:** If the log on attempt is successful, the operating system creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those privileges granted to the user as mentioned in the access control list. If there is a match, the user is granted access.
- **Discretionary Access Control:** The system administrator usually determines who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.
- **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means

to alert the authorities. The design of the duress alarm should be simple enough to be operated under stressful situations.

- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time. For example, no computer access after 8.00 p.m. and before 8.00 a.m. or on a Saturday or Sunday.

V. Application and Monitoring System Access Control: Applications are most common assets that access information. Users invoke the programmes or modules of application to access, process and communicate information. Hence, it is necessary to control the accesses to application. Some of the controls are as follows:

- **Information Access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user can access only to those items, s/he is authorized to access. Controls are implemented on access rights like read, write, delete, and execute to users, and further to ensure that sensitive output is sent only to authorized terminals and locations.
- **Sensitive System isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect/report any unauthorized activities.
- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
- **Monitor System use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events, and alerts that will be monitored. The extent of detail and the frequency of the review

	would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs. • **Clock Synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.
VI.	**Controls when mobile:** In today's organizations, computing facility is not restricted to a certain data center alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security. Theft of data carried on the disk drives of portable computers is a high-risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

3.4.3 Classification based on "Information Systems Functions"

Auditors might choose to factor systems in several different ways. Auditors have found two ways to be especially useful when conducting information systems audits, as discussed below. Fig. 3.4.2 and Fig. 3.4.3 provide overview of The Management Control Framework and Application Control Framework respectively.

A. The Management Control Framework

Managerial functions must be performed to ensure the development, implementation, operation, and maintenance of information systems in a planned and controlled manner in an organization. These functions provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

I. Top Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly, and they meet the strategic business objectives. The management has the responsibility to determine whether the controls that their enterprise system has put in place are sufficient so that the IT activities are adequately controlled. The scope of control here includes framing high-level IT policies, procedures, and standards on a holistic view and in establishing a sound internal controls framework within the organization. The high- level policies establish a framework on which the controls for lower hierarchy of the

enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management. Top management is responsible for preparing a master plan for the information systems function. The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior management must perform are Planning, Organizing, Leading and Controlling.

(a) **Planning –** This includes determining the goals of the information systems function and the means of achieving these goals which could either be a short term or long term one. The steering committee shall comprise of representatives from all areas of the business, and IT personnel that would be responsible for the overall direction of IT. The steering committee should assume overall responsibility for activities of information systems function.

(b) **Organizing –** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during planning function. Unless Top management performs the organizing function properly, the Information systems function is unlikely to be effective and efficient.

(c) **Leading –** This includes the activities like motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives, i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.

(d) **Controlling –** This includes comparing actual performance of the information systems functions with their planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities.

II. Systems Development Management Controls

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities. The activities discussed below deal with system development controls in an IT setup.

(a) ***Problem definition and Feasibility assessment: Information Systems can be developed to help resolve problems or to take advantage of opportunities. All the stakeholders must reach to agreement on the problem and should understand the possible threats associated with possible solutions/systems related to asset safeguarding, data integrity, system effectiveness, and system efficiency. The feasibility assessment is done to obtain a commitment to change and to evaluate whether cost-effective solutions are available to address the problem or opportunity that has been identified. All solutions must be properly and formally authorized to ensure their economic justification and feasibility. This requires that each new solution request to be submitted in written form by stakeholders to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.***

(b) ***Analysis of existing system: Designers need to analyze the existing system that involves two major tasks:***

- ***Studying the existing organizational history, structure, and culture to gain an understanding of the social and task systems in place, the ways these systems are coupled, and the willingness if stakeholders to change.***
- ***Studying the existing product and information flows as the proposed system will be based primarily on current product and information flows. The designers need to understand the strengths and weaknesses of existing product to determine the new system requirements and the extent of change required.***

(c) ***Information Processing System design: This phase involves following activites:***

- ***Elicitation of detailed requirements: Either ask the stakeholders for their requirement in case they are aware about it or discover the requirement through analysis and experimentation in case stakeholders are uncertain about their need.***
- ***Design of data/information flow: The designers shall determine the flow of data/information and transformation points, the frequency and timing of the data and information flows and the extent to which data and information flows will be formalized. Tools such as DFD can be used for this purpose.***

- ***Design of Database and user interface: Design of database involves determining its scope and structure, whereas the design of user interface determines the ways in which users interact with a system.***
- ***Physical design: This involves breaking up the logical design into units which in turn can be decomposed further into implementation units such as programs and modules.***
- ***Design of the hardware/software platform: In case the hardware and software platforms are not available in the organization, the new platforms are required to be designed to support the proposed system.***

(d) Hardware/Software acquisition and procedures development: To purchase the new application system or hardware, a request for a proposal must be prepared, vendor proposals are sought, and final decisions is made based on evaluation. During procedures development, designers specify the activities that users must undertake to support the ongoing operation of the system and to obtain useful output.

(e) Acceptance Testing and Conversion: Acceptance Testing is carried out to identify errors or deficiencies in the system prior to its final release into production use. The conversion phase comprises the activities undertaken to place the new system in operation.

(f) Operation and Maintenance: In this phase, the new system is run as a production system and periodically modified to better meet its objectives. A formal process is required to identify and record the need for changes to a system and to authorize and control the implementation of needed changes. The maintenance activities associated with these systems need to be approved and monitored carefully.

III. Programming Management Controls

Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. Refer Table 3.4.5.

Table 3.4.5: Program Development Life Cycle

Phase	Controls
Planning	This phase estimates the resources required for software development, acquisition, and implementation. The importance and complexity of planning decision can vary based on factors

	such as size of software to be developed and uncertainty relating to user requirement or support technology.
Design	In this, programmers seek to specify the structure and operation of programs that will meet the requirements articulated. Any systematic approach to program design like structured design approach or object-oriented design is adopted. The design of program depends on the type of programming language that has been or will be used to implement the program.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down and Bottom-up approach), a coding strategy (that follows percepts of structured programming) and a documentation strategy to ensure program code is easily readable and understandable.
Testing	Three types of testing can be undertaken in this phase: ♦ **Unit Testing** which focuses on individual program modules; ♦ **Integration Testing** which focuses on groups of program modules; and ♦ **Whole-of-Program Testing** which focuses on whole program to determine whether it meets the requirement. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so that maintenance needs can be identified on a timely basis. Below are three types of maintenance: ♦ **Repair Maintenance –** in which logic errors detected in the system are corrected; ♦ **Adaptive Maintenance –** in which the program is modified to meet changing user requirements; and ♦ **Perfective Maintenance -** in which the program is tuned to decrease the resource consumption and improve processing efficiency.
The **Control** phase that runs in parallel to all other phases during software development or acquisition is to monitor progress against plan and to ensure that software released for production use is authentic, accurate, and complete. Techniques like Work Breakdown Structures (WBS), Gantt Charts and PERT	

(Program Evaluation and Review Technique) Charts can be used to monitor progress against plan. The Control phase has two major purposes:

- Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations.
- Control over software development, acquisition, and implementation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.

IV. Data Resource Management Controls

In organizations, the data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed better; users must be able to share data; data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further, it must be possible to modify data easily if the change is required and the integrity of the data must be preserved.

If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities. Data integrity is defined as maintenance, assurance, accuracy, consistency of data and the control activities that are involved in maintaining it are as under:

(a) ***~~Definition Controls:~~ These controls are placed to ensure that database always corresponds and comply with its definition standards.***

(b) ***Existence/Backup Controls: These controls ensure the existence of the database by establishing backup and recovery procedures. Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases. Various backup strategies like dual recording of data; periodic dumping of data; logging input transactions and changes to the data may be used.***

(c) ***Access Controls: These controls are designed to prevent unauthorized individual from viewing, retrieving, computing, or destroying the entity's***

data. User Access Controls are established through passwords, tokens and biometric controls; and Data Encryption controls are established by keeping the data in database in encrypted form.

(d) ***Update Controls: These controls restrict update of the database to authorized users in two ways either by permitting only addition of data to the database or allowing users to change or delete existing data.***

(e) ***Concurrency Controls: These controls provide solutions, agreed-upon schedules, and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.***

(f) ***Quality Controls: These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.***

V. Security Management Controls

Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure. Assets are secure when the expected losses that will occur over some time, are at an acceptable level. The Environmental Controls, Physical Controls and Logical Access Controls are all security measures against the possible threats. However, despite the controls on place, there could be a possibility that a control might fail. Disasters are events/incidents that are so critical that has capability to hit business continuity of an entity in an irreversible manner.

When disaster strikes, it still must be possible to recover operations and mitigate losses using the controls of last resort - A **Disaster Recovery Plan (DRP)** and **Insurance**.

- DRP deals with how an organization recovers from a disaster and comes back to its normalcy. The plan lays down the policies, guidelines, and procedures for all Information System personnel. A comprehensive DRP comprise four parts – **an Emergency Plan** (actions to be undertaken immediately when a disaster occurs **, a Backup Plan** (specifies the type of backup to be kept, frequency of taking backup, the procedures for making backup etc.), a **Recovery Plan** (to restore full IS capabilities) and a **Test Plan** (to identify deficiencies in the test plan). **Business Continuity Plan** (BCP) as compared

to a DRP mainly deals with carrying on the critical business operations in the event of a disaster so as to ensure minimum impact on the business.

- **Insurance** is a contract, represented by a policy, in which an individual or entity receives financial protection or reimbursement against losses from an insurance company. Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.

VI. Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities so that production application systems can accomplish their work and development staff can design, implement and maintain application systems. Operations management typically perform controls over the functions as discussed below:

(a) Computer Operations: The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available.

(b) Network Operations: Data may be lost or corrupted through component failure. To avoid such situation, the proper functioning of network operations, monitoring the performance of network communication channels, network devices, and network programs and files are required.

(c) Data Preparation and Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from say customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the wellbeing of keyboard operators.

(d) Production Control: This includes the major functions like receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

(e) File Library: This includes the management of not only machine-readable storage media like magnetic tapes, cartridges, and optical disks of an organization but also its fixed storage media.

(f) Documentation and Program Library: This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. There should also

B. The Application Control Framework

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. Any function or activity that works to ensure the processing accuracy of an application can be considered as application control. For example, a counter clerk at a bank is required to perform various business activities as part of his/her job description and assigned responsibilities. S/he can relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives. ***Application System Controls involve ensuring that individual application systems safeguard assets (reducing expected losses), maintain data integrity (ensuring complete, accurate and authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.***

An **Audit Trail** should record all the material events that occur within the boundary subsystem to analyze and search for error or irregularities. **Audit Trail Controls** attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error, and allow system monitoring and tuning. Two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of events within the subsystem.
- An **Operations Audit Trail** to maintain a record of attempted or actual resource consumption associated with each event in the subsystem.

I. Boundary Controls

The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access. The boundary subsystem establishes the interface between the would-be user of a computer system and the computer itself. Major Controls at the Boundary subsystem are as follows:

(a) Cryptographic Controls: These are designed to protect the privacy of data and prevent unauthorized modification of data by scrambling data. These deal with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access

the respective system resource or file. A cryptographic technique transforms (encrypts) data (known as cleartext) into cryptograms (known as ciphertext) and its strength depends on the time and cost to decipher the ciphertext by a cryptanalyst. Three techniques of cryptography that are used are **Transposition** (permute the order of characters within a set of data), **Substitution** (replace text with a key-text) and **Product Ciphers** (combination of transposition and substitution).

(b) ***Access Controls: These controls restrict the use of computer system resources to authorized users, limit the actions authorized users can take with these resources and ensure that users obtain only authentic computer system resources. The access control mechanism involves three steps: Identification, Authentication and Authorization.***

- ***User's identification is done by user itself by providing his/her unique user id allotted to him/her or account number.***
- ***Authentication mechanism is used for proving the identity with the help of a password which may involve personal characteristics like name, birth date, employee code, designation or a combination of two or more of these. Biometric identification including thumb or finger impression, eye retina etc. and information stored in identification cards can also be used in an authentication process.***
- ***Authorization refers to the set of actions allowed to a user once authentication is done successfully. For example – Read, Write, Print, etc. permissions allowed to an individual user.***

An access control mechanism is used to enforce an access control policy which are mainly of two types - Discretionary Access Control and Mandatory Access Control policies (already discussed in Chapter 2).

(c) ***Personal Identification Numbers (PIN): As already discussed before, we may recall that it is a form of remembered information used to authenticate users like verification of customers in electronic fund transfer systems. PIN is like a password assigned to a user by an institution, a random number stored in its database independent to a user identification details. Several phases of the life cycle of PINs include the steps that are (a) Generation of the PIN; (b) Issuance and delivery of PIN to users; (c) Validation of the PIN upon entry at the terminal device; (d) Transmission of the PIN across communication lines; (e) Processing***

of the PIN; (f) Storage of the PIN; (g) Change of the PIN; (h) Replacement of the PIN; and (i) Termination of the PIN.

A PIN may be exposed to vulnerabilities at any stage of the life cycle of PIN and therefore, controls need to be put in place and working to reduce exposures to an acceptable level.

(d) ***Digital Signatures: Establishing the authenticity of persons and preventing the denial of message or contracts are critical requirements when data is exchanged in electronic form. A counterpart known as Digital Signature (a string of 0's and 1's) is used as an analog signature for such e-documents. Digital Signatures are not constant like analog signatures – they vary across messages and cannot be forged.***

(e) ***Plastic Cards: We may recall that while PIN and Digital Signatures are used for authentication purposes, plastic cards are used primarily for identification purpose. This includes the phases namely - application for a card, preparation of the card, issue of the card, use of the card and card return or card termination.***

(f) **Audit Trail Controls:** This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. The events associated with both types of audit trail control are given below in Table 3.4.6:

Table 3.4.6: Audit Trail Controls - Boundary Control

Accounting Audit Trail	Operations Audit Trail
All material application-oriented events occurring within the boundary subsystem should be recorded that may include the data related to identity of the would-be user of system; authentication information supplied; resources requested/provided or denied; terminal Identifier and Start/Finish Time; number of Sign-on attempts; & Action privileges allowed/denied.	This includes the details like resource usage from log-on to log-out time and log of resource consumption.

II. Input Controls

Data that is presented to an application as input data must be validated for authorization, reasonableness, completeness, accuracy, and integrity. These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important and critical since substantial time is spent on input of data, involve human intervention

and are, therefore error and fraud prone. These are of following types as shown in the Fig. 3.4.4:

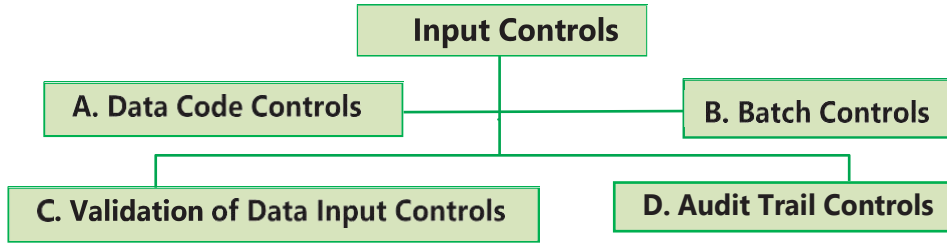


Fig. 3.4.4: Classification of Input Controls

In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example- an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment. To control against this type of exposure, an organization must implement control procedures over source documents to account for each document.

(a) Data Code Controls: These controls are aimed at reducing the user error during data feeding. Two types of errors - **Transcription** and **Transposition** errors can corrupt a data code and cause processing errors. Any of these errors can cause serious problems in data processing if they go undetected. These simple errors can severely disrupt operations.

- **Transcription Errors:** It is a special type of data entry error that is commonly made by human operators or by Optical Character Recognition (OCR) programs. These can be **Addition errors** (when an extra digit is added to the code); **Truncation Errors** (when a digit is removed from the code) and **Substitution Errors** (replacement of a digit in a code with another).
- **Transposition Errors:** It is a simple error of data entry that occurs when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed.

(b) **Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercises over the batch to prevent or detect errors or irregularities. To identify errors or irregularities in either a physical or logical batch, three types of control totals are as follows:

- **Financial Totals:** Grand totals calculated for each field containing monetary amounts. For example - the total salary paid to employees of an organization can be totaled using DA, TA, house allowance, medical and PF etc.
- **Hash Totals:** Grand totals calculated for any code on a document in the batch, e.g., the source document serial numbers can be totaled.
- **Document/Record Counts:** Grand totals for number of documents / record in batch.

(c) **Validation of Data Input Control:** Input validation controls are intended to detect errors in the transaction data before the data are processed. These errors need to be corrected and if not corrected, the same should be written immediately to an error file. Some of these controls include the following:

- **Field check:** It involves programmed procedures that examine the characters of the data in the field. This includes the checks like **Limit Check** (against predefined limits), **Picture Checks** (against entry into processing of incorrect/invalid characters), **Valid check codes** (against predetermined transactions codes, tables) etc.
- **Record Check:** This includes the **reasonableness** check of whether the value specified in a field is reasonable for that particular field; **Valid sign** to determine which sign is valid for a numeric field and **Sequence Check** to follow a required order matching with logical records etc.
- **Batch Check:** This includes the checks like the **transaction type** if all input records in a batch are of particular type; **sequence check** if input records are in a particular order or not etc.
- **File Check:** This includes file's version usage; internal and external labeling; data file security; file updating and maintenance authorization etc.

(d) **Audit Trail 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 (Refer Table 3.4.7).

Table 3.4.7: Audit Trail Controls - Input Controls

Accounting Audit Trail	Operations Audit Trail
This must record the origin, contents, and timing of transaction entered into application system, thus involving the details regarding the identity of the person (organization) who was the source of the data and 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.	Some of the data that might be collected include 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 different input devices like light pen or mouse.

III. Communication Controls

These discuss exposures in the communication subsystem, controls over physical components, communication line errors, flows and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, and audit trail controls. Some communication controls are as follows:

(a) ***Physical Component Controls:*** ***In the communications subsystem, the physical components shall have characteristics that make them reliable and incorporate features and controls that mitigate the possible effects of exposures. Major physical components that affect the reliability of communication subsystem are Transmission media, Communication lines, Modem, Port protection devices, Multiplexers, and Concentrators etc.***

(b) **Line Error Controls:** Whenever data is transmitted over a communication line, it can be received in error because of attenuation, distortion, or noise that occurs on the line. These errors must be detected and corrected.

(c) **Flow Controls:** Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can be sent, receive, and process data. For example- data transmission between mainframe and microcomputers may become erroneous because of difference in their speed and storage capacity. ***Flow controls will be used therefore to prevent the mainframe flooding the microcomputer and as a result, data being lost.***

(d) **Link Controls:** In Wide Area Network (WAN), line error control and flow control are important functions in the component that manages the link between two nodes in a network. The way these link-management components operate is specified via a protocol.

(e) ***Topological Controls: A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. The network must be available for use at any one time by a given number of users that may require alternative hardware, software, or routing of messages.***

(f) **Channel Access Controls:** Two different nodes in a network can compete to use a communication channel simultaneously, leading to the possibility of contention for the channel existing. Therefore, some type of channel access control techniques like **polling method** (defining an order in which a node can gain access to a channel capacity) or **contention method** (nodes in network must compete with each other to gain access to a channel) must be used.

(g) ***Controls over Subversive threats: Firstly, the physical barriers are needed to be established to the data traversing into the subsystem. Secondly, in case the intruder has somehow gained access to the data, the data needs to be rendered useless when access occurs.***

(h) ***Internetworking Controls: Different internetworking devices like bridge, router, gateways are used to establish connectivity between homogeneous or heterogeneous networks. Therefore, several control functions in terms of access control mechanisms, security and reliability of the networks are required to be established.***

(i) Audit Trail Controls: This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message. Few examples of data item that might be kept in both types of audit trail is shown in Table 3.4.8.

Table 3.4.8: Audit Trail Controls - Communication Controls

Accounting Audit Trail	Operations Audit Trail
This includes collection of the data like unique identifier of the source, destination and each node 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 and received by the sink node; time and date at which node in the network was traversed by the message; message sequence number; and the image of the message received at each node traversed in the network.	This includes the details like 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.

IV. Processing Controls

The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements. Some of these controls are as follows:

(a) Processor Controls: Table 3.4.9 enlists the Controls to reduce expected losses from errors and irregularities associated with Central processors.

Table 3.4.9: Processor Controls

Control	Explanation
Error Detection and Correction	Occasionally, processors might malfunction because of design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. The failure might be transient (that disappears after a short period), intermittent (that reoccurs periodically), or permanent (that does not correct with time). For the transient and intermittent errors, re-tries and re-execution might be successful, whereas for permanent errors, the processor must halt and report error.

Multiple Execution States	It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities, such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes.
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might reconfigure itself to isolate the failed processor.

(b) **Real Memory Controls:** This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor. Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

(c) **Virtual Memory Controls:** Virtual Memory exists when the addressable storage space is larger than the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses. When an executing program references virtual memory addresses, the mechanism then translates these addresses into real memory addresses.

(d) **Application Software Controls:** These perform validation checks to identify errors during processing of data. These are required to ensure both the completeness and the accuracy of data being processed. Normally, the processing controls are enforced through database management system that stores the data. However, adequate controls should be enforced through the front-end application system also to have consistency in the control process.

(e) **Audit Trail Controls:** This 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. Table 3.4.10 shows the Audit Trail Controls of Processing Controls.

Table 3.4.10: Audit Trail Controls - Processing Controls

Accounting Audit Trail	Operations Audit Trail
This includes the data items like- to trace and replicate the processing performed on a data item that enters into the processing subsystem, 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 and to check whether audit log entries recorded the changes made in the data items at any time including who made them.	This includes a comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used and comprehensive log on software consumption – compilers, subroutine libraries, file management facilities and communication software used.

V. Database Controls

These controls are used within an application software to maintain the integrity of data, to prevent integrity violations when multiple programs have concurrent access to data, and the ways in which data privacy can be preserved within the database subsystem.

(a) Access Controls: These controls in database subsystem seek to prevent unauthorized access to and use of the data. A security policy has to be specified followed by choosing an access control mechanism that will enforce the policy chosen. If database is replicated, the same access control rules must be enforced by access control mechanism at each site.

(b) Integrity Controls: These are required to ensure that the accuracy, completeness, and uniqueness of instances used within the data or conceptual modeling are maintained. Integrity Constraints are established to specify the type of relationship and consistency among rows (tuple) in relationship.

(c) Application Software Controls: When application software acts as an interface to interact between the user and the database, the DBMS

depends on application software to pass across a correct sequence of commands and update parameters so that appropriate actions can be taken when certain types of exception condition arise. This is achieved through Update Controls that ensure that changes to the database reflect changes to the real-world entities and associations between entities that data in the database is supposed to represent and Report Controls that identify errors or irregularities that may have occurred when the database has been updated.

(d) ***Concurrency Controls: These are required to address the situation that arises either due to simultaneous access to the same database or due to deadlock.***

(e) ***Cryptographic Controls: (Already discussed under Boundary Controls) These controls can be well used for protecting the integrity of data stored in the database using block encryption.***

(f) ***File Handling Controls: These controls are used to prevent accidental destruction of data contained on a storage medium. These are exercised by hardware, software, and the operators or users who load/unload storage media.***

(g) **Audit Trail Controls:** The audit trail maintains the chronology of events that occur either to the database definition or the database itself as shown in Table 3.4.11.

Table 3.4.11: Audit Trail Controls - Database Controls

Accounting Audit Trail	Operations Audit Trail
This includes the data items 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, and to not only test the stated input, calculation, and output rules for data integrity; but also should assess the efficacy of the rules themselves.	This maintains a chronology of resource consumption events that affects the database definition or the database.

VI. Output Controls

These controls ensure that the data delivered to users will be presented, formatted, and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media. Various Output Controls are as follows:

(a) ***Inference Controls: These are used to prevent compromise of statistical databases from which users can obtain only aggregate statistics rather than the values of individual data items. These are restriction controls which limit the set of responses provided to users to try to protect the confidentiality of data about persons in the database.***

(b) ***Batch Output Production and Distribution Controls: Batch output in the form of tables, graphs or images etc. is produced at some operations facility and distributed to users of the output. This includes several controls like Report program execution Controls to ensure that only authorized users are permitted to execute batch report programs and these events are logged and monitored; Spooling file Controls so that the user(s) can continue working while a queue of documents waiting to be printed on a particular printer to ensure that the waiting files to get printed shall not be subject to unauthorized modifications; Printing Controls to ensure that output is made on the correct printer, and unauthorized disclosure of printed information does not take place; Report collection Controls to ensure that report is collected immediately and secured to avoid unauthorized disclosure and data leakage; User/Client service Review Controls to ensure user should obtain higher quality output and detection of errors or irregularities in output; Report distribution Controls ensuring that the time gap between generation and distribution of reports is reduced, and a log is maintained for reports that were generated and to whom these were distributed; User output Controls to be in place to ensure that users review output on a timely basis; Storage Controls to ensure proper perseverance of output in an ideal environment, secured storage of output and appropriate inventory controls over the stored output and Retention and Destruction Controls in terms of deciding the time duration for which the output shall be retained and then destroyed when not required.***

(c) ***Batch Report Design Controls: Batch report design features should comply with the control procedures laid down for them during the output process. The information incorporated in a well-designed batch report***

shall facilitate its flow though the output process and execution of controls.

(d) ***Online output production and Distribution Controls: It deals with the controls to be considered at various phases like establishing the output at the source, distributing, communicating, receiving, viewing, retaining and destructing the output. Source controls ensure that output which can be generated or accessed online is authorized, complete and timely; Distribution Controls to prevent unauthorized copying of online output when it was distributed to a terminal; Communication Controls to reduce exposures from attacks during transmission; Receipt Controls to evaluate whether the output should be accepted or rejected; Review Controls to ensure timely action of intended recipients on the output; Disposition Controls to educate employees the actions that can be taken on the online output they receive; and Retention Controls to evaluate for how long the output is to be retained and Deletion Controls to delete the output once expired.***

(e) **Audit Trail 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. The data items that need to be considered are provided in Table 3.4.12.

Table 3.4.12: Audit Trail Controls - Output Controls

Accounting Audit Trail	Operations Audit Trail
This includes what output was assimilated for presentation to the users; what output was then presented to the users; who received the output; when the output was received; and what actions were subsequently taken with the output.	This maintains the record of resources consumed by components in the output subsystem to assimilate, produce, distribute, use, store and dispose of various types of output like graphs, images etc., to record data that enables print times, response times and display rates for output to be determined and to manage the information that enables the organization to improve the timelines of output production and reduce the number of resources consumed in producing output.

3.5.3 Audit Trail

We may recall that 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. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

(i) Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact, detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished or attempted and failed.
- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(ii) **Implementing an Audit Trail:** The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs provide a valuable evidences to auditors in assessing both the adequacies of controls in place and the need for additional controls. Audit logs, however, can generate data in overwhelming detail, and therefore, at times, important information can easily get lost among the superfluous detail of daily operations. Thus, poorly designed logs can be dysfunctional.

3.6 AUDITING OF INFORMATION SYSTEMS CONTROLS

3.6.1 Auditing Environmental Controls

Related aspects are given as follows:

(a) **Role of IS Auditor in auditing Environmental 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 environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks.

(b) **Audit of Environmental Controls:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. Auditing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective. Auditing environmental controls requires attention to these and other factors and activities, including:

- **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.
- **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. S/he should examine maintenance records to see how frequently

these components are maintained and if this is done by qualified personnel.

- **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine, if HVAC systems are providing adequate temperature and humidity levels, and if they are monitored. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.
- **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. S/he should determine how frequently these are tested and if these are monitored.
- **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if these are tested. S/he should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills.
- **Cleanliness:** The IS auditor should examine data centers to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

3.6.2 Auditing Physical Security Controls

(a) Role of IS Auditor in auditing Physical Access Controls: Auditing 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 activities:

- **Risk Assessment:** The auditor must satisfy him/herself 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.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

3.6.4 Auditing The Management Control Framework

The auditor's primary objective in examining the management control framework for the information system function is to evaluate whether management manages well. If high-quality management controls are not in place and working reliably; Application Controls are unlikely to be effective.

Though there are many concerns, however, some key areas that auditors should pay attention to while evaluating management controls at each level in an organization are provided below:

I. Auditing Top Management Controls

The major activities that senior management must perform are – **Planning**, **Organizing**, **Leading** and **Controlling**. The role of auditor at each activity is discussed below:

- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.
- **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources.
- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff.
- **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. 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.

II. Auditing Systems Development Management Controls

- Auditors can conduct following three types of reviews/audits of the systems development process as discussed in the Table 3.6.1:

Table 3.6.1: Types of Audit during System Development Process

Concurrent Audit	As a member of the system development team, the auditors need to assist the team in improving the quality of systems development for the specific system they are building and implementing. They shall ensure that needed controls are built into the system to produce high-quality systems.
Post - implement ation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating the current status of the system in terms of attaining asset safeguarding, data integrity, system effectiveness and system efficiency objectives so that the decision on whether the system needs to be scrapped, continued, or modified in some way can be taken.
General Audit	Auditors evaluate the quality of overall systems development process. This review allows them to make judgments on the likely quality of individual application systems developed by the system development management subsystem, the control risk associated with this subsystem, and to determine whether the extent of substantive testing needed to form an audit opinion about management's assertions relating to the systems effectiveness and efficiency, can be reduced or not. An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. Internal auditors generally participate in the development of material application systems or undertake post-implementation review of the system.

III. Auditing Programming Management Controls

Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are provided in Table 3.6.2.

Table 3.6.2: Auditing Programming Management Controls

Phase	Key Areas
Planning	♦ They should evaluate whether nature of and extent of planning are appropriate to different types of software that are developed or acquired.

Operation and Maintenance	♦ Auditors need to ensure effective and timely reporting of maintenance needs that occur so that maintenance is carried out in a well-controlled manner. ♦ Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

IV. Auditing Data Resource Management Controls

- ♦ Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.
- ♦ Auditors might employ test data to evaluate whether access controls and update controls are working.
- ♦ ***Auditors might interview the Data Administrator (DA) and Database Administrator (DBA) to determine the procedures used by them to monitor the database environment.***
- ♦ ***Auditors need to assess how well the DA and DBA carry out the functions of database definition, creation, redefinition, and retirement.***

V. Auditing Security Management Controls

- ♦ Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- ♦ ***Auditors need to evaluate the performance of BCP controls. The BCP controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan and its related business requirements to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption .***
- ♦ Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place or not; and
- ♦ Auditors check whether the organizations have opted for an appropriate insurance plan or not.

VI. Auditing Operations Management Controls

- ♦ Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

- Auditors can use interviews, observations, and review of documentation to evaluate -
  - the activities of documentation librarians;
  - how well operations management undertakes the capacity planning ad performance monitoring function;
  - the reliability of outsourcing vendor controls;
  - whether operations management is monitoring compliance with the outsourcing contract; and
  - Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

VII. Auditing Quality Assurance Management Controls

- Auditors might use interviews, observations, and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
- Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
- Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

3.6.5 Auditing The Application Control Framework

Based on the evaluation of management controls over the IS functions in an organization, auditors might decide to evaluate application system further. In case the external auditors have evaluated the reliability of management controls, the next step is to determine the adequacy of application controls. From various concerns that an auditor might have while auditing the application controls over the IS functions, some key areas that they should pay attention to while evaluating application controls at each level in an organization are provided below:

I. Auditing Boundary Controls

- ***Auditors need to determine how well the safeguard assets are used and preserve data integrity.***

- ***For any application system in particular, auditors need to determine whether the access control mechanism implemented in that system is sufficient or not.***
- ***Auditors need to ensure that careful control must be exercised over maintenance activities, in case of hardware failure.***
- ***Auditors need to address three aspects to assess cryptographic key management -***
  - ***How keys will be generated?***
  - ***How they will be disributed to users?***
  - ***How they will be installed in cryptographic facilities?***
- ***Auditors need to understand which approach has been used to implement access control so that they can predict the likely problems they will encounter in the application systems they are evaluating.***

II. Auditing Input Controls

- ***Auditors must understand the fundamentals of good source document design so as to analyze what and how the data will be captured and by whom, how the data will be prepared and entered into the computer systems and how the document will be handled, stored and filed.***
- ***Auditors must be able to examine the data-entry screens used in an application system and to come to judgement on the frequency with which input errors are likely to be made and the extent to which the screen design enhances or undermines effectiveness and efficiency.***
- ***Auditors must evaluate the quality of the coding systems used in application system to determine their likely impact in the data integrity, effectiveness, and efficiency objectives.***
- ***Auditors need to comprehend various approaches used to enter data into an application system and their relative strengths and weaknesses.***
- ***Auditors need to check whether input files are stored securely and backup copies of it are maintained at an offsite location so that recovery remains unaffected in case system's master files are destroyed or corrupted.***

III. Auditing Communication Controls

- ***Auditors shall adopt a structured approach to examine and evaluate various controls in the communication subsystem.***

- ***Auditors need to collect enough evidence to establish a level of assurance that data transmission between two nodes in a wide area network is being accurate and complete.***
- ***Auditors need to look whether adequate network backup and recovery controls are practiced regularly or not. These controls may include automatic line speed adjustments by modems based on different noise-levels, choice of network topology, alternative routes between sender and receiver etc., to strengthen network reliability.***
- ***Auditors must assess the implementation of encryption controls to ensure the protection of privacy of sensitive data.***
- ***Auditors must assess the topological controls to review the logical arrangement of various nodes and their connectivity using various internetworking devices in a network.***

IV. Auditing Processing Controls

- ***Auditors should determine whether user processes are able to control unauthorized activities like gaining access to sensitive data.***
- ***Auditors should evaluate whether the common programming errors that can result in incomplete or inaccurate processing of data has been taken care or not.***
- ***Auditors should assess the performance of validation controls to check for any data processing errors.***
- ***Auditors need to check for the checkpoint and restart controls that enable the system to recover itself from the point of failure. The restart facilities need to be implemented well so that restart of the program is from the point the processing has been accurate and complete rather than from the scratch.***

V. Auditing Database Controls

- ***Auditors should check for the mechanism if a damaged or destroyed database can be restored in an authentic, accurate, complete, and timely way.***
- ***Auditors should comprehend backup and recovery strategies for restoration of damaged or destroyed database in the event of failure that could be because of application program error, system software error, hardware failure, procedural error, and environmental failure.***

- ***Auditors shall evaluate whether the privacy of data is protected during all backup and recovery activities.***
- ***Auditors should check for proper documentation and implementation of the decisions made on the maintenance of the private and public keys used under cryptographic controls.***
- ***Auditors should address their concerns regarding the maintenance of data integrity and the ways in which files must be processed to prevent integrity violations.***

VI. Auditing Output Controls

- ***Auditors should determine what report programs are sensitive, who all are authorized to access them and that only the authorized persons are able to execute them.***
- ***Auditors should review that the action privileges that are assigned to authorized users are appropriate to their job requirement or not.***
- ***Auditors must evaluate how well the client organizations are provided controls in terms of alteration of the content of printer file, number of printed copies etc.***
- ***Auditors should determine whether the report collection, distribution and printing controls are well executed in an organization or not.***

3.7 DATA RELATED CONCEPTS

3.7.1 Database Models

Databases can be organized in many ways, and thus take many forms. A Database Model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated. Let's now look at the database model hierarchy given as under:

- **Database:** This is a collection of Files/Tables.
- **File or Table:** This is a collection of Records, also referred as Entity.
- **Record:** This is a collection of Fields.
- **Field:** This is a collection of Characters, defining a relevant attribute of Table instance.
- **Characters:** These are a collection of Bits.

This hierarchy is shown in the Fig. 3.7.1:

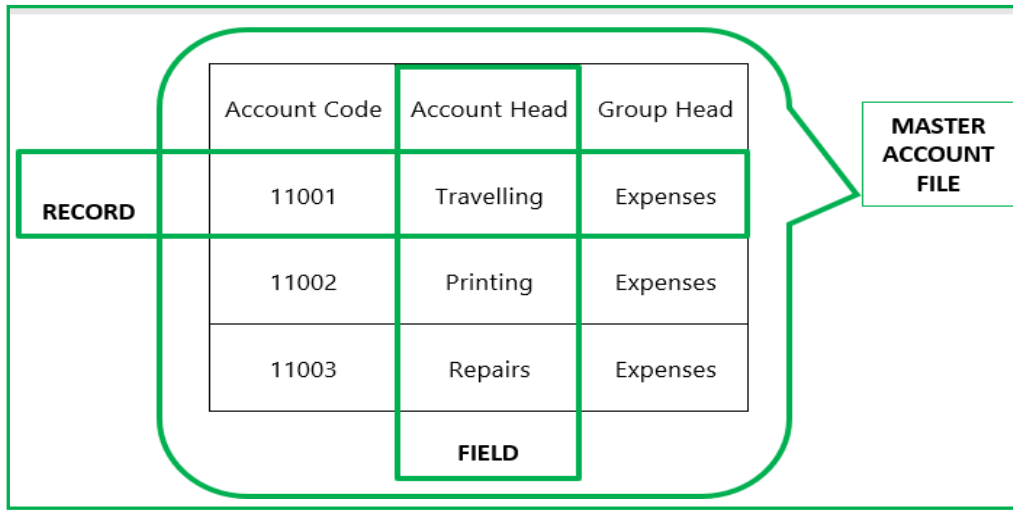


Fig. 3.7.1: Hierarchy of Data

Some prominent database models are provided in the Table 3.7.1 below.

Table 3.7.1: Database Models

Hierarchical Database Model	Network Database Model	Relational Database Model	Object Oriented Data Base Model(OODBM)
Records/Nodes are logically organized into a hierarchy of relationships in an inverted tree pattern.	This structure views all records in sets; wherein each set is composed of an owner record and one or more member records.	This allows collection of records in a tabular structure where each record contains some fields defining the nature of the data stored in that table. A record is one instance of a set of fields in a table. Main terms used in this model are **Relation** defined as a table with columns and rows; Named columns of the table as **Attributes**	It is based on the concept that the world can be modeled in terms of objects and their interactions. This provides a mechanism to store complex data such as images, audio and video, etc.

		(fields) and **Domains** as set of values the attributes can take.	
The top parent record that "own" other records is called **Parent Record/ Root Record** which may have one or more child records, but no child record may have more than one parent record.	The network model implements one-to-one, one-to-many, many-to-one and the many-to-many relationship types.	All relations adhere to some basic rules - First, the ordering of columns is immaterial in a table. Second, there cannot be identical record in a table. And third, each record will contain a single value for each of its attributes.	In this, the data is modeled and created as objects. It combines different aspects of object-oriented programming language into a DBMS like complex data types, multi valued attributes (e.g. address field can have many values like house number, location, zip code etc.).
Each node is related to the others in a parent-child relationship. Thus, the hierarchical data structure implements one-to-one and one-to-many relationships. Refer Example 3.6.	The network model can represent redundancy in data more efficiently than in the hierarchical model. Refer Example 3.7.	A relational database contains multiple tables, with all the tables connected by one or more common fields. For each table, one of the fields is identified as a **Primary Key**, which is the unique identifier for each record in the table. If the primary key of one table is used in another table to access the former, it is called **Foreign Key**. Popular examples of relational	OODBMS helps programmers make objects which are an independently functioning application or program, assigned with a specific task or role to perform. Refer Example 3.9.

		databases are Microsoft Access, MySQL, and Oracle. Refer Example 3.8.	

Example 3.6: Consider an equipment database shown in Fig. 3.7.2 that has building records, room records, equipment records, and repair records. The database

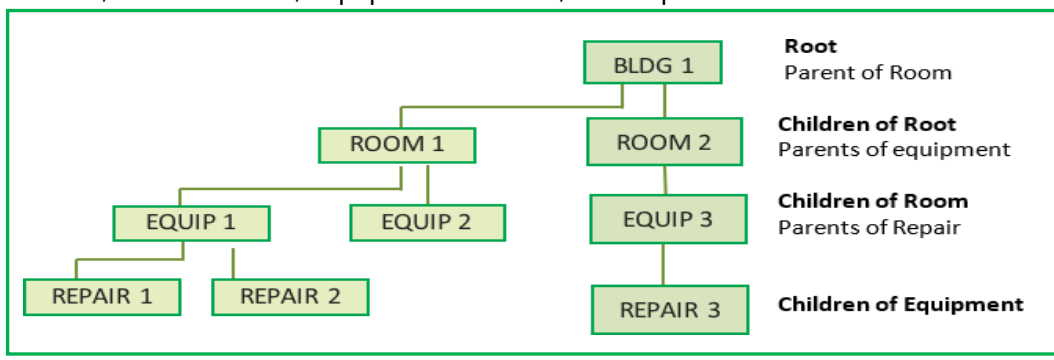


Fig. 3.7.2: Hierarchical Database Model

structure reflects the fact that repairs are made to equipment located in rooms that are part of buildings. Entrance to this hierarchy by the DBMS is made through the root record i.e., Building. The building records are the root to any sequence of room, equipment, and repair records. Room records are the parents of equipment records and at the same time, Room records are also children of the parent record, Building. There can be many levels of node records in a database.

Example 3.7: Suppose that in our database, it is decided to have these records - Repair Vendor (RV) records for the companies that repair the equipment, Equipment Records (ER) for the various machines we have, and Repair Invoice (RI) records for the repair bills for the equipment. Suppose four Repair Vendors have completed repairs on equipment items 1,2,3,4,5,6,7 and 8. These records might be logically organized into the sets shown in Fig. 3.7.3. Notice these relationships:

- **One-to-One relationship:** RV-1 record is the owner of the RI-1 record.
- **One-to-Many relationship:** RV-2 record is owner of the RI-2 and RI-3 records.
- **Many-to-Many relationship:** Many ER can be owned by many RI records. RV-3 record is the owner of RI-4 and RI-5 records, and the ER-7 is owned by both the RI-5 and RI-6 records because it was fixed twice by different vendors.
- **Many-to-One relationship**: Equipments 7 and 8 are owned by RI-6 because the repair to both machines were listed on the same invoice by RV-4.

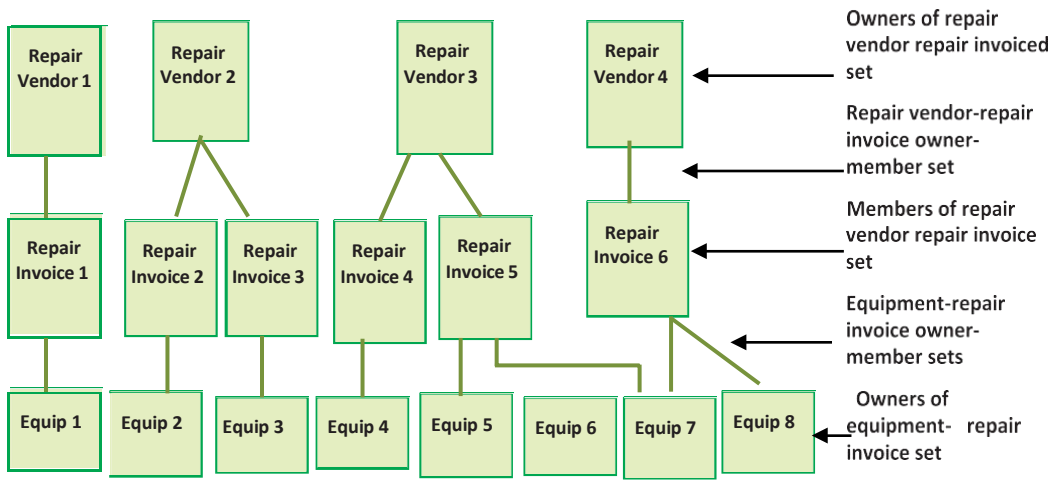


Fig. 3.7.3: Example of Network Database Model

- Equipment 6 record does not own any record now because it is not required to be fixed yet.

Example 3.8: A company manufactures black and blue ball pens and stores its data using relational database wherein the data is stored in table structures defined below in table 3.7.2.

Table 3.7.2: Description of Example 3.8

Table 1: Product_table that contains the detail of all products. Each product is assigned a unique code represented as Prd_code in the table.

Prd_code	Description	Price
P001	Black pen	` 50
P002	Blue pen	` 70

Table 2: Invoice_table has the description of invoices. Invoice table has Invoice_code, Quantity(Qty) and total amount (Total_Amt) with respect to products sold. Each invoice has unique number as Invoice_code.

Prd_code	Invoice_code	Qty	Total_Amt
P001	2304	10	` 500
P002	2306	20	` 1400

Both tables Product_table and Invoice_table have a relationship through the common attribute - Prd_code. Prd_code is the Primary (unique) key in Product_table and it acts as key of relationship (foreign key) with Invoice_table. For a specific Invoice_code, the description of product and price can be retrieved from Product_table.

Example 3.9: Refer the Fig. 3.7.4. The light rectangle indicates that 'Engineer' is an object possessing attributes like 'date of birth', 'address', etc. which is interacting with another object known as 'civil jobs'. When a civil job is executed commenced, it updates the 'current job' attribute of the 'Engineer' object, because 'civil job' sends a message to the latter object.

Objects can be organized by first identifying them as a member of a class/subclass. Different objects of a particular class should possess at least one common attribute. The dark rectangles indicate 'Engineer' as a class and 'Civil Engineer' and 'Architect' as both subclasses of 'Engineer'. These subclasses possess all the attributes of 'Engineer' over and above each possessing at least one attribute not possessed by 'Engineer'. The line intersecting particular object classes represents the class of structure.

Secondly, objects can be identified as a component of some other object. 'Engineer' is components of a 'Civil Job Team' which may have one to more than one number of member(s). An 'Engineer' may not be a member of the 'Civil Job Team' and may not be a member of more than one team. The dotted line intersecting particular object classes represents the part of structure. Apart from possessing attributes, objects as well as possess methods or services that are responsible for changing their states. Like the service 'Experience' as a Civil Engineer or Architect for the object 'Engineer' calculates how much experience the engineers of these particular two subclasses have as professionals.

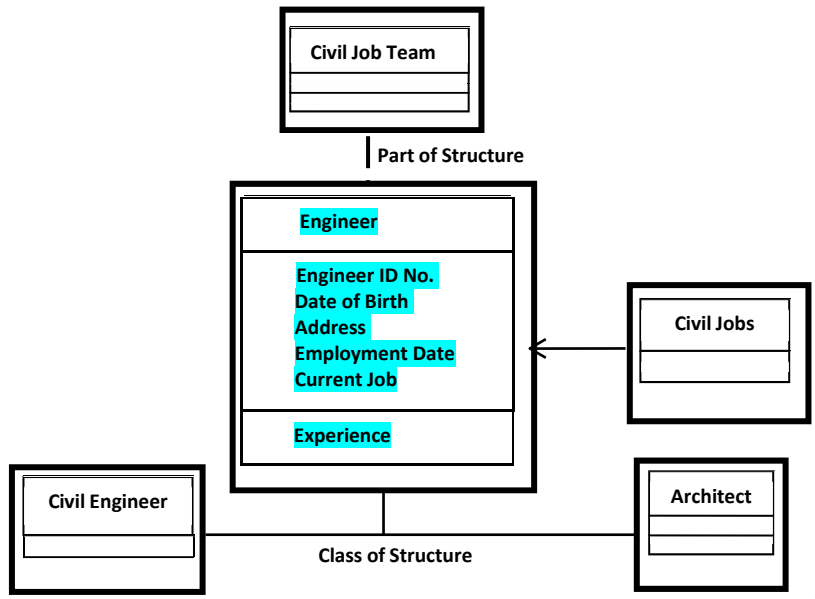


Fig. 3.7.4: An object-oriented database design

3.7.2 Big Data

A new buzzword that has been capturing the attention of businesses lately is Big Data. The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them. For example, Flipkart must process over millions of customer transactions every hour during the Billion Day Sale. Storing and analyzing that much data is beyond the power of traditional database-management tools. Understanding the best tools and techniques to manage and analyze these large data sets is a problem that governments and businesses alike are trying to solve. This is an interesting space to explore from a career perspective since everything is nothing more than data. In fact, we are nothing more than data points in databases on various companies.

Some examples of industries that use big data analytics include the hospitality industry, healthcare companies, public service agencies, and retail businesses.

Benefits of Big Data Processing are as follows:

(a) Ability to process Big Data brings in multiple benefits, such as-

- Businesses can utilize outside intelligence while taking decisions.
- Access to social data from search engines and sites like Facebook, Twitter is enabling organizations to fine tune their business strategies.
- Early identification of risk to the products/services, if any.

(b) Improved customer service

- Traditional customer feedback systems are getting replaced by new systems designed with Big Data technologies. In these new systems, Big Data and natural language processing technologies are being used to read and evaluate consumer responses.

(c) Better operational efficiency

- Integration of Big Data technologies and data warehouse helps an organization to offload infrequently accessed data, this leading to better operational efficiency.

3.7.3 Data Warehouse

As organizations have begun to utilize databases as the centre piece of their operations, the need to fully understand and leverage the data they are collecting has become more and more apparent. However, directly analyzing the data that is needed for day-to-day operations is not a good idea; we do not want to tax the

operations of the company more than we need to. Further, organizations also want to analyze data in a historical sense: How does the data we have today compare with the same set of data of last month, or last year? From these needs arose the concept of the data warehouse. The process of extracting data from source systems and bringing it into the data warehouse is commonly called **ETL**, which stands for **Extraction, Transformation**, and **Loading**. The process is described below and shown in the Fig. 3.7.5:

- In the first stage, the data is **Extracted** from one or more of the organization's databases. This stage involves extracting the data from various sources such as ERP systems used, databases, flat files including plain text files, Excel spreadsheet etc.
- In the second stage, the data so extracted is placed in a temporary area called **Staging Area** where it is **Transformed** like cleansing, sorting, filtering etc. of the data as per the information requirements.
- The final stage involves the **Loading** of the transformed data into a data warehouse which itself is another database for storage and analysis.
- The information loaded on to the data warehouse could further be used by different data marts which are nothing but databases pertaining to specific departmental functions like Sales, Finance, Marketing etc. from where the information is used for further reporting and analyzes to take informed decision by the management.

However, the execution of this concept is not that simple. A data warehouse should be designed so that it meets the following criteria:

- It uses **non-operational data**. This means that the data warehouse is using a copy of data from the active databases that the company uses in its day-to-day operations, so the data warehouse must pull data from the existing databases on a regular scheduled basis. Relevance and nature of the data in the data warehouse depend on the time the jobs are scheduled to pull data from the active databases.
- The data is **time-variant**. This means that whenever data is loaded into the data warehouse, it receives a time stamp which allows for comparisons between different time periods.
- The data is **standardized**. Because the data in a data warehouse usually comes from several different sources, it is possible that the data does not use the same definitions or units. For example- Events table in a our Student Clubs database lists the event dates using the mm/dd/yyyy format (e.g.,

01/10/2013). A table in another database might use the format yy/mm/dd (e.g.13/01/10) for dates. For the data warehouse to match up dates, a standard date format would have to be agreed upon and all data loaded into the data warehouse would have to be converted to use this standard format.

❖ There are two primary schools of thought when designing a data warehouse: **Bottom-Up** and **Top- Down**.

- The **Bottom-Up Approach** starts by creating small data warehouses, called Data Marts to solve specific business problems. As these data marts are created, they can be combined into a larger data warehouse.
- The **Top-Down Approach** suggests that we should start by creating an enterprise-wide data warehouse and then, as specific business needs are identified, create smaller data marts from the data warehouse.

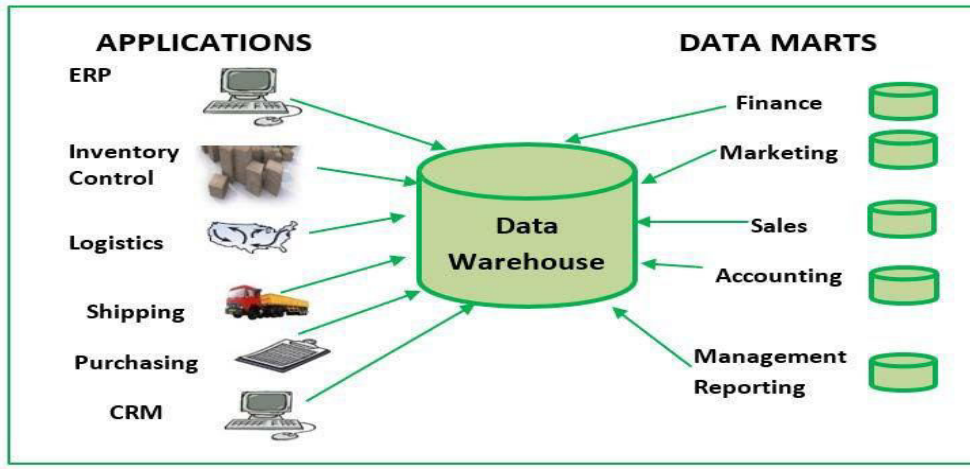


Fig. 3.7.5: Centralized view of Data Warehouse

❖ **Benefits of Data Warehouse**

Organizations find data warehouses quite beneficial for several reasons

- The process of developing a data warehouse forces an organization to better understand the data that it is currently collecting and, equally important, what data is not being collected.
- A data warehouse provides a centralized view of all data being collected across the enterprise and provides a means for determining data that is inconsistent.
- Once all data is identified as consistent, an organization can generate one version of the truth. This is important when the company wants to

report consistent statistics about itself, such as revenue or number of employees.

- By having a data warehouse, snapshots of data can be taken over time. This creates a historical record of data, which allows for an analysis of trends.
- A data warehouse provides tools to combine data, which can provide new information and analysis.

3.7.4 Data Mining

Data Mining is the process of analysing data to find previously unknown trends, patterns, and associations to make decisions. It involves extracting useful data as per the requirement from a collection of raw facts. To start with, one can use the simplest yet powerful tool, Microsoft Excel for data mining. Other examples of data mining tools include Oracle Data mining, R-language etc. Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse. The examples of data mining are- an analysis of sales from a large grocery chain that might determine that milk is purchased more frequently the day after it rains in cities with a population of less than 50,000; The analysis of the popularity of a particular recharge scheme introduced by the telecommunication provider among people of a specific age group, gender and the peak call hours' location wise; A bank may find that loan applicants whose bank accounts show particular deposit and withdrawal patterns are not good credit risks; A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.

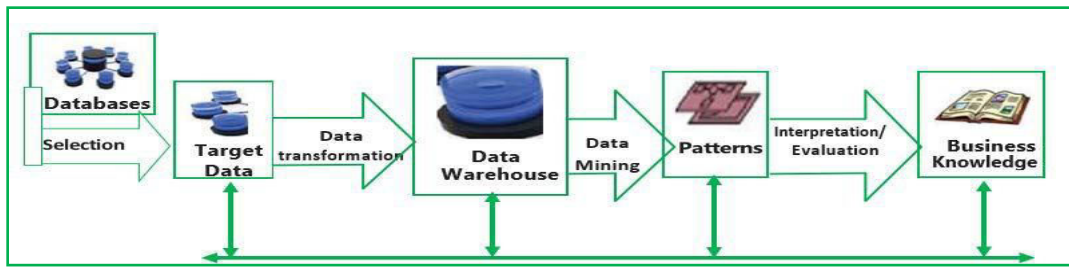


Fig. 3.7.6: Steps involved in Data Mining

The steps involved in the Data Mining process are as follows (Refer Fig. 3.7.6):

a. **Data Integration:** Firstly, the data are collected and integrated from all the different sources which could be flat files, relational database, data warehouse or web etc.

b. **Data Selection:** It may be possible that all the data collected may not be required in the first step. So, in this step we select only those data which we think is useful for data mining.

c. **Data Cleaning:** The data that is collected are not clean and may contain errors, missing values, noisy or inconsistent data. Thus, we need to apply different techniques to get rid of such anomalies.

d. **Data Transformation:** The data even after cleaning are not ready for mining as it needs to be transformed into an appropriate form for mining using different techniques like - smoothing, aggregation, normalization etc.

e. **Data Mining:** In this, various data mining techniques are applied on the data to discover the interesting patterns. Techniques like clustering and association analysis are among the many different techniques used for data mining.

f. **Pattern Evaluation and Knowledge Presentation:** This step involves visualization, transformation, removing redundant patterns etc. from the patterns we generated.

g. **Decisions / Use of Discovered Knowledge:** This step helps user to make use of the knowledge acquired to take better informed decisions.

In some cases, a data-mining project is begun with a hypothetical result in mind. For example, a grocery chain may already have some idea that buying patterns change after it rains and want to get a deeper understanding of exactly what is happening. In other cases, there are no pre-suppositions and a data-mining program is run against large data sets to find patterns and associations. Table 3.7.3 provides the basic differences between Database, Data Warehouse and Data Mining.

Table 3.7.3: Differences between Database, Data Warehouse & Data Mining

DATABASE	DATA WAREHOUSE	DATA MINING
This stores real time information. For example-In a telecommunication sector, the database stores information related to monthly billing details, call records, minimum balance etc.	This store both the historic and transactional data. For example- In the same telecommunication sector, information in a data warehouse will be used for product promotions, decisions relating to sales, cash back offers etc.	This analyses data to find previously unknown trends. For example- In the same telecommunication sector, information will be analysed by data mining techniques to find out call duration with respect a particular age group from the entire data available.

It's function is to record.	It's function is to report and analyse.	It's function is to extract useful data.
Examples include MySQL, MS Access.	Examples include Teradata, Informatica.	Examples include R-Language, Oracle data mining.

3.8 ORGANIZATION STRUCTURE AND RESPONSIBILITIES

Organizations require structure to distribute responsibility to groups of people with specific skills and knowledge. The structure of an organization is called an **Organization Chart**. Organizing and maintaining an organization structure requires that many factors be considered. In most organizations, the organization chart is a living structure that changes frequently, based upon several conditions.

Short and long-term objectives: Organizations sometimes move departments from one executive to another so that departments that were once far from each other (in terms of the organizational chart structure) will be near each other. This provides new opportunities for developing synergies and partnerships that did not exist before the reorganization (reorg). These organizational changes are usually performed to help an organization meet new objectives that require new partnerships and teamwork that were less important before.

- **Market conditions:** Changes in market positions can cause an organization to realign its internal structure to strengthen itself. For example, if a competitor lowers its prices based on a new sourcing strategy, an organization may need to respond by changing its organizational structure to put experienced executives in-charge of specific activities.
- **Regulation:** New regulations may induce an organization to change its organizational structure. For instance, an organization that becomes highly regulated may elect to move its security and compliance group away from IT and place it under the legal department, since compliance has much more to do with legal compliance than industry standards.
- **Available talent:** When someone leaves an organization (or moves to another position within the organization), particularly in positions of leadership, a space opens in the organization chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else. Often, the decisions of how to change the organization will

3.8.2 Job Titles based on Responsibilities

A **Job Title** is a label that is assigned to a job description. It denotes a position in the organization that has a given set of responsibilities and which requires a certain level and focus of education and prior experience.

In an organization, **Executive Management** includes executive managers, the senior managers and executives who are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executive managers are responsible for enacting security policy, which defines (among other things) the protection of assets. Executive managers set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of an organization. Table 3.8.1 describes in detail the functioning of Executive Management in organization.

Table 3.8.1: Executive Management in an organization

CIO (Chief Information Officer)	This is the most senior executive in an organization who works with IT and computer system to support orgnizations' goals.
CTO (Chief Technology Officer)	The CTO is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate from IT.
CSO (Chief Security Officer)	A CSO is responsible for all aspects of security, including information security, physical security, and possibly executive protection (protecting the safety of senior executives).
CISO (Chief Information Security Officer)	This position is responsible for all aspects of data-related security that includes incident management, disaster recovery, vulnerability management, and compliance.
CPO (Chief Privacy Officer)	This position is found in organizations that collect, store and protect sensitive information for large numbers of persons.

Fig. 3.8.1 provides an illustrative overview of positions that report to CIO in general.

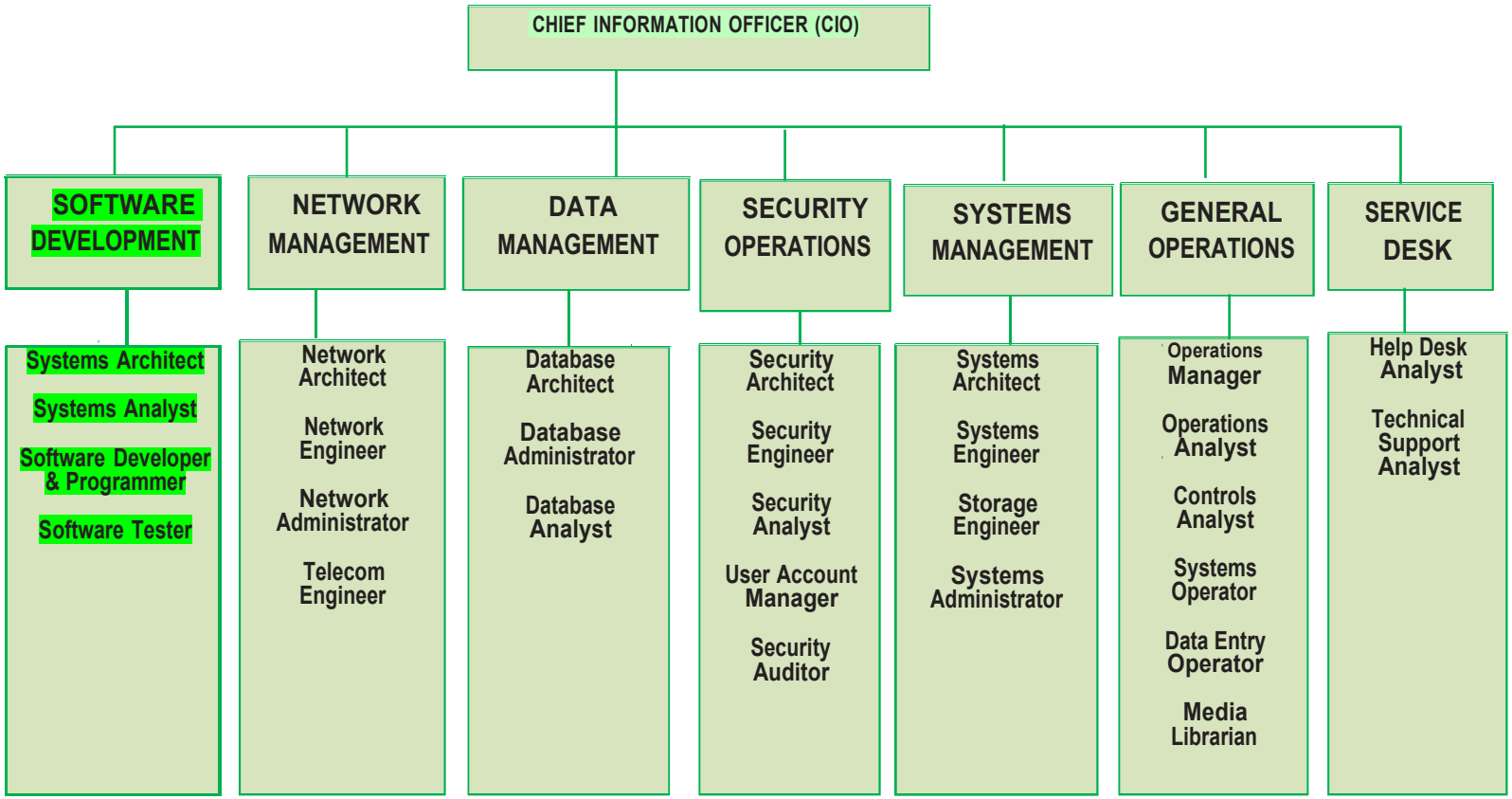


Fig. 3.8.1: Positions under CIO (illustrative)

Database Analyst	This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

(c) Network Management: Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet.

- **Network Architect:** They are involved in the creation of plans and overall layout of the communication network focusing on the aspect on information security as well.
- **Network Engineer:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.
- **Network Administrator:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.
- **Telecom Engineer:** Positions in this role work with telecommunications technologies such as data circuits, phone systems, and voice email systems.

(d) Systems Management: Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. Various positions in system management are shown in Table 3.8.4.

Table 3.8.4: Positions in Systems Management

Systems Architect	Systems Engineer	Storage Engineer	Systems Administrator
This position is responsible for the overall architecture of systems (usually servers), both in terms of the internal architecture of a system, as well as the relationship between systems and design of services such as authentication, e-mail, and time synchronization.	This position is responsible for designing, building, and maintaining servers and server operating systems.	This position is responsible for designing, building, and maintaining storage subsystems.	This position is responsible for performing maintenance and configuration operations on systems.

CHAPTER 4

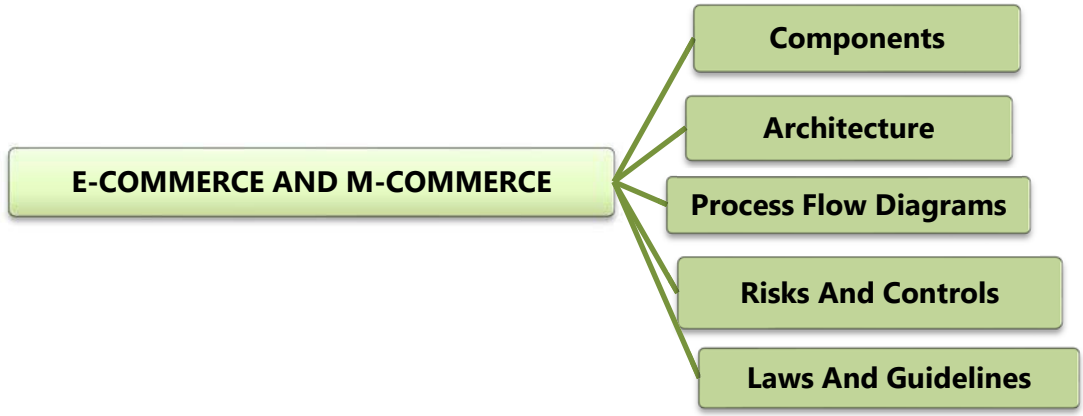
E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

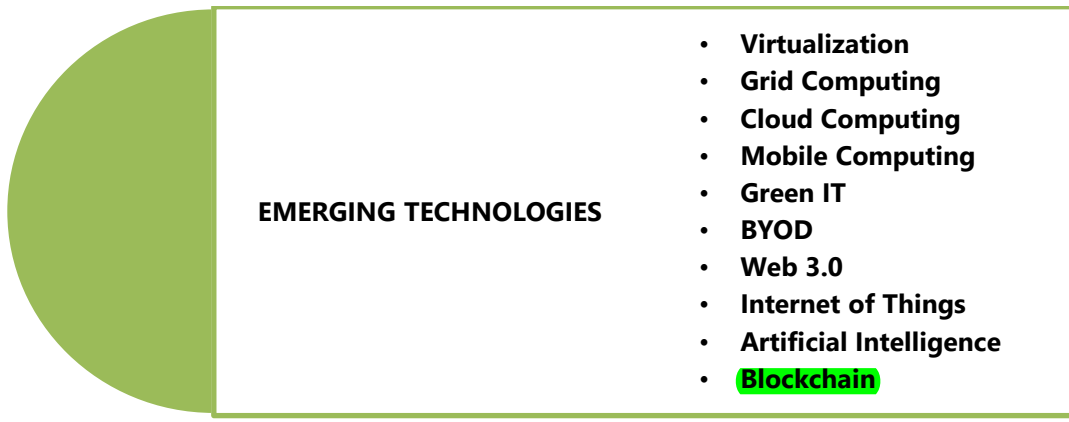
LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Understand the meaning, components and architecture of E-commerce.
- Grasp the knowledge about the process flows in E-commerce transactions.
- Comprehend various aspects of risks and controls in E-commerce and various digital payment used in E-commerce.
- Recognise applicable laws and guidance governing E-Commerce.
- Acknowledge a basic understanding on the paradigms of various Computing Technologies like Cloud Computing, Grid Computing, Mobile Computing, Green Computing, BYOD, Artificial Intelligence, Blockchain etc.

CHAPTER OVERVIEW





4.1 INTRODUCTION TO E-COMMERCE

E-Commerce: "Sale / Purchase of goods / services through electronic mode is e-commerce." This could include the use of technology in the form of Computers, Desktops, Mobile Applications, etc.

The greatest change due to technology innovations in last five years has been the way users perform their daily chores / activity of life. E-Commerce and its related technologies are unquestionably the current leading-edge business and finance delivery systems.

The explosion in the application of technologies and the delivery of these technologies into the hands of consumers has made the vision, the dream, the fantasy of conducting business electronically, anywhere in the global community,

payment is made vide the Credit Card. Once the payment is made, the confirmation email / SMS are received by the user.

STEP 8: Based on the delivery terms, the product is delivered to the customer in specified time.

The first e-commerce transaction vide mobile is supposed to have been done in Norway in 1997, when a Coco-Cola vending machine were configured to respond to mobile messages received from customers. The vending machine delivered products on receiving text messages.

4.1.4 Benefits of E-Business

E-business benefits individuals, businesses, government, and society at large. The major benefits from e-business are as follows:

A. Benefits to Customer/Individual/User

- **Convenience:** Every product/service is easily available at the tip of individual's fingertips on internet.
- **Time saving:** Buyers have enjoy their purchases of many electronic products such as e-books, recharge of mobile, appliances etc. through internet, which reduces the time.
- **Various options for comparison:** There are several options available for customers which are not only being easy to compare but are provided by different players in the market. Buyers are provided with a wider range of choices because they can consider many different products and services from a wider variety of sellers.
- **Easy to find reviews:** There are often reviews about a particular site or product from the previous customers which provides valuable feedback.
- **Coupon and Deals:** There are discount coupons and reward points available for customers to encourage online transaction.
- **Anytime Access:** The customers can evaluate the products 24 hours a day, each day as per their convenience.

B. Benefits to Business / Seller

- **Increased Customer Base:** E-commerce enables a business to offer its products and services to almost everyone in the world who has an internet-enabled device. It facilitates to reach narrow market segments

that are widely scattered geographically, thereby rapidly increasing the number of online customers.

- **Recurring payments made easy:** Each business has number of operations that are homogeneous in nature. This brings in uniformity of scaled operations.
- **Instant Transaction:** The interaction with the system takes place on real time and therefore, allows the customers to respond quickly. This has made possible to crack number of deals.
- **Provides a dynamic market:** Since there are several players, a dynamic market is provided which enhances quality and business.
- **Reduction in:**
  - costs to buyers from increased competition in procurement as more suppliers can compete in an electronically open marketplace.
  - costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
  - overhead costs through uniformity, automation, and large-scale integration of management processes.
  - advertising costs.
- **Efficiency improvement due to:**
  - reduction in time to complete business transactions, particularly from delivery to payment.
  - reduction in errors, time, for information processing by eliminating requirements for re-entering data.
  - reduction in inventories and reduction of risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- **Creation of new markets:** This is done through the ability to reach potential customers easily and with low cost.

- **Easier entry into new markets:** This is especially for entry into geographically remote markets for enterprises regardless of size and location.
- **Low barriers to entry:** Home page gives equal footing to small organizations with large international firms. Small and large organizations have like opportunity to be on WWW and conduct business on the internet.
- **Better quality of goods:** Standardized specifications and competition have increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- **Elimination of Time Delays:** Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.

C. Benefits to Government

- **Instrument to fight corruption:** In line with Government's vision, e-commerce provides a pivotal hand to fight corruption. The Information Technology Act, 2000 provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures.
- **Reduction in use of ecologically damaging materials:** There has been reduction in the use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects.

Clearly, the benefits of corporate-wide implementation of e-business are many, and this list is by no means complete. With the benefits, however, also come the risks. An organization should be cautious not to leap blindly into e-business, but rather first develop an e-business strategy, and then organize a corporate-wide team to implement that strategy.

4.1.5 Disadvantages of E-Business

Following are the disadvantages of e-business:

- **Internet Connection:** Internet connectivity is a pre-requisite to perform online transactions. Internet connectivity may not be available in rural or remote areas. Many people may not have Internet connectivity due to which they may not be able to do online transactions.

and sellers because market information is available to all parties involved in the transaction.

Some relevant terms related to e-marketing are as follows:

(i) **Portal:** Portal is a website that serves as a gateway or a main entry point on the internet to a specific field of interest or an industry. It is a website that is positioned as an entrance to other sites on the internet. A portal consists of web pages that act as a starting point for using the web or web-based services. The control of content can be a source of revenue for firms through charging firms for advertising or charging consumers a subscription for access. For example - Yahoo! Stores is a shopping cart software app that offers small business operators and owners a variety of tools and features to help them build their online stores.

(ii) **e – Shop (electronic shop/ e-tailers):** An e-shop is a virtual store front that sells products and services online where customers can shop at any hour of the day or night without leaving home. It is a convenient way of affecting direct sales to customers; allowing manufacturers to bypass intermediate operators and thereby reducing costs and delivery times. For example: www.sonicnet.com, www.wforwomen.com.

(iii) **e – Mall (electronic mall):** An e-mall, in its basic form, consists of a collection of e-shops usually grouped under a single Internet address. It is a website that displays electronic catalog from several suppliers, and charges commission from them for the sales revenue generated at that site. The basic idea of it is the same as retailing model of a regular shopping mall, a conglomeration of different e-shops that provide consumers a one-stop shopping place offering variety of products and services. They are mainly of following types:

- ***General stores/malls: These are online stores that have a variety of items for sale and do not specialize in selling any one item and are thus called General stores. It includes store like amazon.com which is primarily an e-mall that provides platform to vendors sell and users to purchase various products ranging from books, music, movies, housewares, electronics, toys, clothes etc.***
- ***Specialized stores/malls: The specialized stores would sell only specialized items. For example - www.99acres.com is a website that specializes in buying and selling property and housing on an online platform.***

(iv) e-auctions (electronic auctions): These provide a channel of communication through which the bidding process for products and services can take place between competing buyers. At e-auctions, people buy and sell through an auction website. In e-auctions, almost perfect information is available about products, prices, current demand, and supply. E-auction has become an increasingly popular tool for the buyer to access the lowest price the suppliers are willing to charge. For example – www.salasarauction.com is an online auction platform providing trustworthy solutions to auctioneers and bidders all across the country.

(v) Buyer Aggregator: The Buyer Aggregator brings together large numbers of individual buyers so that they can gain the types of savings that are usually the privilege of large volume buyers. In this, the firm collects the information about goods/service providers, make the providers their partners, and sell their services under its own brand. For example - www.zomato.com is a website that provides information, menus, and user-reviews of restaurants as well as food delivery options from partner restaurants in select cities.

(vi) Virtual Community: Virtual Community is a platform for community of customers who share a common interest and use the internet to communicate with each other. Virtual communities are benefitted when more people join and contribute to the community, the greater the benefits they accrue, but without any additional cost to them. Virtual communities may be of different types based on communities of interest in a common goal, communities of learning, and communities of practice based on the characteristics of bonds and intentions etc. For example - www.facebook.com allows the creation of virtual community that let any user to connect with others who share similar interests and experiences.

(vii) e-distribution: e-distribution is a concept wherein a company supplies products and services directly to individual businesses. This model helps distributors to achieve efficiency savings by managing large volumes of customers, automating orders, communicating with partners, and facilitating value-adding services such as order tracking through each point in the supply chain. For example - www.wipro.com uses the internet to provide fully integrated e-business enabled solutions that help to unify the information flows across all the major distribution processes including sales and marketing automation, customer service, warehouse logistics, purchasing and inventory management, and finance.

(viii) e-procurement: e-procurement is the management of all procurement activities via electronic means. Many companies now prefer to procure the required goods and services through a website devoted to procurement. Business models based on e-procurement seek efficiency in accessing information on suppliers, availability, price, quality, and delivery times as well as cost savings by collaborating with partners to pool their buying power and secure best value deals. E-procurement infomediaries specialize in providing up-to-date and real-time information on all aspects of the supply of materials to businesses. For example- www.eprocure.gov.in is an e-procurement System of India that enables the tenderers to download the tender schedule free of cost and then submit their bids online.

4.1.7 E-Commerce Business Models

A **Business Model** can be defined as the mechanism by which a business intends to generate revenue and profits and includes products, services and information flows, the sources of revenues, and benefits for suppliers and customers. Internet has created new business models for online business. An e-business model is an adaptation of an organization's business model to the internet economy. A Business Model is adopted by an organization as a framework to describe how it makes money on a sustainable basis and grows. A business model also enables a firm to analyze its environment more effectively and thereby exploit the potential of its markets; better understand its customers; and raise entry barriers for rivals. E-business models utilize the benefits of electronic communications to achieve the value adding processes.

Example 4.2: The e-business models relating to e-business markets can be summarized as given below in the Table 4.1.3.

Table 4.1.3: Some Business Models for E-Commerce

Models	Definition	e-business markets	Examples
Business-to-Consumer (B2C)	B2C is typically used to refer to online retailers who sell products and services to consumers through the Internet. Generally, this supports the activities within the consumer chain that	e-shops, e-malls, e-auctions, Buyer aggregators etc.	This may involve direct sellers like www.cisco.com; Online intermediaries like www.amazon.com and communities built around common interests like education, For example

	focuses on sell-side activities.		www.byjus.com.
Business-to-Business (B2B)	This supports the supply chain of organizations that involves commerce between a company and its suppliers or other partners. A website sells its products to an intermediate buyer who then sells the product to the final customer.	e-auctions, e-procurement, e-distribution etc.	A wholesaler places an order from a company's website and after receiving the consignment, sells the end-product to the final customer who comes to buy the product at one of its online retail store. For example - www.indiamart.com is a website that helps in connecting prospective buyers to sellers and vice-versa.
Consumer-to-Consumer (C2C)	With C2C e-business model, consumers sell directly to other consumers via on-line classified ads and auctions, or by selling personal services and expertise on-line. C2C e-commerce allows unknown, untrusted parties to sell goods and services to one another. The model facilitates plain and simple commerce between consumers, wherein revenue streams are typically matching buyers with sellers and vice-versa.	e-auctions	A consumer selling his/her mobile phones, cameras, computers, laptops, tablets, video game consoles, and home appliances like television, refrigerators, air conditioners, oven to even hair driers and ceiling fan etc. by publishing the relevant information on the website. For example-www.olx.com

Consumer to Business (C2B)	With C2B, consumers create value and businesses consume that value. In the model, a reverse auction allows consumers to set and demand their own price and companies bid to consume their offers and services.	e-distribution	The best example for this model are the job portals like TimesJobs.com etc. Another example could be www.paisabazaar.com in which various banks/financial institutions provide different offers to which the consumers place an estimate of amount s/he wants to spend on hiring the particular service. The financial institution/ bank that fulfills the consumer's requirement within the specified budget, approaches the consumers and provides its services to them.
Consumer to Government (C2G)	This covers all the e-commerce transactions between consumers and government.	portal	www. incometaxindia.gov.in
Government to Consumer (G2C)	This allows consumers to provide feedback or ask information about government authority from public sector. Consumers can reach higher authority without going around in cities. The aim is to reduce the average time for fulfilling citizen's requests for various government services.	portal	Services include land searches, confirmation of genuine licenses and vehicle ownership searches, disputes such as non-payment of tax or tax refunds are resolved through online support on the government platforms. For example- e-Seva (Andhra Pradesh)

Business to Government (B2G)	B2G model is a variant of B2B model. Such websites are used by governments to trade and exchange information with various business organizations.	portal	B2G websites are accredited by the government and provide a medium to businesses to submit application forms to the government. For example - any business that pays taxes, submit file reports, or sell goods and services to Government agencies.

According to India Brand Equity Foundation, the Indian E-commerce industry has been on an upward growth trajectory and is expected to surpass the US to become the second largest E-commerce market in the world by 2034. The E-commerce market is expected to reach ₹ 13,97,800 crores (US$ 200 billion) by 2027 from ₹ 2,69,076.5 crores (US$ 38.5 billion) in 2017, supported by rising income and surge in internet users.

4.2 COMPONENTS OF E-COMMERCE

Referring to the Fig, 4.2.1, E-commerce components include the following:

(i) **User:** The user may be individual/organization or anybody using the e-commerce platforms. As e-commerce has made procurement easy and simple just on a click of button, e-commerce vendors need to ensure that user's loyalty is built and also that their products are not delivered to wrong person. For example, e-commerce vendors selling products like medicine/drugs need to ensure that their products are not delivered to wrong person/user. Customer loyalty is built through expediting order processing, timely delivery, easy redressal, customer-friendly return policy, and complete customer satisfaction throughout the transaction and after it. Although users accept the shipping speeds that are offered by e-commerce companies, what they do not accept is promises broken. Therefore, shipping time should be promised to users only if e-business has certainty in its ability to do so. If users engage in a flawless transaction with e-business once, their confidence will increase.

fall into the hand of a malicious hacker while transferring from his/her computer to the web server.

Privacy Policy and Security are also gaining importance under the Information Technology Act, 2000 (as amended 2008). The act specifically states that security of such data (the one collected by e-commerce vendor from customer) shall be responsibility of e-commerce vendor.

(iii) Technology Infrastructure: E-commerce is technology driven. Various types of e-commerce applications and technologies are being used by the organizations to increase scope of business. New methods for building and running websites are constantly evolving, and the specific technology used may differ greatly from one organization to another. For an e-commerce retailer's website to be successful, it needs to be well integrated. This means that it needs to be properly developed, designed, and managed so that it functions effectively over time.

The technology used in e-commerce should possess following characteristics:

- **Scalable** with minimal effort to handle peak traffic and to accommodate the needs of business's online growth.
- **Easy to use and convenient** for the customers. The technology selected should enable the customers to find what they want as well as enable the merchant to promote its products. There is nothing more frustrating to customers than searching for but not finding something that is available on the website somewhere.
- Implementing **Responsive Design** to make a website accessible and usable on every device is important for the success of an e-commerce site. The use of mobile devices to access websites is continually growing, and m-commerce sales are a large portion of this traffic. E-commerce website should be optimized for mobile, providing the best experience for users no matter what device they are using to access to the website.

The computers, servers, database, mobile apps, digital libraries, data interchange are the components of Technology Infrastructure that enable the e-commerce transactions. These components are discussed as below:

(a) Computers, Servers, and Database

- These are the backbone for the success of the venture. Big e-commerce organization invests huge amount of money/time in

exchange of documents and customers' data. There are defined standards to ensure seamless / exact communication in e-commerce.

(iv) Internet/Network: This is the key to success of e-commerce transactions.

- This is the critical enabler for e-commerce. Internet connectivity is important for any e-commerce transactions to go through. Net connectivity in present days can be through traditional as well as new technology.
- The faster net connectivity leads to better e-commerce. Many mobile companies in India have launched 4G services.
- The success of e-commerce trade depends upon the internet capability of organization. At a global level, it is linked to the countries' capability to create a high-speed network. The latest communication technologies like 4G, 5G have already made in-roads in India.

(v) Web Portal: This shall provide the interface through which an individual/organization shall perform e-commerce transactions.

- Web Portal is an application through which user interacts with the e-commerce vendor. These are the front end through which user interacts for an e-commerce transaction and can be accessed through desktops/laptops/PDA/hand-held computing devices/mobiles and now through smart TVs also.
- The sale process starts from the very moment the visitor looks at the Web portal. First impressions are very important. If the portal has weak design, users create a bad impression of the business. The simplicity and clarity of content on web portal is directly linked to customer experience of buying a product online. E-commerce vendors put a lot of money and effort in this aspect. Sophisticated portal design allows the small business to compete on equal footing with larger and better financed companies.

(vi) Payment Gateway: The payment gateway is another critical component of e-commerce set up. In an e-commerce transaction, the major proportion of online payments is being performed based on payment gateway technology. Payment gateway represents the way e-commerce/m-commerce vendors collect their payments. A payment gateway is a server that is dedicated to linking websites and banks so that online transactions can be completed in real-time. It is a system of computer processes that

authorizes, verifies, and accepts or declines credit/debit card transactions on behalf of the merchant through secure Internet connections. PayPal and WorldPay are some of the most popular payment gateways. A payment gateway allows a secure connection directly between a website and a bank that facilitates direct placement of payments from client's account and straight deposit into the website's bank account.

4.3 ARCHITECTURE OF NETWORKED SYSTEMS

Architecture is a term used to define the style of design and method of construction, used generally for buildings and other physical structures. In e-commerce, it denotes the way network architectures are built. E-commerce runs through network-connected systems which can have two types of architecture namely **Two tier** and **Three tier**.

4.3.1 Two Tier Client Server Architecture

In a **Two-tier network**, client (user) sends request to Server and the Server responds to the request by fetching the data from it. The Two-tier architecture is divided into two tiers - **Presentation Tier** and **Database Tier** as shown in the Fig. 4.3.1.

(i) **Presentation Tier (Client Application/Client Tier):** This is the interface that allows user to interact with the e-commerce/m-commerce vendor. User can login to an e-commerce vendor through this tier. This application also connects to database tier and displays the various products/prices to customers.

(ii) **Database Tier (Data Tier):** The product data/price data/customer data and other related data are kept here. User has no access to data/information at this level, but s/he can display all data/information stored here through application tier.

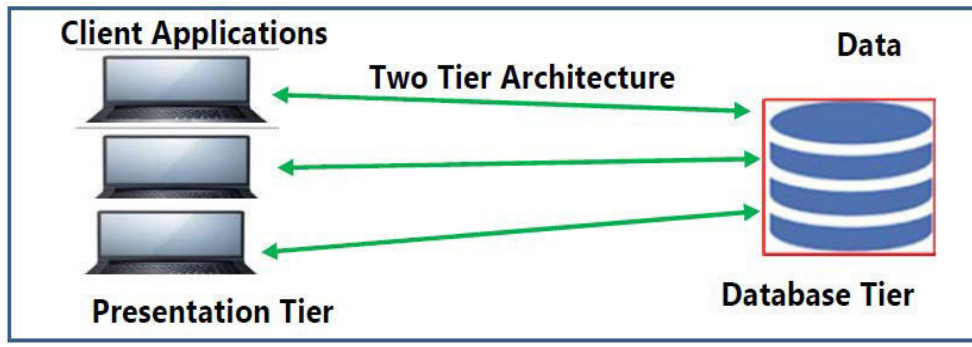


Fig. 4.3.1: Two Tier Client Server Architecture

		♦ Above is only an illustrative list. Imagine numerous possible combinations based on fact of incorrect delivery.
2	Service ordered by **'A'** not provided by online vendor. For example: Courier company does not collect an important document by online vendor and provides to **'A'**.	♦ Who bears the loss that may be incurred by **'A'**?
3	**'A'** auction website sells inadvertently sales products which cannot be sold at all, or sale of those products is illegal. For example: Guns/ Narcotics Drugs.	♦ What is the legal liability of seller of such products? ♦ What is legal liability of buyers of such products? ♦ What is the legal liability of auction website?
4	**'A'** downloads a software from a server in USA. **'A'** is in state of MP and then he sells the software to a person in Mumbai or sells the same to another person in Singapore.	♦ Whether such a download is import? ♦ If **'A'** re-exports, can s/he claim benefits under customs?

4.6.3 Special Laws governing e-Commerce

E-commerce is covered under few other laws as these transactions are done electronically.

- Information Technology Act, 2000 (As amended 2008)
- Reserve Bank of India Act, 1934.

I. Information Technology Act, (IT) 2000

Due to anonymous nature of the internet, people with intelligence have been grossly misusing internet to commit criminal activities in the cyberspace. This necessitated a need for framing and enforcing suitable laws for providing adequate legal protection and recourse against people who cause threat to the

and approved in a court of law. **Section 4 of the IT Act** confers for "legal recognition of electronic records". It provides that where any law requires that any information or matter should be in writing or in the typewritten or printed form, then such requirement shall be deemed to be satisfied if it is in an electronic form.

- The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government on a later date. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital Signatures have been given legal validity and sanction in the IT Act, 2000. **Section 3 of the IT Act** contains provisions related to authentication of electronic records by affixing digital signature. The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature.
- **Section 35 of IT Act** throws open the doors for the entry of any person corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates in such forms as may be prescribed by Central Government.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- **Section 6 of the IT Act** lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.
- The IT Act also addresses the important issues of security which are so critical to the success of electronic transactions. **Section 14 of the IT Act** relates to secure electronic record and provides that where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. **Section 15 of the IT Act** provides for the security procedure to be applied to Digital Signatures for being treated as a secure digital signature.

initially denied me a refund or replacement, claiming that my complaint was not genuine. This was very annoying, so I filed a complaint with the police and on various customer complaint websites, after which they refunded my money on July 31, 2019," Mr. A said.

"We will begin our investigation by taking the statement of the delivery boy, after which we will look into other aspects of the case," police sub-inspector said.

For its part, online retailer said in written statement: "The company observes a zero-tolerance policy on incidents that impact customer trust. We are conducting an internal investigation into this case and are putting all efforts to find out the real facts of this incident. Meanwhile, as a responsible marketplace, the money has been refunded to the customer in good faith."

Case 2: Online Retailer not being paid by companies putting ads on online retailer's portal.

India's top online retailer filed first such case in the Delhi High Court against a US-based computer data storage company WD for allegedly not paying more than ₹ 1 crore for placing advertisements on the retailer's website.

4.6.4 The Forces Behind the E-Commerce Revolution

E-commerce business is expected to grow at a rapid pace. With the advancement in technology, such as smart phones and Apps, it is clear that there will be astonishing growth for this sector in the coming years. Those businesses which have the vision to anticipate change and catch the trend before the competitors do would definitely be more successful. This is due to the reason that competition in e-commerce is growing at a rapid pace and the customers have abundance of options to choose from. E-marketers will have to improve not only their product quality but will have to work on user experience to retain the customers. It is time to gain a better understanding of the forces underpinning its emergence. Broadly speaking, they can be categorized as follows:

- **Proliferation of Mobile Device:** The user is moving from desktop to mobile computing. 55% of the online traffic is generated from mobile devices and still it is on the increase. The most spectacular growth in mobile phone ownership contributes to the growth of e-commerce through mobile app. The creation of mobile application for e-commerce website is the latest trend to drive many online shoppers who use mobile apps for online shopping. The latest trend is using videos for product to attract customers. Shoppable videos for customers instead of using images and content would enable them to shop for products

and services directly from videos. The product content and recommendation increase the sales conversion through competitive analysis and identifying the basic style, studying, and using trending keywords and trying new trends.

- **Convergence of Mobile Telecommunication Network and the Internet:** The mobile internet is also about a very different user experience. It is characterized by goal-oriented activities reserving movie tickets or looking for directions. These activities are often conducted when time pressure, such as knowing that movie starts at 8 PM and are subject to distraction. The transition from 3G to 5G and faster data rate along with many new applications and services makes the success of e-commerce possible.

- **Social Network:** Social media these days is an integral part of almost every consumer's online habits. The latest trend is the inclusion of e-commerce in social networks, such as Facebook, Twitter, YouTube, etc. This allows the consumer to buy the product without even leaving the social media platform. The concept of commerce using social media tool box will help the e-marketer to become more familiar with their clients and at the same time will also enable the customers to develop deep relationships with the merchants they buy from. Promotion of products on social media platforms is another trend.

- **Biometrics:** E-commerce is a rapidly growing industry where the main concern for every retailer is to offer maximum comfort and security to the buyer. Serious security issues such as hacking, spamming, online fraud and theft of confidential data are still holding back many online users from purchasing products online. Biometric verification is a recent e-commerce technology trends that measure the physical characteristics of users such as fingerprints, palm, face, or voice to solve security issues. With the use of biometrics, there will be no more stolen or forgotten password problem, also this enhanced security measures will make forging difficult for intruders.

- **Artificial Intelligence (AI):** Artificial intelligence in e-commerce offers personalized and interactive buying experiences. Another trend in e-commerce is the use of Chatbot, a form of AI which is fully automated chat agent that will answer all the questions of consumers and act as a first point of contact. Chatbots commonly known as messenger bots is a piece of software that can be used by a retailer to chat with customers via text or voice. Well-designed chatbots can offer personalized assistances, enhance the user experience, process orders, track shipments, provide product suggestion, automates processes, and lot more. A chatbot can offer guided, interactive browsing to

the consumers and provide personalized answers to customers' questions at all times.

- **Predictive Analysis:** The use of predictive analysis tools is increasing to predict the online customers' behaviour, their buying habits, their tastes, and preferences, both quantitative and qualitative. By segmenting the customers in different categories, the company can optimize its e-mail communication in order to increase conversions by offering the right customer; the right product; in the right way; and at the right time. The analytical approach would lead to an increase in the number of new customers, as well as tools can determine the probability of a customer purchasing certain products in certain situations. Based on this information, marketer can create unique, personalized promotions for each customer.
- **Support of IT governing Laws:** As already discussed, various provisions of IT Act, 2000 and laws now govern E-commerce which has proven to be a game-changer for the Indian economy and the future of "Digital India". The availability of jurisprudence in India on the various issues related to e-commerce sector is in abundance. These laws empower the e-businesses and lower the chances of any upsetting legal conflicts or lost business.

4.7 DIGITAL PAYMENTS

Digital Payment also known as Electronic 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. No hard cash is involved in the digital payments and all the transactions in digital payments are completed online. It is an instant and convenient way to make payments.

New digital payment platforms such as UPI and IMPS are becoming increasingly popular. Using these new platforms, banks have been scaling rapidly. Every Bank is impacted by new digital disruptions, so new banking services and ways should be adapted to use various digital channels to interact and provide services to customers. To reach out to customers at their convenience, banks are aggressively going digital. For millennials, banking is all about convenience – a seamless user interface akin to that of games or app. They value transparency and minimal processes. Convenience can be delivered through mobile apps and digital banking, the latter is provided by relationship managers, who need to be proficient in products and process knowledge. A high level of adaptability is a must for banking sector in this highly digital and tech-savvy age, where banking transactions can happen even on a mobile or tablet with a few clicks.

digital currency produced by a public network, rather than any government, that uses cryptography to ensure that payments are sent and received safely. A cryptocurrency is a medium of exchange wherein records of individual coin ownership are stored in a computerized database using strong cryptography.

Cryptocurrency is called so because all the data is ensured with strong cryptography. The strong cryptography makes it almost impossible to counterfeit or double spend. The other digital currencies such as DigiCash utilizes a trusted third party approach in which a third party verifies and facilitates the transactions. Cryptocurrency is completely decentralized, which means that there are no servers involved and no central controlling authority.

Cryptocurrency is digital money which does not involve any physical coin. Since it is all online, the user can transfer cryptocurrency to someone online without going to the bank. It can be used for making quick payments without any transaction fees. Cryptocurrency is stored in a digital wallet either on the computer or on other hardware. The first cryptocurrency was Bitcoin which was launched in 2009. The other cryptocurrencies prevailing in the world today include Litecoin, Peercoin, Namecoin, as well as Ethereum.

(ix) ***e-Rupi: Recently, the Government of India has launched a new mode of cashless and contactless digital payment named e-Rupi based on UPI systems to ensure seamless transfer of benefits to the citizens in a "leak-proof" manner.***

Fig. 4.7.3: e-Rupi

It is an e-voucher, which will be delivered to beneficiaries in the form of a QR code and SMS-string-based voucher through which funds will be directly transferred to their bank account. These vouchers are person- and purpose-specific, meaning if they are released by the government for the purpose of vaccination, for instance, then they can be redeemed only for that. This contactless e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential. The entire transaction process through this voucher is relatively faster and at the same time reliable, as the required amount is

already stored in the voucher. Any government agency and corporation can generate e-RUPI vouchers via their partner banks.

4.7.2 Advantages of Digital Payments

(i) Easy and convenient: Digital payments are easy and convenient. E-payment eliminates the security risks associated with handling cash.

(ii) Pay or send money from anywhere: With digital payment modes, one can pay from anywhere anytime.

(iii) Discounts from taxes: Government has announced many discounts to encourage digital payments. Users get 0.75% discounts on fuels and 10% discount on insurance premiums of government insurers.

(iv) Written record: User often forgets to note down his/her spending, or even if nothing is done it takes a lot of time. These are automatically recorded in passbook or inside E-Wallet app. This helps to maintain record, track spending and budget planning.

(v) Less Risk: Digital payments have less risk if used wisely. If user losses mobile phone or debit/credit card or Aadhar card, he/she need not to worry a lot. No one can use anyone else's money without MPIN, PIN or fingerprint in the case of Aadhar. It is advised that user should get card blocked, if lost.

(vi) Competitive advantage to business: Digital payment enables businesses to make sales to customers who choose to pay electronically and gain a competitive advantage over those who accept payment only through traditional methods.

(vii) Environment Friendly: Digital payment eliminates the use of paper.

4.7.3 Drawbacks of Digital Payments

Every coin has two sides so as the digital payments. Despite many advantages, digital payments have few drawbacks also.

(i) Difficult for a non-technical person: As most of the digital payment modes are based on mobile phone, the internet and cards; these modes are somewhat difficult for non-technical persons such as farmers, workers etc.

environments. Virtualization helps in cutting IT expenses, in enhancing security, and also in increasing operational efficiency. Virtualization refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them. By providing a logical view of computing resources, rather than a physical view; virtualization allows its' users to manipulate their systems' operating systems into thinking that a group of servers is a single pool of computing resources and conversely, allows its users to run multiple operating systems simultaneously on a single machine.

I. Concept of Virtualization

The core concept of Virtualization lies in Partitioning which divides a single physical server into multiple logical servers. Once the physical server is divided, each logical server can run an operating system and applications independently. For example - Partitioning of a hard drive is considered as virtualization because one drive is partitioned in a way to create two separate hard drives. Devices, application and human users are able to interact with the virtual resource as if it were a real single logical resource.

II. Application Areas of Virtualization

- **Server Consolidation:** Virtual machines are used to consolidate many physical servers into fewer servers, which in turn host virtual machines. Each physical server is reflected as a virtual machine "guest" residing on a virtual machine host system. This is also known as "Physical-to-Virtual" or 'P2V' transformation.
- **Disaster Recovery:** Virtual machines can be used as "hot standby" environments for physical production servers. This changes the classical "backup-and-restore" philosophy, by providing backup images that can "boot" into live virtual machines, capable of taking over workload for a production server experiencing an outage.
- **Testing and Training:** Virtualization can give root access to a virtual machine thus providing the testers an environment, where they can actually test the software on all possible configurations on a single hardware system. If the virtual system crashes, it will not affect the actual system, and within a few minutes, a new virtual environment will be created. This can be very useful such as in kernel development and operating system courses.
- **Portable Applications:** Portable applications are needed when running an application from a removable drive, without installing it on

the system's main disk drive. Virtualization can be used to encapsulate the application with a redirection layer that stores temporary files, windows registry entries and other state information in the application's installation directory and not within the system's permanent file system.

- **Portable Workspaces:** A portable workspace is like an offline workspace that can be moved across multiple computers without requiring repeated installation, customization, and data setup. Recent technologies have used virtualization to create portable workspaces on devices like iPods and USB memory sticks.

III. Common Types of Virtualization

- **Hardware Virtualization:** Hardware Virtualization or Platform Virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. This enables the users to run different operating systems on the same machine simultaneously. 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.

  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. The software that creates a virtual machine on the host hardware is called a Hypervisor or Virtual Machine Manager. The hypervisor controls the processor, memory, and other components by allowing several different operating systems to run on the same machine without the need for a source code. The operating system running on the machine will appear to have its own processor, memory and other components.

- **Network Virtualization:** Network Virtualization 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. This allows a large physical network to be provisioned into multiple smaller logical networks and conversely allows multiple physical LANs to be combined into a larger logical network. This behavior allows administrators to improve

network traffic control, enterprise, and security. Network virtualization involves platform virtualization, often combined with resource virtualization.

Various equipment and software vendors offer network virtualization by combining any of the Network hardware such as switches and Network Interface Cards (NICs); Network elements such as firewalls and load balancers; Networks such as Virtual LANs (VLANs); Network storage devices; Network machine-to-machine elements such as telecommunications devices; Network mobile elements such as laptop computers, tablet computers, smart phones, and Network media such as Ethernet and Fiber Channel. Network virtualization is intended to optimize network speed, reliability, flexibility, scalability, and security.

- **Storage Virtualization:** Storage Virtualization is an 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. Storage virtualization 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). Administrators can implement virtualization with software applications or by using hardware and software hybrid appliances. The servers connected to the storage system are not aware of where the data really is. Storage virtualization is sometimes described as "abstracting the logical storage from the physical storage".

4.8.2 Grid Computing

The computing resources in most of the organizations are underutilized but are necessary for certain operations. The idea of Grid computing is to make use of such non-utilized computing power by the needy organizations, and thereby the Return on Investment (RoI) on computing investments can be increased.

Grid Computing 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. A typical Grid Model is shown in Fig. 4.8.1.

performed on the grid can temporarily be suspended or even cancelled and performed again later to make room for the higher priority work.

- **Parallel CPU Capacity:** The potential for usage of massive parallel CPU capacity is one of the most common vision and attractive feature of a grid. A CPU-intensive grid application can be thought of as many smaller sub-jobs, each executing on a different machine in the grid. To the extent that these sub-jobs do not need to communicate with each other, the application becomes more scalable. A perfectly scalable application will, for example, finish in one tenth of the time if it uses ten times the number of processors.
- **Virtual resources and virtual organizations for collaboration:** Grid computing provides an environment for collaboration among a wider audience. The users of the grid can be organized dynamically into several virtual organizations each with different policy requirements. These virtual organizations can share their resources such as data, specialized devices, software, services, licenses, and so on, collectively as a larger grid. The grid can help in enforcing security rules among them and implement policies, which can resolve priorities for both resources and users.
- **Access to additional resources:** In addition to CPU and storage resources, a grid can provide access to other resources as well. For example, if a user needs to increase their total bandwidth to the Internet to implement a data mining search engine, the work can be split among grid machines that have independent connections to the Internet. In this way, total searching capability is multiplied, since each machine has a separate connection to the Internet.
- **Reliability:** High-end conventional computing systems use expensive hardware to increase reliability. The machines also use duplicate processors in such a way that when they fail, one can be replaced without turning the other off. Power supplies and cooling systems are duplicated. The systems are operated on special power sources that can start generators if utility power is interrupted. All of this builds a reliable system, but at a great cost, due to the duplication of expensive components.
- **Better Management:** The goal to virtualize the resources on the grid and more uniformly handle heterogeneous systems create new

- **Globalize the workforce:** Cloud computing allows users to globalize their workforce and improve accessibility while shortening training time and new employee learning curves.
- **Streamline business processes:** Cloud Service Providers (CSPs) manage underlying infrastructure to enable organizations to focus on application development in less time with less resources.
- **Reduce capital costs:** Cloud computing users worldwide can access the cloud with Internet connection that subsequently does not require them to spend on technology infrastructure, hardware, software, or licensing fees.
- **Easy access to information/applications:** One can access information and applications as utilities anytime and anywhere, over the internet using any smart computing device.
- **Pervasive accessibility:** Data and applications can be accessed anytime, anywhere, using any smart computing device, making our life so much easier.
- **Backup and Recovery:** It is relatively much easier to backup and restore data stored in cloud. Even if one hard disk fails, data will be safe and will continue to be available automatically on another one.
- **Monitor projects more effectively:** It is feasible to confine within budgetary allocations and can be ahead of completion cycle times.
- **Less personnel training is needed:** It takes fewer people to do more work on a cloud with a minimal learning curve on hardware and software issues.
- **Minimize maintenance and licensing software:** As there is not much of non-premise computing resources, maintenance becomes simple and updates and renewals of software systems rely on the cloud vendor or provider.
- **Load balancing:** Load balancing is defined as the process of distributing workloads across multiple servers to prevent any single server from getting overloaded and possibly breaking down. It plays an important role in maintaining the availability of cloud-based applications to customers, business partners, and end users, thus making it more reliable.

- **Improved flexibility:** Cloud users can make fast changes in their work environment without serious issues at stake in order to scale services to fit their needs.

III. Drawbacks of Cloud Computing

- If Internet connection is lost, the link to the cloud and thereby to the data and applications is lost.
- Security is a major concern as entire working with data and applications depend on other cloud vendors or providers.
- Although Cloud computing supports scalability (i.e. quickly scaling up and down computing resources depending on the need), it does not permit the control on these resources as these are not owned by the user or customer.
- Depending on the cloud vendor or service provider, customers may have to face restrictions on the availability of applications, operating systems, and infrastructure options.
- Interoperability (ability of two or more applications that are required to support a business need to work together by sharing data and other business-related resources) is an issue wherein all the applications may not reside with a single cloud vendor and two vendors may have applications that do not cooperate with each other.

IV. Cloud Computing Environment

The Cloud Computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows (given in Fig. 4.8.3).

(A) **Private Cloud:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for an organization's benefits. Also called **Internal Clouds** or **Corporate Clouds,** Private Clouds can either be private to an organization and managed by the single organization **(On-Premises Private Cloud)** or can be managed by third party **(Outsourced Private Cloud)**. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

- **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

(ii) Instances of IaaS (refer Table 4.8.1)

Table 4.8.1: Instances of IaaS

Instance	Description
Network as a Service (NaaS)	• It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis. • Provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. • Allows network architects to create virtual networks; virtual Network Interface Cards (NICs), virtual routers, virtual switches, and other networking components. • Allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
Storage as a Service (STaaS)	• It is an ability given to the end users to store the data on the storage services provided by the service provider. • This provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. • STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center.
Database as a	• It is an ability given to the end users to access the database service without the need to install and maintain it on the

Service (DBaaS)	pay-per-use basis. • This provides users with seamless mechanisms to create, store, and access databases at a host site on demand. • The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
Backend as a Service (BaaS)	• This provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
Desktop as a Service (DTaaS)	• It is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security, and upgrades. • This provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. • The end-users are responsible for securing and managing their own desktop images and applications. These services are simple to deploy, are highly secure, and produce better experience on almost all devices.

(B) Platform as a Service (PaaS): PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider. In traditional application development, the application will be developed locally and will be hosted in the central location. In stand-alone application development, the application developed by traditional development platforms result in licensing - based software whereas PaaS changes the application development from local machine to online. PaaS providers provide a pre-built computing platform consisting of operating system, programming languages, database, testing tools apart from some build tools, deployment tools, and software load balancers. The software developers can develop and run their software solutions on cloud platform without incurring cost and complexity of acquiring and managing the underlying software and hardware. For example- Google App Engine, Windows Azure Compute etc.

(C) Software as a Service (SaaS): SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure. SaaS has changed the way the software is delivered to the customers. SaaS provides users to access large variety of applications over internet that is hosted on service provider's infrastructure. The main difference between SaaS and PaaS is that PaaS normally represents a platform for application development, while SaaS provides online applications that are already developed. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system - thus Google is provisioning software as a service. Different instances of SaaS are discussed in the Table 4.8.2.

Table 4.8.2: Instances of SaaS

Instance	Description
Testing as a Service (TaaS)	This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
API as a Service (APIaaS)	This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
Email as a Service (EaaS)	This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

(D) Other Cloud Service Models (refer Table 4.8.3)

Table 4.8.3: Other Cloud Service Models

Instance	Description
Communication as a Service (CaaS)	• It is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to

VI. Pertinent Issues related to Cloud Computing

As an emerging technology, cloud computing involves several issues, out of which some of them are as follows:

- **Threshold Policy:** The main objective of implementing threshold policy is to inform cloud computing service consumers and providers what they should do. Quite often, this policy does not exist. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do. However, there is no standard format for the SLA, and as such, there may be services not documented in the SLA that the customer may be requiring in future. A carefully drafted threshold policy outlines what cloud computing service consumers and providers should do. It is important to consider how the cloud service provider will handle sudden increases or decreases in demand. How will unused resources be allocated?
- **Interoperability:** If a company enters into a contract with one cloud computing vendor, it may find it difficult to change to another computing vendor that has proprietary APIs (Application Programming Interfaces) and different formats for importing and exporting data. Industry cloud computing standards do not exist for APIs or formats for importing/exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. Once a company is locked in with one cloud provider, it is not easy to move an entire infrastructure to other clouds. Moreover, each cloud provider offers a unique set of services and tools for operating and controlling its cloud. Learning a new cloud environment is similar to learning a new technology.
- **Hidden Costs:** Such costs may include higher network charges for storage and database applications, or latency issues for users who may be located far from cloud service providers.
- **Unexpected Behaviour:** An application may perform well at the company's internal data center. It does not necessarily imply that the application will perform the same way in the cloud. Therefore, it is essential to test its performance in the cloud for unexpected behavior. Testing may include checking how the application allocates resources on sudden increase in demand for resources and how it allocates unused

I. Advantages of BYOD

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise, he would be carrying his personal as well as organization provided devices.
- **Lower IT budgets:** It may involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the outlay of an organization in providing devices to employees.
- **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that results in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency:** The efficiency of employees is more when an employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

II. Emerging BYOD Threats

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in '**Lack of Device Visibility**'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. 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. For example, if a virus hits the network and all the devices connected to the

(A) Risk to Product manufacturer

- **Impact on Business:** Manufacturers may be out of business in few years if IoT becomes a necessary product feature.
- **Data storage and analytics:** The manufacturers need to ensure that the huge data generated from IoT devices is kept secured. Hacking/Loosing this data may be distractors for entity as well as the individual to whom it relates to.
- **Intentional obsolescence of devices:** This may happen due to following:
  - Companies which want to bring a new product may force users to dump the old products. This they can do by disabling the operating software of old product.
  - A manufacturer is bought out by another manufacturer. The buyer does not support old products sold.

(B) Risk to user of these products

- **Security:** This is the greatest risk due to IoT. As home devices / office equipment's are connected to network they shall be hit by all network related risks, including hacking, virus attacks, stealing confidential data etc.
- **Privacy, autonomy and control:** There is a huge risk that individuals may lose control over their personal life. Their personal life can be hacked and made public. The other major concern is who has the ownership of this personal data.

Example 4.8: A person daily eats a burger at 12.00 in night and takes bottle of chilled hard drink with it. S/he uses his/her mobile to operate the griller and refrigerator. The griller and refrigerator are both sold by say XYZ ltd. This data is available on database of XYZ Ltd.

- Who owns this information?
- The data can be used by insurance companies to deny an insurance claim saying the person was a habitual drinker or raise his/her medical insurance premium as the person is having a risky lifestyle.
- Above illustrates the big risk IoT may create for individuals.

(C) Technology Risk

Platform fragmentation and lack of technical standards are situations where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications tough.

(D) Environmental Risks due to Technology

The studies are being done to evaluate the impact on environmental resources like house air quality, soil etc. due to use of heavy earth metals in devices. Though, there is no definitive data available as of now, but the risk is being considered in term of resource depletion, harm to biodiversity, ecological balance disruption, nuclear and space waste etc.

4.8.9 Artificial Intelligence (AI)

I. Definition

Intelligence, as defined in Chambers dictionary; "The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgement to solve problems and adapt to new situations". The ability described above when exhibited by machines is called as **Artificial Intelligence (AI)**. It is intelligence exhibited by machines.

In other words, AI is an ability of a computer to stimulate human capabilities based on predetermined set of rules.

Example 4.9: Consider the following.

- AI has been used for image, video, and text recognition, as well as serving as the power behind recommendation engines. Apple online assistant Siri is a good example.
- This technology is being is being used in autonomous vehicles, the Google car.

Machine learning is the science and art of programming computers so that they can learn from data. It is a subset and application of AI that provides system the ability to automatically learn without being explicitly programmed. For example, spam filter is a machine learning program that can learn to flag spam e-mails and regular e-mails by automatically learning the words or phrases which are good predicators of spam by detecting unusually frequent pattern of words in the spam.

II. Applications

Artificial Intelligence is being used in many fields, some of them are placed below:

- Autonomous vehicles such as drones and self-driving cars.
- Medical diagnosis like in cancer research and predicting the chances of an individual getting ill by a disease.
- Creating art such as poetry by providing various suggestions to the writer.
- Playing games such as chess and predicting the outcomes say which number on a lottery ticket may win;
- Providing a real time quotation of export/import in finance application as the goods move to different stakeholders with different types and levels of risks.
- Providing the match results of asset sellers and needs of buyers through automated matching and enabling the service providers in learning the behavior pattern of its customers based on the available historical transactions.
- Detecting unusual credit card transactions to prevent frauds by training the system with normal instances. Whenever the system sees a new instance, it can notify whether it looks like a normal transaction, or it is likely to be abnormal such as multiple credits other than salary credit, many transactions with a few related accounts etc.
- Solving problems that either are too complex for traditional approaches or have no known algorithm such as speech recognition and proving mathematical theorems using Machine learning.
- Training human beings/users so that they can inspect machine learning algorithms to see what machines have learned. For example, once the spam filter has been trained on spam, it can be easily inspected to reveal the list of words and combinations of words that it believes are the predictors of spam. Sometimes this will reveal unsuspected correlations or new trends and thereby lead to better understanding of the problem.
- Helps in discovering hidden patterns in data through Data Mining. In case a company has lot of visitors to its website, it can detect group of

similar visitors using data mining tools. For example, an organization may notice that 40% of its website visitors are males who love comic books and generally visit the website in the evening and 20% of the visitors are females who love fashion-related books and generally visit the website in the afternoon, and so on. This information may help the organization in targeting their marketing efforts for each group.

III. Risks

1. AI relies heavily on the input data. The incorrect input data sets in machine learning systems lead to incorrect identification and knowledge, thus making it harder for AI based systems to deliver the correct results. No matter how advanced the analytical tools and algorithms are, the results might be disastrous if the input data is incorrect; thus, leading to incorrect conclusions and decisions.
2. With growing technology, there has been increased dependence of human beings on AI for various critical functions and services in different fields like medical, robotics, banking facilities etc. The attack on the AI algorithms may lead to severe threat and consequences to the security of these AI systems. Therefore, many countries are in consensus for the need of control measures so that in case of adversary, the AI machines can be inhibited from causing the disaster. For example - countries are discussing to have a KILL button in all AI capable machines otherwise someday machine may start controlling humans.
3. AI in long term may kill human skills of thinking the unthinkable. All data shall be processed in a structured manner, where machines shall provide solution based on their learning over a period. These machines shall not have capability of thinking out of box.

IV. Controls

The set of controls in AI will be extremely complex because of the nature of processing of information and must be dealt adequately based on the nature of the AI tool and the purpose, etc.

4.8.10 Blockchain

I. Definition

Blockchain, sometimes referred to as Distributed Ledger Technology (DLT) is a shared, peer-to-peer, and decentralized open ledger of

transactions system with no trusted third parties in between. This ledger database has every entry as permanent as it is an append-only database which cannot be changed or altered. All transactions are fully irreversible with any change in the transaction being recorded as new transaction. The decentralised network refers to the network which is not controlled by any bank, corporation, or government. A blockchain generally uses a chain of blocks, with each block representing the digital information stored in public database ("the chain").

A simple analogy for understanding blockchain technology is a Google Doc. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the document are being recorded in real-time, making changes completely transparent. Fig. 4.8.8 represents the working of any Blockchain transaction.

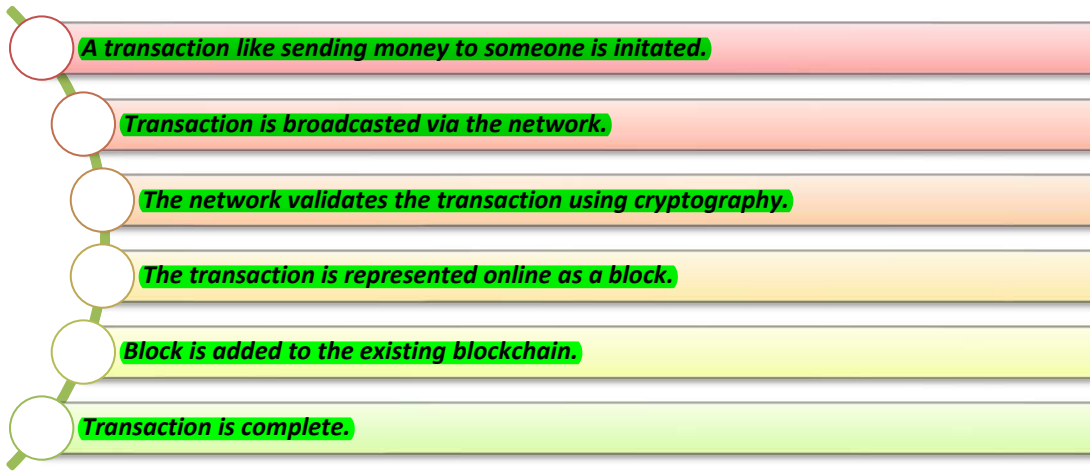


Fig. 4.8.8: Blockchain working

II. Applications

Some initiatives that are already existing in various fields like financial services, healthcare, government, travel industry, economic forecasts etc. are discussed below:

- *Financial Services: Blockchain can be used to provide an automated trade lifecycle in terms of the transaction log of any transaction of asset or property - whether physical or digital such*

as laptops, smartphones, automobiles, real estate, etc. from one person to another.

- ***Healthcare:*** *Blockchain provides secure sharing of data in healthcare industry by increasing the privacy, security, and interoperability of the data by eliminating the interference of third party and avoiding the overhead costs.*
- ***Government:*** *At the government front, there are instances where the technical decentralization is necessary but politically should be governed by governments like land registration, vehicle registration and management, e-voting etc. Blockchain improves the transparency and provides a better way to monitor and audit the transactions in these systems.*
- ***Travel Industry:*** *Blockchain can be applied in money transactions and in storing important documents like passports/other identification cards, reservations and managing travel insurance, loyalty, and rewards thus, changing the working of travel and hospitality industry.*
- ***Economic Forecasts:*** *Blockchain makes possible the financial and economic forecasts based on decentralized prediction markets, decentralized voting, and stock trading, thus enabling the organizations to plan and shape their businesses.*

III. Risks

- *With the use of blockchain, organizations need to consider risks with a wider perspective as different members of a particular blockchain may have different risk appetite/risk tolerances that may further lead to conflict when monitoring controls are designed for a blockchain. There may be questions about who is responsible for managing risks if no one party is in-charge and how proper accountability is to be achieved in a blockchain.*
- *The reliability of financial transactions is dependent on the underlying technology and if this underlying consensus mechanism has been tampered with, it could render the financial information stored in the ledger to be inaccurate and unreliable.*
- *In the absence of any central authority to administer and enforce protocol amendments, there could be a challenge in the establishment of development and maintenance of process control*

activities and in such case, users of public blockchains find difficult to obtain an understanding of the general IT controls implemented and the effectiveness of these controls.

- As blockchain involves humongous data getting updated frequently, risk related to information overload could potentially challenge the level of monitoring required. Furthermore, to find competent people to design and perform effective monitoring controls may again prove to be difficult.

IV. Controls

Though there could be many ways, however, some activities that may help in mitigating the possible threats and risks to blockchain are as follows:

- As opposed to traditional manual techniques, computerized continuous monitoring techniques shall be used to perform ongoing evaluations, considering the large volume of data processed and the frequency at which these transactions are getting processed.
- Suitable data analytics procedures shall be developed to identify and obtain relevant and quality data from the blockchain so that it can then be processed into information that subsequently can be used to support management's business processes and reporting objectives.
- Communication methods shall be developed to ensure that operational changes and updates relating to the use of blockchain are communicated to appropriate personnel so that internal control related responsibilities are carried out in proper manner.
- The unique aspects of blockchain such as consensus protocols, smart contracts, and private keys, as well as factors relating to the ongoing health, governance, and overall reliability of the blockchain in use; shall be assessed thoroughly.
- Both internal and external auditors shall be engaged in discussions during the development or identification of a blockchain so as to make the management understand the typical auditability issues associated with using blockchain. Subsequently, processes can be established to mitigate against those issues so that the appropriate information and support for transactions is available.

CHAPTER 5

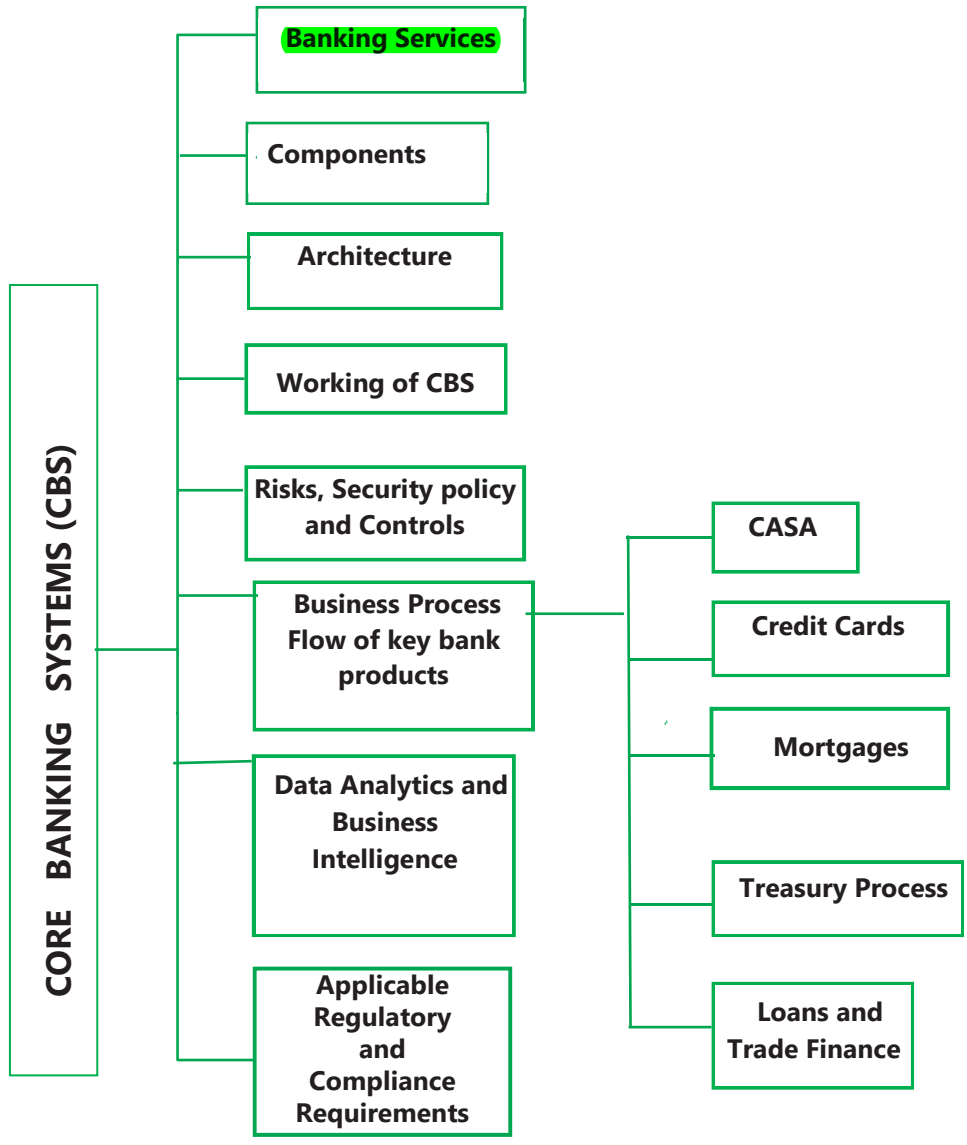
CORE BANKING SYSTEMS

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Understand components and architecture of Core Banking System (CBS) and impact of related risks and controls.
- Acknowledge the functioning of core modules of banking and business process flow and impact of related risks and controls.
- Comprehend regulatory and compliance requirements applicable to CBS such as
  - Banking Regulations Act,
  - RBI regulations,
  - Prevention of Money Laundering Act, 2002 and
  - Information Technology Act, 2000.

CHAPTER OVERVIEW



moving over to Core Banking System and IT-based operations have abled banks to reach customers and facilitate seamless transactions with lesser dependence on physical infrastructure. This has resulted in all the core functions at the branches, such as loan processing and sanctioning, safe keeping of security documents, post sanction monitoring and supervision of borrower's accounts, accounting of day-to-day transactions, receipts and payments of cash/cheques and updating passbooks/statements, being either centralized or made online or with the use of ATMs. The accounting transactions and all services of the banks are being done from a central server using core banking solutions. This is changing the modus operandi of how banking services are delivered to customers by using alternate delivery channels such as ATM, Internet Banking and Mobile Banking.

5.1.2 Overview of Banking Services

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:

- As the custodian of large volumes of monetary items including cash and negotiable instruments, the banks need to ensure their physical security.
- The banks deal in large volume of data in terms of number, value, and variety of transactions.
- The banks need to operate through a wide network of their geographically dispersed branches and departments.
- There is an increased possibility of frauds as banks directly deals with money making. Therefore, its mandatory for banks to provide multi-point authentication checks and the highest level of information security.

Some of the major products and services provided and rendered by commercial banks which constitute core banking services are briefly explained here in the Fig 5.1.1.

I. Acceptance of Deposits

Deposits involve deposits made by customers in various schemes for pre-defined periods. Deposits fuel the growth of banking operations; this is the most important function of a commercial bank. Commercial banks accept deposits in various forms such as term deposits, savings bank deposits,

a potential borrower. During this stage of the loan process, an underwriter checks the borrower's ability to repay the loan based on an analysis of his/her credit history, value of collateral provided and capacity. Underwriting typically happens behind the scenes, but it is a crucial aspect of loan approvals.

- **Life Insurance:** Life Insurance can be defined as a contract between an insurance policy holder and an insurance company, where the insurer promises to pay a sum of money in exchange for a premium, upon the death of an insured person or after a set period.
- ***Non-life Insurance:* Insurance contracts that do not come under the ambit of life insurance are called Non-life or General Insurance. As the tangible assets like home, vehicle etc. are susceptible to damages, the general insurance provides protection against unforeseeable contingencies like loss of the asset due to fire, marine, motor, accident etc.**

Note: The Fig. 5.1.1 includes some non-banking services such as claims, insurance, etc. which may be done by the bank or an independent subsidiary. All banks may not carry all given services as these are not core banking activities. Some services such as insurance, underwriting, etc. may be done through separate subsidiaries.

5.1.3 Overview of Core Banking Systems (CBS)

Core Banking System/Solution (CBS) refers to a common IT solution wherein a central shared database supports the entire banking application. It allows the customers to use various banking facilities irrespective of the bank branch location. The characteristics of CBS are as follows:

- CBS is a centralized Banking Application software that has several components which have been designed to meet the demands of the banking industry.
- CBS is supported by advanced technology infrastructure and has high standards of business functionality.
- There is a common database in a central server located at a Data Center, which gives a consolidated view of the bank's operations.
- Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch.

- CBS is modular in structure and is capable of being implemented in stages as per requirements of the bank.
- All branches of bank function as delivery channels providing services to its customers.
- A CBS software enables integration of all third-party applications including in-house banking software to facilitate simple and complex business processes.

Example 5.1: Some CBS software are given below. These are only illustrative and not exhaustive.

- **Finacle:** It is a core banking software suite developed by Infosys that provides universal banking functionality covering all modules for banks covering all banking services.
- **FinnOne:** This is a web-based global banking product designed to support banks and financial solution companies in dealing with assets, liabilities, core financial accounting and customer service.
- **Flexcube:** It is an automated, comprehensive, integrated, interoperable, and modular solution developed by Oracle Financial Services that enables banks to manage evolving customer expectations.
- **BaNCS:** It is a customer-centric business model which offers simplified operations comprising loans, deposits, wealth management, digital channels and risk and compliance components.
- **bankMate:** It is a full-scale banking solution which is scalable and integrated e-banking system that meets the deployment requirements in traditional and non-traditional banking environments. It enables communication through any touch point to provide full access to provide complete range of banking services with anytime, anywhere paradigm.

Further, there are many CBS software developed by vendors which are used by smaller and co-operative banks. Some of the banks have also developed in-house CBS software. However, the trend is for using high-end CBS developed by vendors depending on cost-benefit analysis and needs.

Core Banking Solution has become a mandatory requirement to provide a range of services demanded by customers and the competitive banking environment. This requires that most of bank's branches access applications from centralized data centers. CBS for a bank, functions not only as a heart (circulatory system) but also as a brain (nervous system). All transactions flow through these core systems,

which, at an absolute minimum, must remain running and responsive during business hours. These systems are usually running 24x7 to support Internet banking, global operations, and real time transactions via ATM, Internet, mobile banking, etc. Key modules of CBS are given in the Fig. 5.1.2:

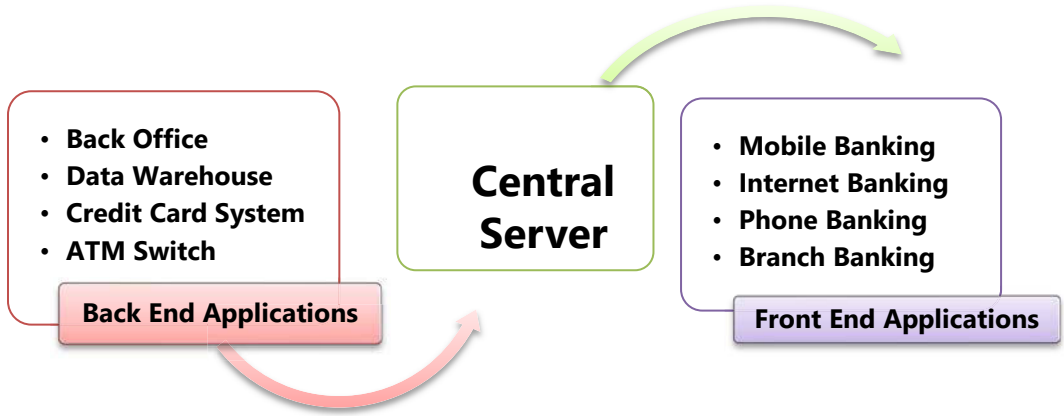


Fig. 5.1.2: Key Modules of CBS

We may recall from Chapter 2 that the **Front End** is a part of the overall application which interacts with the user who is using the software whereas the **Back End** is a part of the overall software that does not interact with the user but interact with front end only. Fig. 5.1.2 is a simple diagram illustrating how most of the key modules of bank are connected to a common central server. In the case of a CBS, at the core is **Central Server**. All key modules of banking such as back office, data warehouse, ATM switch, mobile banking, internet banking, phone banking and credit-card system etc. are all connected and related transactions are interfaced with the central server and are explained below:

- **Back Office:** The Back Office is the portion of a company made up of administration and support personnel, who are not client-facing. Back-office functions include settlements, clearances, record maintenance, regulatory compliance, accounting and IT services. Back office professionals may also work in areas like monitoring employees' conversations and making sure they are not trading forbidden securities on their own accounts.
- **Data Warehouse:** Banking professionals use data warehouses to simplify and standardize the way they gather data - and finally get to one clear version of the truth. Data warehouses take care of the difficult data management - digesting large quantities of data and ensuring accuracy - and make it easier for professionals to analyze data.

deployed by the Banks as a part of the CBS Project includes Data Centre (DC) and the Disaster Recovery Centre (DRC). With the introduction to core banking systems, a customer is not only having accessibility with the branch but to the bank.

The key technology components of CBS are as follows:

- **Database Environment:** This consists of the centrally located database servers that store the data for all the branches of the bank which includes customer master data, interest rates, account types etc. Whenever a customer requests for a particular service to be performed, the application server performs a particular operation it updates the central database server. The databases are kept very secure to prevent any unauthorized changes.
- **Application Environment:** In general, Application environment consist of the application servers that host the different core banking systems like Flex Cube, bankMate etc. and is centrally used by different banks. The access to these application servers will generally be routed through a firewall.
- ***Cyber Security: Comprehensive Cyber Security Framework is prescribed by RBI for Banks to ensure effective information security governance. Some key features of Cyber Security Framework as prescribed by are RBI for banks are as under:***

(i) ***Network Security and Secure Configuration: The following key measure are required to be implemented:***

- ***Multi-layered boundary defense through properly configured proxy servers, firewalls, intrusion detection systems to protect the network from any malicious attacks and to detect any unauthorized network entries.***
- ***Different LAN segments for in-house/onsite ATM and CBS/branch network to confirm the adequacy of bandwidth to deal with the volume of transactions so as to prevent slowing down and resulting in lower efficiency.***
- ***To ensure secure network configuration; proper usage of routers, hubs and switches should be envisaged.***
- ***Periodic security review of systems and terminals to assess the network's vulnerability and identify the weaknesses.***
- ***Identification of the risks to ensure that risks are within the bank's risk appetite and are managed appropriately.***

(ii) ***Application Security:*** *Full-fledged Security policy to ensure Confidentiality, Integrity and Availability (CIA) of data and information needs to be development and implemented covering following key features:*

- *Implementation of bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing (security measures to prevent steal of user data) and anti-malware software (software tool/program to identify and prevent malicious software/malware from infecting network) with controls enforced at the email solution.*
- *Two factor authentication, an extra step added to the log-in process, such as a code sent to user's phone or a fingerprint scan, that helps verify the user's identity and prevent cybercriminals from accessing private information.*
- *Implementation of Password Management policy to provide guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.*
- *Effective training of employees to educate them to strictly avoid clicking any links received via email.*
- *Proper reporting mechanism to save the banks from the effects of misconduct – including legal liability, lasting reputational harm, and serious financial losses.*
- *Required to conduct effective due diligence and oversight to thoroughly assess the credentials of vendors/third party service providers/partners and making non-disclosure and security policy compliance agreements mandated for them.*
- *Effective change management process to record/ monitor all the changes that are moved/ pushed into production environment.*
- *Robust configuration management processes to register changes to business applications, supporting technology, service components and facilities.*
- *Incident response and management mechanism to take appropriate action in case of any cyber security incident with well written incident response procedures elaborating the roles of staff handling such incidents.*
- *Capturing of the audit logs pertaining to user actions and an alert mechanism to monitor any change in the log settings.*

- ***Continuous surveillance to stay regularly updated on the latest nature of emerging cyber threats.***

(iii) Data Centre and Disaster Recovery Centre: The core banking systems consist of a Data Centre which includes various application servers, database servers, web servers etc. and various other technological components. The bank should adopt full-fledged documentation and prepare necessary manuals dealing with the disaster recovery procedures. Arrangements for alternate connectivity of the banks with the data center should be established whenever there is a disruption in the primary connectivity. Proper awareness should be created among the employees through periodic trainings and mock drills.

(iv) Online Transaction monitoring for fraud risk management: Risk evaluations are carried out and considering the risk profile and other regulatory requirements of the bank, effective monitoring should be done as a part of managing fraud risk management across all delivery channels. There are also methods that facilitate fraud reporting in CBS environment. Proper alert system should be enabled to identify any changes in the log settings and the audit logs pertaining to user actions are captured.

Some key aspects in-built into architecture of a CBS are as follows:

- **Information flow:** This facilitates information flow within the bank and improves the speed and accuracy of decision-making. It deploys systems that streamline integration and unite corporate information to create a comprehensive analytical infrastructure. It ensures various interfaces like payment channels, ATM, mobile/internet banking, Point of Sale (PoS) capability are readily available.
- **Customer centric:** Through a holistic core banking architecture, this enables banks to target customers with the right offers at the right time with the right channel to increase profitability.
- **Regulatory compliance:** This holds the compliance for banks which is complex and expensive. CBS has built-in and regularly updated regulatory platform which will ensure compliance by providing periodic regulatory and compliance reports required for the day-to-day operations of the bank.
- **Resource optimization:** This optimizes utilization of information and resources of banks and lowers costs through improved asset reusability, faster turnaround times, faster processing, and increased accuracy.

- **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.

5.3 CBS RISKS, SECURITY POLICY AND CONTROLS

5.3.1 Risks associated with CBS

Risk Management: Risks are all pervasive in the banking sector. This should be done at strategic, tactical, operational and technology areas of the bank. Risk management is best driven as per policy with detailed standards, procedures and guidelines provided for uniform implementation.

(a) **Operational Risk:** It is defined as a risk arising from direct or indirect loss to the bank which could be associated with inadequate or failed internal process, people and systems. For example- Inadequate audits, improper management, ineffective internal control procedures etc. The components of operational risk include transaction processing risk, information security risk, legal risk, compliance risk and people risk and necessarily excludes business risk and strategic risk.

- **Transaction Processing Risk** arises because faulty reporting of important market developments to the bank management may occur due to errors in entry of data for subsequent bank computations.
- **Information Security Risk** comprises the impact to an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate. Data breaches can cost a bank its reputation, customers can lose time and money and above all their confidential information.
- **Legal Risk** arises because of the treatment of clients, the sale of products, or business practices of a bank. There are countless examples of banks being taken to court by disgruntled corporate customers, who claim they were misled by advice given to them or business products sold. Contracts with customers may be disputed.

- **Authorization process:** What is the authorization process, if anybody with access to the CBS, including the customer himself, can enter data directly. If the process is not robust, it can lead to unauthorized access to the customer information.
- **Authentication procedures:** Usernames and Passwords, Personal Identification Number (PIN), One Time Password (OTP) are some of the most commonly used authentication methods. However, 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 interfaces and application software. A data center must also contain adequate infrastructure such as power distribution and supplemental power subsystems including electrical switching; uninterruptable power supplies; backup generators and so on. Lapse in any of these may lead to real-time data loss.
- **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 and therefore every user's identity and his/her level of access to a particular system need to be verified.
- **Access Controls:** Designing and monitoring access control is an extremely challenging task. Bank environments are subject to all types of attacks; thus a strong access control system is a crucial part of a bank's overall security plan. Access control, however, does vary between branch networks and head office locations.
- **Incident handling procedures:** Incident handling procedures are used to address and manage the aftermath of a security breach or cyberattack. However, these at times, may not be adequate considering the need for real-time risk management.
- **Change Management:** Though change management reduces the risk that a new system or other change will be rejected by the users; however, at the same time, it requires changes at application level and data level of the database - Master files, transaction files and reporting software.

5.3.2 Security Policy

Large corporations like banks, financial institutions need to have a laid down framework for security with properly defined organizational structure. This helps banks create whole security structure with clearly defined roles, responsibilities within the organization. Banks deal in third party money and need to create a framework of security for its systems. This framework needs to be of global standards to create trust in customers in and outside India.

Information Security

Information security is critical to mitigate the risks of Information technology. Security refers to ensure Confidentiality, Integrity and Availability of information. RBI has suggested use of ISO 27001: 2013 implement information security. Banks are also advised to obtain ISO 27001 Certification. Many banks have obtained such certification for their data centers. Information security is comprised of following sub-processes:

- **Information Security Policies, Procedures and practices:** This refers to the processes relating to approval and implementation of information security. The security policy is basis on which detailed procedures and practices are developed and implemented at various units/department and layers of technology, as relevant. These cover all key areas of securing information at various layers of information processing and ensure that information is made available safely and securely. Unauthorized access to information often occurs due to improperly understood poor or unorganized security practices. For example – Non-disclosure agreement with employees, vendors etc., KYC procedures for security.
- **User Security Administration:** This refers to security for various users of information systems. The security administration policy documents define how users are created and granted access as per organization structure and access matrix. It also covers the complete administration of users right from creation to disabling of users is defined as part of security policy.
- **Application Security:** This refers to how security is implemented at various aspects of application right from configuration, setting of parameters and security for transactions through various application controls. For example – Event Logging.
- **Database Security:** This refers to various aspects of implementing security for the database software. For example - Role based access privileges given to employees.

- Exception situations such as limit excess, reactivating dormant accounts, etc. can be handled only with a valid supervisory level password.
- A user timeout is prescribed. This means that after a user logs-in and there is no activity for a pre-determined time, the user is automatically logged out of the system.
- Once the end-of-the-day process is over, the ledgers cannot be opened without a supervisory level password.

(c) Controls in Banks' Application Software

Application Software whether it is a high-end CBS software, ERP software or a simple accounting software, have primarily four gateways through which enterprise can control functioning, access and use the various menus and functions of the software. These are **Configuration**, **Masters**, **Transactions** and **Reports**.

(Details of concepts of Configuration, Masters, Transactions have already been discussed in Chapter 1 in detail).

Example 5.3: Configuration - Some examples of configuration in the context of CBS software are given here:

- Defining access rules from various devices/terminals;
- Creation of User Types;
- Creation of Customer Type, Deposit Type, year-end process;
- User Access & privileges - Configuration and its management; and
- Password Management

Example 5.4: Masters - Some examples of masters in context of CBS software are as follows:

- **Customer Master:** Customer type, details, address, PAN details,
- **Employee Master:** Employee Name, Id, designation, level, joining details, salary, leave, etc.
- **Income Tax Master:** Tax rates applicable, Slabs, frequency of TDS, etc.

Example 5.5: Transactions - Some examples of transactions in the context of CBS software are given here:

- **Deposit transactions:** Opening of account, deposits, withdrawals, interest computation, etc.

- **Top Up Loan:** Here the customer already has an existing loan and is applying for additional amount either for refurbishment or renovation of the house.
- **Loans for Under Construction Property:** In case of under construction properties, the loan is disbursed in tranches/parts as per construction plan.

Mortgage loans are conventionally the loans that one can use to buy or refinance a home. Due to the evolution in Banking industry, various other Mortgage Loans like Loan against residential property, Loan against commercial property, Loan against agricultural property, Loan against property etc. now exist apart from the ones that are discussed above.

(b) Process Description (as shown in the Fig. 5.4.4)

(i) Loans are provided by the lender which is a financial institution such as a bank or a mortgage company. There are two types of loan widely offered to customer - first is **Fixed Rate Mortgage** where rate of interest remains constant for the life of the loan and second is **Variable/Floating Rate Mortgage** where rate of interest is fixed for a period but then it fluctuates with the market interest rates.

(ii) Borrower/Customer approaches the bank for a mortgage and relationship manager/loan officer explains the customer about home loan and its various features. Customer fills the loan application and provide requisite KYC documents (Proof of Identity, Address, Income, and obligation details etc.) to the loan officer.

(iii) Loan officer reviews the loan application and sends it to Credit risk team who will calculate the financial obligation income ratio which is to determine customer's financial eligibility on how much loan can be provided to the customer. This is done basis the credit score as per Credit Information Bureau (India) Limited (CIBIL) rating, income and expense details and Rate of Interest at which loan is offered. Once financial eligibility is determined, then along with customer documents the details are sent to the underwriting team for approval.

(iv) Underwriting team will verify the financial (applicant's credit history) and employment information of the customer. Underwriter will ensure

deposits and withdrawals to continually vary the amount of money in the accounts, changing the money's currency, purchasing high-value items (boats, houses, cars, diamonds) to change the form of money. This step is quite complex as it involves making the 'dirty' money as hard to trace as possible.

3. Integration

Integration involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations. Integration creates the illusion of a legitimate source for criminally derived funds and involves techniques as numerous and creative as those used by legitimate businesses. For example, false invoices for goods exported, domestic loan against a foreign deposit, purchasing of property and commingling of money in bank accounts.

II. Anti-Money laundering (AML) using Technology

Negative publicity, damage to reputation and loss of goodwill, legal and regulatory sanctions and adverse effect on the bottom line are all possible consequences of a bank's failure to manage the risk of money laundering. Banks face the challenge of addressing the threat of money laundering on multiple fronts as banks can be used as primary means for transfer of money across geographies. The challenge is even greater for banks using CBS as all transactions are integrated. With regulators adopting stricter regulations on banks and enhancing their enforcement efforts, banks are using special fraud and risk management software to prevent and detect fraud and integrate this as part of their internal process and daily processing and reporting.

III. Financing of Terrorism

Money to fund terrorist activities moves through the global financial system via wire transfers in and out of personal and business accounts. The money can lie in the accounts of illegitimate charities and be laundered through buying and selling securities and other commodities or purchasing and cashing out insurance policies. Although terrorist financing is a form of money laundering, it does not work the way conventional money laundering works. The money frequently starts out clean i.e. as a 'charitable donation' before moving to terrorist accounts. It is highly time sensitive requiring quick response.

As per compliance requirements of (PMLA) The Prevention of Money Laundering Act ***(discussed in later part of the chapter)***, CBS software should

The Act gives the Reserve Bank of India (RBI) the power to license banks, have regulation over shareholding and voting rights of shareholders; supervise the appointment of the boards and management; regulate the operations of banks; lay down instructions for audits; control moratorium, mergers and liquidation; issue directives in the interests of public good and on banking policy, and impose penalties. In 1965, the Act was amended to include cooperative banks under its purview by adding the Section 56. Cooperative banks, which operate only in one state, are formed and run by the state government. But RBI controls the licensing and regulates the business operations. The Banking Act was a supplement to the previous acts related to banking.

RBI has been proactive in providing periodic guidelines to banking sector on how IT is deployed. It also facilitates banks by providing specific guidelines on technology frameworks, standards and procedures covering various aspects of functioning and computerization of banks in India. RBI also provides the technology platform for NEFT/ RTGS and other centralized processing from time to time.

I. 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 (digitalization of a physical paper cheque into a substitute electronic form for transmission to the paying bank) 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.

A cheque in the electronic form has been defined as 'a mirror image' of a paper cheque. The expression 'mirror image' is not appropriate. It is perhaps not even the intention that a cheque in the electronic form should look like a paper cheque as seen in the mirror. Further, requiring a paper cheque being written first and then its mirror image or electronic image being generated does not appear to have been contemplated as the definition requires generation, writing and signature in a secure system etc. The expression, 'mirror image of' may be substituted by the expression, electronic graphic which looks like' or any other expression that captures the intention adequately.

The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year 2000, it is understandable that it has captured only digital signature and asymmetric crypto system dealt with

the conduct of the business of the company as well as the company, shall be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of any company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation 1 - For the purposes of this section -

(i) "**company**" means anybody corporate and includes a firm or other association of individuals; and

(ii) "**director**", in relation to a firm, means a partner in the firm.

Explanation 2 - For the removal of doubts, it is hereby clarified that a company may be prosecuted, notwithstanding whether the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

IV. Information Technology Act, 2000

The Information Technology Act (ITA) was passed in 2000 and amended in 2008. The ITA 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 cyber-crime and facilitates electronic commerce. It also defined cyber-crimes and prescribed penalties for them. The

Sanjay Khemka Classes
Moulding Lives....

Classes Available In
Google Drive | Pendrive | Mobile App

CA SANJAY KHEMKA

Specialist in Finance & IT

Mentored More than 15,000 students

KEY SUBECTS

- SFM
- Risk Management
- Enterprise Information System
- Strategic Management
- Financial Management
- Economics For Finance

CA | CMA Finals | Inter