

AMENDMENTS IN EIS

CHAPTER-1

AUTOMATED BUSINESS PROCESSES

1. Explain the link of various business processes with vision and mission.

The key guiding factor for any business process shall be top management vision and mission. This vision and mission shall be achieved through implementing Operational Support and Management services. These are referred to as categories of business process.

Example 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 was Rs. 10,000/- Crores.
2	Management Process	The top management sat down and listed activities to be done to achieve the said turnover. This included: <ul style="list-style-type: none"> - Enter into new markets. It was decided to have an all India presence. At present the company products were being sold across 20 out of 25 states and all state capital excluding the four metros, namely Delhi, Mumbai, Chennai and Kolkata. - Launch new products. Presently the company was mainly selling milk products. Few new products that were decided to be sold in future included; Biscuits, Toast, Atta, Packaged Drinking Water. - Acquire existing dairies in markets where company had no presence.
3	Support Process	For all activities to be done as envisioned by top management, a huge effort was needed on human resources front. This included - <ul style="list-style-type: none"> - Defining and creating a new management structure - Performing all human resource activities as listed above.
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.

2. Explain various types of risks.

The risks broadly can be categorized as follows:

A. Business Risks: Businesses face all kinds of risks related from serious loss of profits to even bankruptcy and are discussed below:

- **Strategic Risk:** These are the risks that would prevent an organization from accomplishing its objectives (meeting its goals). Examples include risks related to strategy, political, economic, regulatory, and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs
- **Financial Risk:** Risk that could result in a negative financial impact to the organization (waste or loss of assets). Examples include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.
- **Regulatory (Compliance) Risk:** Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations. Examples include Violation of laws or regulations governing areas such as environmental, employee health and safety, protection of personal data in accordance with global data protection requirements and local tax or statutory laws.
- **Operational Risk:** Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations. Examples include risks related to the organization's human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration.
- **Hazard Risk:** Risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.
- **Residual Risk:** Any risk remaining even after the counter measures are analyzed and implemented is called Residual Risk. 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 (covered in chapter 5)

C. Data Risks (covered in chapter 3)

3. Explain several terms like Assets, Vulnerability, Threat, Exposure, Counter Measure, Risk, etc.

Risk Management and Related Terms

Various terminologies relating to risk management are given as follows:

Risk Management: 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.

Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. 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.

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 (e.g. 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 given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- ‘Allows an attacker to execute commands as another user’ or
- ‘Allows an attacker to access data that is contrary to the specified access restrictions for that data’ or
- ‘Allows an attacker to pose as another entity’ or
- ‘Allows an attacker to conduct a denial of service’.

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.

Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example - loss of business, failure to perform the system’s mission, loss of reputation, violation of privacy and loss of resources etc.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

Attack: An attack is an attempt to gain unauthorized access to the system’s services or to compromise the system’s dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system. Basically, it is a set of actions designed to compromise CIA (Confidentiality, Integrity or Availability), or any other desired feature of an information system. Simply, it is the act of trying to defeat Information Systems (IS) safeguards. The type of attack and its degree of success determines the consequence of the attack.

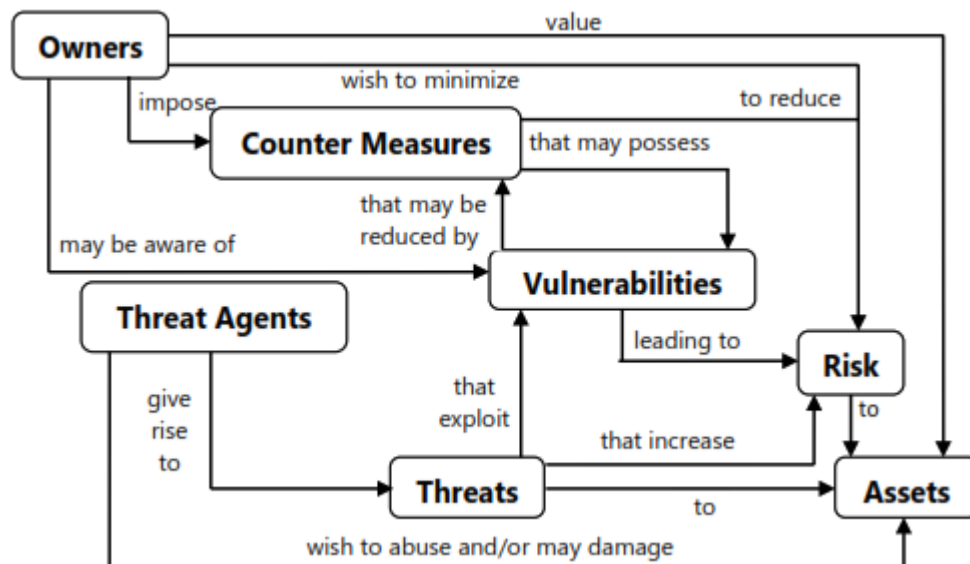


Fig. 1.4.1: Risk and Related Terms

Counter Measure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure. For example, well known threat ‘spoofing the user identity’, has two countermeasures:

- Strong authentication protocols to validate users; and
- Passwords should not be stored in configuration files instead some secure mechanism should be used.

Similarly, for other vulnerabilities, different countermeasures may be used.

The relationship and different activities among these terms may be understood by the Fig.

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

4. Explain various Risk Management Strategies

When risks are identified, and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated below:

- **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, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** 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.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

CHAPTER-2

FINANCIAL AND ACCOUNTING SYSTEMS

1. Explain difference between Installed and Cloud Based Applications.

Cloud Applications: These days many organizations do not want to install Financial Applications on their own IT infrastructure. For many organizations, the thought process is that it is not their primary function to operate complex IT systems and to have a dedicated IT team and hardware which requires hiring highly skilled IT resources and to maintain the hardware and software to run daily operations. The costs may become prohibitive. Thus, organizations increasingly are hosting their applications on Internet and outsource the IT functions. There are many methods through which this can be achieved. Most common among them being SaaS – Software as a Service or IaaS – Infrastructure as a Service.

Table 2.2.5: Installed and Cloud Based Applications

Particulars	Installed Application	Cloud Based Application
Installation and Maintenance	As software is installed on hard disc of the computer used by user, it needs to be installed on every computer one by one. This may take lot of time. Also, maintenance and updating of software may take lot time and efforts.	Installation on user computer is not required. Update and maintenance are defined responsibility of service provider.
Accessibility	As software is installed on the hard disc of the user's computer, user needs to go the computer only, i.e. the computer where software is installed, to use the software. It cannot be used from any computer.	As software is available through online access, to use the software a browser and an internet connection is needed. It can be used from any computer in the world. Access to the software becomes very easy. Also, it can be used 24 x 7.
Mobile Application	Using the software through mobile application is difficult in this case.	Mobile application becomes very easy as data is available 24x7. As technology evolves mobile technology is becoming an industry norm. That makes cloud based application future oriented.
Data Storage	Data is physically stored in the	Data is not stored in the user's

	premises of the user, i.e. on the hard disc of the user's server computer. Hence user will have full control over the data.	server computer. It is stored on a web server. Ownership of data is defined in Service Level Agreement (SLA). SLA defines the rights, responsibilities and authority of both service provider and service user.
Data Security	As the data is in physical control of the user, user shall have the full physical control over the data and he/she can ensure that it is not accessed without proper access.	Data security is a challenge in case of cloud based application as the data is not in control of the user or owner of data. As time evolves; SLAs provides for details of back-up, disaster recovery alternatives being used by service provider.
Performance	A well written installed application shall always be faster than web application, reason being data is picked from local server without internet.	Access is dependent on speed of internet. Slow internet slows access to information and may slow operations.
Flexibility	It shall have more flexibility and controls as compared to web application. It is very easy to write desktop applications that take advantage of the user's hardware (such as: scanners, cameras, Wi-Fi, serial ports, network ports, etc.). Installed applications have this dis-advantage of higher capital expenditure (CAPEX) in comparison to cloud based application.	The success of cloud based applications is that they allow flexibility against both capital expenditure (CAPEX) and Operating Expense (OPEX) to the user. User can scale up operations as per need.

2. Explain benefits of an ERP System

- **Information integration:** The reason ERP systems are called integrated is because they possess the ability to automatically update data between related business functions and components. For example - one needs to only update the status of an order at one place in the order-processing system; and all the other components will automatically get

updated.

- **Reduction of lead-time:** The elapsed time between placing an order and receiving it is known as the Lead-time. The ERP Systems by virtue of their integrated nature with many modules like Finance, Manufacturing, Material Management Module etc.; the use of the latest technologies like EFT (Electronic Fund Transfer), EDI (Electronic Data Interchange) reduce the lead times and make it possible for the organizations to have the items at the time they are required.
- **On-time Shipment:** Since the different functions involved in the timely delivery of the finished goods to the customers- purchasing, material management production, production planning, plant maintenance, sales and distribution – are integrated and the procedures automated; the chances of errors are minimal and the production efficiency is high. Thus, by integrating the various business functions and automating the procedures and tasks the ERP system ensures on-time delivery of goods to the customers.
- **Reduction in Cycle Time:** Cycle time is the time between placement of the order and delivery of the product. In an ERP System; all the data, updated to the minute, is available in the centralized database and all the procedures are automated, almost all these activities are done without human intervention. This efficiency of the ERP systems helps in reducing the cycle time.
- **Improved Resource utilization:** The efficient functioning of the different modules in the ERP system like manufacturing, material management, plant maintenance, sales and distribution ensures that the inventory is kept to a minimum level, the machine down time is minimum and the goods are produced only as per the demand and the finished goods are delivered to the customer in the most efficient way. Thus, the ERP systems help the organization in drastically improving the capacity and resource utilization.
- **Better Customer Satisfaction:** Customer satisfaction means meeting or exceeding customers 'requirements for a product or service. With the help of web-enabled ERP systems, customers can place the order, track the status of the order and make the payment sitting at home. Since all the details of the product and the customer are available to the person at the technical support department also, the company will be able to better support the customer.
- **Improved Supplier Performance:** ERP systems provide vendor management and procurement support tools designed to coordinate all aspects of the procurement process. They support the organization in its efforts to effectively negotiate, monitor and control procurement costs and schedules while assuring superior product quality. The supplier management and control processes are comprised of features that will help the

organization in managing supplier relations, monitoring vendor activities and managing supplier quality.

- **Increased Flexibility:** ERP Systems help the companies to remain flexible by making the company information available across the departmental barriers and automating most of the processes and procedures, thus enabling the company to react quickly to the changing market conditions.
- **Reduced Quality Costs:** Quality is defined in many different ways- excellence, conformance to specifications, fitness for use, value for the price and so on. The ERP System's central database eliminates redundant specifications and ensures that a single change to standard procedures takes effect immediately throughout the organization. The ERP systems also provide tools for implementing total quality management programs within an organization.
- **Better Analysis and Planning Capabilities:** Another advantage provided by ERP Systems is the boost to the planning functions. By enabling the comprehensive and unified management of related business functions such as production, finance, inventory management etc. and their data, it becomes possible to utilize fully many types of Decision Support Systems (DSS) and simulation functions, what-if analysis and so on; thus, enabling the decision-makers to make better and informed decisions.
- **Improved information accuracy and decision-making capability:** The three fundamental characteristics of information are accuracy, relevancy and timeliness. The information needs to be accurate, relevant for the decision-maker and available to the decision-makers when he requires it. The strength of ERP Systems- integration and automation – help in improving the information accuracy and help in better decision-making.
- **Use of Latest Technology:** ERP packages are adapted to utilize the latest developments in Information Technology such as open systems, client/server technology, Cloud Computing, Mobile computing etc. It is this adaptation of ERP packages to the latest changes in IT that makes the flexible adaptation to changes in future development environments possible.

3. Explain Risks and corresponding Controls related to People Issues

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

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

	<p>The way in which organization functions will change, the planning, forecasting and decision-making capabilities will improve, information integration happening etc.</p> <p>Changing the scope of the project is another problem.</p>	<p>ERP System should be provided so that the transition from old system to ERP system is smooth and hassle free.</p> <p>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.</p> <p>This requires clear defining of change control procedures and holds everyone to them.</p>
Training	<p>Since the greater part of the raining takes place towards the end of the ERP implementation cycle, management may curtail the training due to increase in the overall cost budget.</p>	<p>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 package vendors.</p>
Staff Turnover	<p>As the overall system is integrated and connected with each other department, it becomes complicated and difficult to understand. Employee turnover – qualified and skilled personnel leaving the company – during the implementation and transition phases can affect the schedules and result in delayed implementation and cost overrun.</p>	<p>This can be controlled and minimized by allocation of employees to tasks matching their skill-set; fixing of compensation package and other benefits accordingly- thus keeping the employees happy and content and minimizing the staff turnover.</p>
Top Management Support	<p>ERP implementation will fail if the top management does not provide the support and grant permission for the availability of the huge resources that are required during the transition.</p>	<p>The ERP implementation shall be started only after the top management is fully convinced and assure of providing the full support.</p>
Consultants	<p>These are experts in the implementation</p>	<p>The consultants should be</p>

	of the ERP package and might not be familiar with the internal workings and organizational culture.	assigned a liaison officer – a senior manager – who can familiarize them with the company and its working.
--	---	--

2. Process Risks: One of the main reason for ERP implementation is to improve, streamline and make the business process more efficient, productive and effective.

Table 2.3.1(B): Risks and corresponding Controls related to Process Risks

Aspect	Risk Associated	Control Required
Program Management	There could be a possibility of an information gap between day-to-day program management activities and ERP-enabled functions like materials and procurement planning, logistics and manufacturing.	This requires bridging the information gap between traditional ERP-based functions and high value operational management functions, such applications can provide reliable real-time information linkages to enable high-quality decision making.
Business Process Reengineering (BPR)	BPR means not just change – but dramatic change and dramatic improvements.	This requires overhauling of organizational structures, management systems, job descriptions, performance measurements, skill development, training and use of IT.

3. Technological Risks: The organizations implementing ERP systems should keep abreast of the latest technological developments and implementation which is required to survive and thrive.

Table 2.3.1(C): Risks and corresponding Controls related to Technological Risks

Aspect	Risk Associated	Control Required
Software Functionality	ERP systems offer a myriad of features and functions, however, not all organizations require those many features. Implementing all the functionality and features just for the sake of it can be disastrous for an organization.	Care should be taken to incorporate the features that are required by the organization and supporting additional features and functionality that might be required at a future date.

Technological Obsolescence	With the advent of more efficient technologies every day, the ERP system also becomes obsolete as time goes on.	This requires critical choice of technology, architecture of the product, ease of enhancements, ease of upgrading, quality of vendor support.
Enhancement and Upgrades	ERP Systems are not upgraded and kept up-to-date. Patches and upgrades are not installed and the tools are under utilised.	Care must be taken while selecting the vendor and upgrade/support contracts should be signed to minimize the risks.
Application Portfolio Management	These processes focus on the selection of new business applications and the projects required 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. Other Implementation Issues: Many times, ERP implementations are withdrawn because of the following factors.

Table 2.3.1(D): Risks and corresponding Controls related to some other implementation issues

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	Back up arrangement needs to

	data is lost, whole business may come to stand still.	be very strong. Also, strict physical control is needed for data.
Speed of Operation	As data is maintained centrally, gradually the data size becomes more and more and it may reduce the speed of operation.	This can be controlled by removing redundant data, using techniques like data warehousing and updating hardware on a continuous basis.
System Failure	As everybody is connected to a single system and central database, in case of failure of system, the whole business may come to stand still may get affected badly.	This can be controlled and minimized by having proper and updated back up of data as well as alternate hardware / internet arrangements. In case of failure of primary system, secondary system may be used.
Data Access	Data is stored centrally and all the departments access the central data. This creates a possibility of access to non-relevant data.	Access rights need to be defined very carefully and to be given on “Need to know” and Need to do” basis only.

5. Post Implementation issues: ERP operation and maintenance requires a lifelong commitment by the company management and users of the system.

Table 2.3.1(E): Risks and corresponding Controls related to post- implementation issues

Aspect	Risk Associated	Control Required
Lifelong commitment	Even after the ERP implementation, there will always be new modules/versions to install, new persons to be trained, new technologies to be embraced, refresher courses to be conducted and so on.	This requires a strong level of commitment and consistency by the management and users of the system.

4. Explain features of Controlling Module.

- **Cost Element Accounting:** This component provides overview of the costs and revenues that occur in an organization. The cost elements are the basis for cost accounting and enable the user the ability to display costs for each of the accounts that have been assigned to the cost element. Examples of accounts that can be assigned are Cost Centres,

Internal Orders, WBS (work breakdown structures).

- **Cost Centre Accounting:** This provides information on the costs incurred by the business. Cost Centres can be created for such functional areas as Marketing, Purchasing, Human Resources, Finance, Facilities, Information Systems, Administrative Support, Legal, Shipping/Receiving, or even Quality. Some of the benefits of Cost Centre Accounting are that the managers can set budget/cost Centre targets; Planning; Availability of Cost allocation methods; and Assessments/Distribution of costs to other cost objects.
- **Activity-Based-Accounting:** This analyse cross-departmental business processes and allows for a process-oriented and cross functional view of the cost centres.
- **Internal Orders:** Internal Orders provide a means of tracking costs of a specific job, service, or task. These are used as a method to collect those costs and business transactions related to the task. This level of monitoring can be very detailed but allows management the ability to review Internal Order activity for better decision making purposes.
- **Product Cost Controlling:** This calculates the costs that occur during the manufacture of a product or provision of a service and allows the management the ability to analyse their product costs and to make decisions on the optimal price(s) to market their products.
- **Profitability Analysis:** This allows the management to review information with respect to the company's profit or contribution margin by individual market segment.
- **Profit Centre Accounting:** This evaluates the profit or loss of individual, independent areas within an organization.

CHAPTER-3

INFORMATION SYSTEMS AND ITS COMPONENTS

1. Explain benefits of Big Data Processing.

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 are enabling organizations to fine tune their business strategies.
- Early identification of risk to the product/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.

CHAPTER-4

E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

1. Explain various types of E-Commerce Business Models

A **Business Model** can be defined as the organization of product, service and information flows, and the sources of revenues and benefits for suppliers and customers. An e-business model is the 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. Some of the e-markets are explained below in the Table 4.1.2:

Table 4.1.2: Various e-Markets

S. No.	e-Market	Description
1	e-Shops	An e-shop is a virtual store front that sells products and services online. Orders are placed and payments made. They are convenient way of effecting direct sales to customers; allow manufacturers to bypass intermediate operators and thereby reduce costs and delivery times. Examples - www.sonicnet.com , www.wforwomen.com
2	e-Malls	The e-mall is defined as the retailing model of a shopping mall, a conglomeration of different shops situated in a convenient location in e-commerce.
3	e-auctions	Electronic auctions provide a channel of communication through which the bidding process for products and services can take place between competing buyers. Example – www.onsale.com
4	Portals	Portals are the channels through which websites are offered as content. The control of content can be a source of revenue for firms through charging firms for advertising or charging consumers a subscription for access.
5	Buyer Aggregators	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. Example -

		www.zomato.com
6	Virtual Communities	Virtual Community is a community of customers who share a common interest and use the internet to communicate with each other. Amazon.com provides websites for the exchange of information on a wide range of subjects relating to their portfolio of products and services. Virtual communities benefit from network externalities whereby the more people who join and contribute to the community, the greater the benefits that accrue, but without any additional cost to participants.
7	e-marketing	e-marketing is the use of electronic communications technology such as the internet, to achieve marketing objectives. Of course, information on websites also empowers customers and helps them achieve their objectives. For example, they can compare prices of products by rival firms. The internet changes the relationship between buyers and sellers because market information is available to all parties in the transaction.
8	e-procurement	e-procurement is the management of all procurement activities via electronic means. 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 intermediaries specialize in providing up-to-date and real-time information on all aspects of the supply of materials to businesses.
9	e-distribution	The e-distribution 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. An example of a firm specializing in e-distribution is wipro.com (www.wipro.com) who use the internet to provide fully integrated e-businessmen abled 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.

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)	Generally, this supports the activities within the customer chain in that it focuses on sell-side activities.	e-shops, e-malls, e-auctions, buyer aggregators, portals etc.	www.cisco.com www.amazon.com
Business-to-Business (B2B)	This supports the supply chain of organizations that involves repeat commerce between a company and its suppliers or other partners.	e-auctions, e-procurement, e-distribution, portals, e-marketing etc.	www.emall.com
Consumer-to-Consumer (C2C)	This supports the community plan surrounding the organization and can be seen as a commercial extension of community activities.	e-auctions, virtual communities etc.	www.eBay.com

2. Explain applications of Internet Of Things.

These applications have been added. Earlier are already covered in the book.

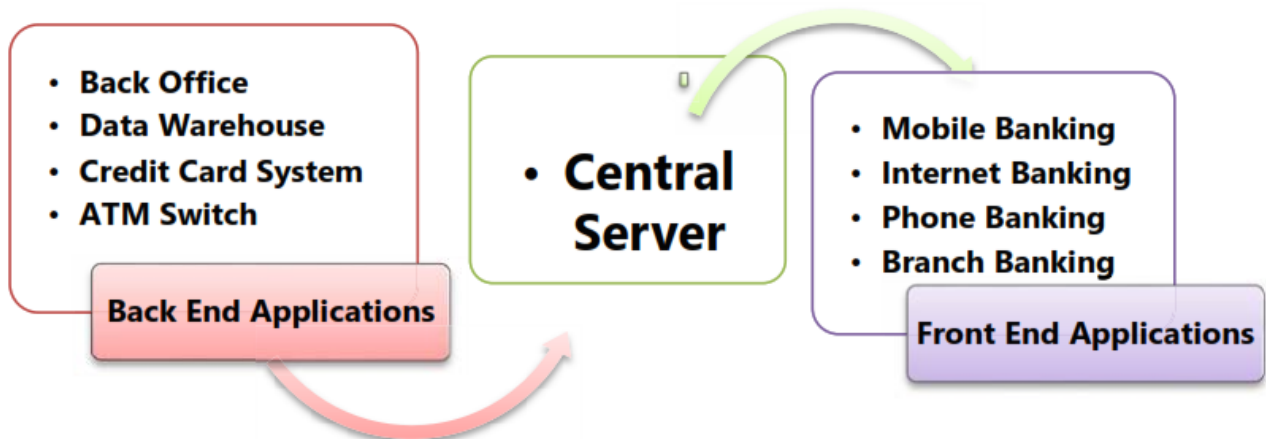
- **Wearables:** Just like smart homes, wearables remain another important potential IoT application like Apple smartwatch.
- **Smart City:** Smart cities, like its name suggests, is a big innovation and spans a wide variety of use cases, from water distribution and traffic management to waste management and environmental monitoring.
- **Smart Grids:** Smart grids are another area of IoT technology that stands out. A smart grid basically promises to extract information on the behaviors of consumers and electricity suppliers in an automated fashion to improve the efficiency, economics, and reliability of electricity distribution.
- **Industrial Internet of things:** One way to think of the Industrial Internet is by looking at connected machines and devices in industries such as power generation, oil, gas, etc. for monitoring and improving control efficiency. With an IoT enabled system, factory equipment that contains embedded sensors communicate data about different parameters, such as pressure, temperature, and utilization of the machine. The IoT system can also process workflow and change equipment settings to optimize performance.

- **Connected Car:** Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in communication to navigate in our complex world.
- **Connected Health (Digital Health/Telehealth/Telemedicine):** IoT has various applications in healthcare, which are from remote monitoring equipment to advance and smart sensors to equipment integration. It has the potential to improve how physicians deliver care and keep patients safe and healthy.
- **Smart Retail:** Retailers have started adopting IoT solutions and using IoT embedded systems across several applications that improve store operations, increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience.
- **Smart Supply Chain:** Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit or helping suppliers exchange inventory information are some of the popular offerings.

CHAPTER-5

CORE BANKING SYSTEMS

1. Explain working of Core Banking Systems through Front End and Back End Applications



Key Modules of CBS

- **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.
- **Credit-Card System:** Credit card system provides customer management, credit card management, account management, customer information management and general ledger functions; provides the online transaction authorization and service of the bank card in each transaction channel of the issuing bank; Support in the payment application; and at the same time, the system has a flexible parameter system, complex organization support mechanism and product factory based design concept to speed up product time to market.
- **Automated Teller Machines (ATM):** An Automated Teller Machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access most ATMs. ATMs are convenient, allowing consumers to perform quick, self-serve transactions from everyday banking like deposits and withdrawals to more complex

transactions like bill payments and transfers.

- **Central Server:** Initially, it used to take at least a day for a transaction to get reflected in the real account because each branch had their local servers, and the data from the server in each branch was sent in a batch to the servers in the data center only at the end of the day (EOD). However, nowadays, most banks use core banking applications to support their operations creating a Centralized Online Real-time Exchange (or Environment) (CORE). This means that all the bank's branches access applications from centralized data centers/servers, therefore, any deposits made in any branch are reflected immediately and customer can withdraw money from any other branch throughout the world.
- **Mobile Banking & Internet Banking:** Mobile Banking and Internet banking are two sides of the same coin. The screens have changes, the sizes have become smaller and banking has become simpler. Mobile banking is a much latest entrant into the digital world of banking.
 - o **Internet Banking** also known as Online Banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system offers over 250+ services and facilities that give us real-time access to our bank account. We can make and receive payments to our bank accounts, open Fixed and Recurring Deposits, view account details, request a cheque book and a lot more, while you are online.
 - o **Mobile Banking** is a service provided by a bank or other financial that allows its customers to conduct financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a Smartphone or tablet. Unlike the related internet banking, it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis.
 - o **Phone Banking:** It is a functionality through which customers can execute many of the banking transactional services through Contact Centre of a bank over phone, without the need to visit a bank branch or ATM. Registration of Mobile number in account is one of the basic prerequisite to avail Phone Banking. The use of telephone banking services, however, has been declining in favor of internet banking. Account related information, Cheque Book issue request, stop payment of cheque, Opening of Fixed deposit etc. are some of the services that can be availed under Phone Banking.

- **Branch Banking:** CBS are the bank's centralized systems that are responsible for ensuring seamless workflow by automating the frontend and backend processes within a bank. CBS enables single-view of customer data across all branches in a bank and thus facilitate information across the delivery channels. The branch confines itself to the following key functions:
 - o Creating manual documents capturing data required for input into software;
 - o Internal authorization;
 - o Initiating Beginning-Of-Day (BOD) operations;
 - o End-Of-Day (EOD) operations; and
 - o Reviewing reports for control and error correction.

2. Explain Risks associated with CBS.

- (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. Operational risk necessarily excludes business risk and strategic risk. The components of operational risk include transaction processing risk, information security risk, legal risk, compliance risk and people risk.
- (b) **Credit Risk:** It is the risk that an asset or a loan becomes irrecoverable in the case of outright default, or the risk of an unexpected delay in the servicing of a loan. Since bank and borrower usually sign a loan contract, credit risk can be considered a form of counterparty risk.
- (c) **Market Risk:** Market risk refers to the risk of losses in the bank's trading book due to changes in equity prices, interest rates, credit spreads, foreign-exchange rates, commodity prices, and other indicators whose values are set in a public market. To manage market risk, banks deploy several highly sophisticated mathematical and statistical techniques
- (d) **Strategic Risk:** Strategic risk, sometimes referred to as business risk, can be defined as the risk that earnings decline due to a changing business environment, for example new competitors or changing demand of customers.
- (e) **Compliance Risk:** Compliance risk is exposure to legal penalties, financial penalty and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.
- (f) **IT Risk:**
Already covered in chapter-5.

Prevention of Money Laundering Act (PMLA)

Only relevant sections pertaining to the topic are discussed below:

CHAPTER II OFFENCE OF MONEY-LAUNDERING**Section 3. Offence of money-laundering**

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the 17 proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.

CHAPTER IV OBLIGATIONS OF BANKING COMPANIES, FINANCIAL INSTITUTIONS AND INTERMEDIARIES**Section 12. Reporting entity to maintain records.**

- (1) Every reporting entity shall—
 - (a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;
 - (b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;
 - (c) Omitted
 - (d) Omitted
 - (e) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

[Note: Clauses (c) and (d) have been omitted]

- (2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.
- (3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.
- (4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.
- (5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

Section 13. Powers of Director to impose fine.

- (1) The Director may, either of his own motion or on an application made by any authority, officer or person, make such inquiry or cause such inquiry to be made, as he thinks fit to

be necessary, with regard to the obligations of the reporting entity, under this Chapter.

- (1A) If at any stage of inquiry or any other proceedings before him, the Director having regard to the nature and complexity of the case, is of the opinion that it is necessary to do so, he may direct the concerned reporting entity to get its records, as may be specified, audited by an accountant from amongst a panel of accountants, maintained by the Central Government for this purpose.
- (1B) The expenses of, and incidental to, any audit under sub-section (1A) shall be borne by the Central Government.
- (2) If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—
- (a) issue a warning in writing; or
 - (b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or
 - (c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
 - (d) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.
- (3) The Director shall forward a copy of the order passed under subsection (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section.

Explanation - For the purpose of this section, "accountant" shall mean a chartered accountant within the meaning of the Chartered Accountants Act, 1949 (38 of 1949).

CHAPTER X MISCELLANEOUS

Section 63. Punishment for false information or failure to give information, etc.

- (1) Any person willfully and maliciously giving false information and so causing an arrest or a search to be made under this Act shall on conviction be liable for imprisonment for a term which may extend to two years or with fine which may extend to fifty thousand rupees or both.
- (2) If any person -
- (a) being legally bound to state the truth of any matter relating to an offence under section 3, refuses to answer any question put to him by an authority in the exercise

of its powers under this Act; or

- (b) refuses to sign any statement made by him in the course of any proceedings under this Act, which an authority may legally require to sign; or
 - (c) to whom a summon is issued under section 50 either to attend to give evidence or produce books of account or other documents at a certain place and time, omits to attend or produce books of account or documents at the place or time, he shall pay, by way of penalty, a sum which shall not be less than five hundred rupees but which may extend to ten thousand rupees for each such default or failure.
- (3) No order under this section shall be passed by an authority referred to in sub-section (2) unless the person on whom the penalty is proposed to be imposed is given an opportunity of being heard in the matter by such authority.
- (4) Notwithstanding anything contained in clause (c) of sub-section (2), a person who intentionally disobeys any direction issued under section 50 shall also be liable to be proceeded against under section 174 of the Indian Penal Code (45 of 1860).

Section 70. Offences by companies.

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to the company, for 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.