CHAPTER-1

Categories Of Business Process:

UNDERSTAND ALL CATEGORIES OF BUSINESS PROCESS THROUGH EXAMPLES:

Sr. No.	Nature of business decision	Description of decision
1.	**Vision and Mission**	A dairy product company leading in Asian market decides to **increase its turnover by double in next ten years.**
2.	**Management Process**	To achieve turnover mentioned above the management needs to list down all activities to be done which may include: • **Enter into new markets** (Market development). • **Launch new products** (Product development). • **Acquire existing dairies** in markets where company had no presence (Acquisition).
3.	**Support Process**	Support processes like Human resource management performs various activities including – ➢ **Defining and creating a new management structure** ➢ Performing **all human resource activities** as listed above.
4.	**Operational Process**	Operational managers here are responsible to **do actual ground work** and ensure proper implementation of decisions taken above.

RISKS AND ITS MANAGEMENT

RISKS;

What is risk?

"Risk is **any event** that may results into **significant deviation from planned objective** resulting into some **unwanted negative consequences."**

For example: Unauthorized disclosure of assets, accidental or intentional data loss, system crash etc.

Here "Planned objective" is in what context?

"Planned objective could be any aspect of an enterprise's financial, strategic, operational processes, products etc."

SOURCES OF RISK

Sources of risks are basically the areas from where risks can occur.

Some of the common sources of risk are;

a. **Commercial and Legal Relationships,**
b. **Economic Circumstances,**
c. **Human Behavior,**
d. **Natural Events,**
e. **Political Circumstances,**
f. **Technology and Technical Issues,**
g. **Management Activities and Controls, and**
h. **Individual Activities.**

Characteristics of Risk:

Broadly, risk has **the following characteristics:**

i. **Potential loss:** Potential loss that exists as the result of threat/vulnerability process.

ii. **Uncertainty of loss:** Uncertainty of loss which is **expressed in terms of probability of such loss.**

iii. **Probability/likelihood:** Probability that a threat agent mounting a **specific attack against a particular system.**

Types of Risks

Broad categorization of risks:

A. Business Risks

B. Technology Risk

C. Data related risks

A. Business Risks:

Businesses face various kinds of risks which may be financial, strategical, and regulatory etc in nature. Various types of business risks are:

I. Strategic Risk

II. Financial Risk

III. Regulatory Risk

IV. Operational Risk

V. Hazard Risk

VI Residual Risk

Sr. No.	Risk type	Meaning
1.	**Strategic Risk**	These are the risks that would **prevent an organization from accomplishing its objectives.** **Example:** Competitive risk: Inability to respond move of competitor.
2.	**Financial Risk**	Risk that could result in a **negative financial impact** to the organization (waste or loss of assets). **Example:** Liquidity risk, interest rates, credit risk, market risk etc.
3.	**Regulatory Risk**	• It is also called as **compliance risk.** • It is risk that could **expose the organization to fines and penalties** from government due to non-compliance with laws and regulations. **Example:** GST violation.
4.	**Operational Risk**	Risk that could **prevent the organization from operating in the most effective and efficient manner** or be disruptive to other operations. **Example:** Lack of or faulty BCP.
5.	**Hazard Risk**	Risks those are **insurable.** **Example:** Natural disasters, Insurable liabilities, terrorism etc.
6.	**Residual Risk**	It refers to the **risk remaining even after the counter measures** are analyzed and implemented.

Management of risk focuses on reducing the impact what organization would face otherwise when safeguard is lacking. An organization's management of risk should consider these two

areas:

a.Acceptance of residual risk and

b.Selection of safeguards.

100% elimination of risk is not possible and even after implementation of safeguard some residual risks remain. Here management needs to have clear focus on keeping residual risk at an acceptable level so to manage it.

B. Technology Risk:

In modern world technology is a key enabler of business. It is used in business process automation which also raises certain challenges.

With continuous innovation in technology, increased complexity, dependence on vendors etc, the business processes and standards adapted by enterprises should consider various new set of IT risks and challenges like:

Sr. No.	Risks/Challenges	Description
1.	**Frequent changes or obsolescence of technology**	• **If anything that doesn't change then that is change itself.** Technology is **changing continuously** and everyday new things are being introduced and existing is becoming **obsolete quickly.** And this ever changing technology brings in **challenge to select technology in a properly planned way and keeping future in mind** so to avoid loss.
2.	**Multiplicity and complexity of systems**	Companies now days are **using multiple digital platforms** like we see in case of banking system which makes **it quite complex.** Hence, this requires both personnel and vendors involvement. The **personnel should have knowledge about requisite technology skills** or the **management of the technology could be outsourced** to a company having the relevant skill set or combination may be used.
3.	**Different types of controls for different types of technologies/systems**	There comes need to apply **different types of controls as per the kind of technology or system deployed.**
4.	**Proper alignment with business objectives and legal/regulatory**	A system is designed, developed and deployed considering objectives to be achieved but at the same time **it should also comply with legal requirements.** Creating a **proper alignment**

	requirements	between **business requirements and legal requirements** is a challenge for business.
5.	**Dependence on vendors due to outsourcing of IT services**	In an automated environment **organization needs to highly qualified employees with specialized domain skills to manage systems and IT resources and the problem is organization usually lacks it** which results into outsourcing it to vendor. Outsourcing results into over dependence on vendor which gives rise to vendor risk.
6.	**Vendor related concentration risk**	• Organization depends on **multiple vendors for different types of services** like network, system software, application software and hardware etc. • This results in higher risks due to heavy dependence on vendors.
7.	**Segregation of Duties (SoD)**	SoD is basically **splitting of tasks** with clearly defined roles, authority and responsibility. Like in case of banking transaction It doesn't allow a single employee to initiate, authorize and disburse a loan, the possibility of misuse cannot be ignored.
8.	**External threats leading to cyber frauds/ crime**	Technology and online systems has its own disadvantages as well like **cyber-crime and frauds.**
9.	**Higher impact due to intentional or unintentional acts of internal employees**	**End users are not very security conscious** and employees in a technology environment are the weakest link in an enterprise.
10.	**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 unauthorized to commit frauds.

C. **Data related risks:** These include **Physical access of data and Electronic access of data.** This topic will be covered in details in later chapters.

Risk Management and Related Terms

Various terminologies relating to risk management are:

Sr. No.	Term	Description
1.	**Risk Management**	It refers to the process of **assessing risk,** taking **steps to reduce**

		risk to an acceptable level and **maintaining that level of risk.**
2.	**Asset**	Asset can be defined as **something of value to the organization.** Assets may include **hardware, software, facilities, employees etc** but Irrespective the nature of the assets they all have one or more of the **following characteristics:** **a.** **Recognized to be of value to organization.** **b.** **Not easily replaceable without cost, skill, time,** resources or a combination. **c.** **Form a part of the organization's corporate identity.** **d.** Their **data classification** would normally be **Proprietary, Highly confidential or even Top Secret.**
3.	**Vulnerability**	➢ Vulnerability is the **weakness in the system** safeguards that renders the system susceptible to attack. ➢ Vulnerabilities potentially **"allow" a threat to harm** or exploit the system. Some examples of **vulnerabilities** are given as follows: **a.** **Poor physical access control.** **b.** **Short and weak passwords.** Normally, **vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:** **a.** Allows an attacker to **execute commands** as another user **or** **b.** Allows an attacker **to access data** that is contrary to the specified access restrictions for that data **or** **c.** Allows an attacker to **pose as another entity** **or** **d.**Allows an attacker to conduct a **denial of service.**

4.	**Threat**	• Threat can be any entity, circumstances, an action, event or condition which **cause harm** or have **potential to harm system** or it's components. • It effects quality and have ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm.
5.	**Exposure**	An exposure is the **extent of loss the enterprise has to face when a risk materializes** like loss of business due to some natural disaster, loss of reputation due to unethical practices or lack of security standards for users credentials etc.
6.	**Likelihood**	It is the **estimation of the probability that the threat will succeed** in achieving an undesirable event.
7.	**Attack**	➢ An attack is an **attempt to gain unauthorized access** to the system's services. ➢ 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 safeguards.
8.	**Counter Measure**	An **action, device, procedure, technique or other measure** that reduces the vulnerability of a component or system is referred as Counter Measure.

Risk Management Strategies

Risk management strategies involve decisions to deal with various types of risks based on exposures, probability, impact, nature of risks etc. After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified.

There are various risk management strategies which can be applied in isolation or in combination:

Sr. No.	Risk management strategy	Definition/Description
1.	**Tolerate/Accept the risk**	• There may be certain risks which are considered minor as **their impact and probability of occurrence is low** and such risks are **accepted as a cost of doing business.** • These risks should be periodically reviewed to ensure its impact remains low.
2.	**Terminate/Eliminate the risk**	Certain risks can be easily **eliminated** by addressing cause like if a risk is associated with a technology then this risk can be **eliminated by replacing technology with better one.**

3.	**Transfer/Share the risk**	In this risk is **transferred or shared with trading partners, suppliers, insurers etc.**
4.	**Treat/mitigate the risk**	It involves **implementing controls to** prevent the risk from manifesting to prevent the risk from manifesting itself or to minimize its effects.
5.	**Turn back**	In cases where the probability or impact of the risk is very low, then management may decide to **ignore the** risk.

APPLYING IT CONTROLS

IT controls are **subset of organization's internal controls.** It controls objectives are related to CIA (Confidentiality, Integrity and Availability) of data and overall management of IT functions of business enterprises.

It is of 2 types:

(a) IT General Controls (ITGC)
(b) Application Controls

(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.

General controls include, but are not limited to:

Some General controls:: Keeping CBS(Core banking system) in Mind::		
(i)	**Information Security Policy**	The security policy is **approved by the senior management** and encompasses all areas of operations of bank and **drives access to information across the enterprise** and other stakeholders.
(ii)	**Administration, Access, and Authentication**	IT should be administered with appropriate policies and procedures clearly defining the **levels of access to information and authentication of users.**
(iii)	**Separation of key IT functions**	Bank should 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** conflicts.
(iv)	**Management of Systems Acquisition**	Software solutions for **CBS are most developed**

	and Implementation	**acquired and implemented.** Hence, **process of acquisition and implementation of systems should be properly controlled.**
(v)	**Change Management**	As per **changing compliance requirements, technology environment, and business processes etc. IT solutions** should be **deployed and changed** on **continuous basis** with management approval.
(vi)	**Backup, Recovery and Business Continuity**	Bank relies on IT heavily which makes it imperative to have appropriate **BCP, backup, off-site data center and disaster recovery** etc.
(vii)	**Proper Development and Implementation of Application Software**	Development and implementation of solutions must be **properly controlled by using standard software development process.**
(viii)	**Confidentiality, Integrity and Availability of Software and data files**	**Security is** implemented **to ensure Confidentiality, Integrity and Availability of information.**
(ix)	**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**.
(x)	**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.**
(xi)	**Value Add areas of Service Level Agreements (SLA)**	**SLA** with vendors is regularly reviewed to ensure that the **services are delivered as per specified performance parameters**.
(xii)	**User training and qualification of Operations personnel**	The personnel deployed have **required competencies and skill-sets to operate and monitor the IT environment.**

(c) Application Controls

- ❒ Application Controls are controls which **are implemented in an application to prevent or detect and correct errors.**
- ❒ These controls are **in-built in the application software** to ensure accurate and reliable processing.

- These are designed to **ensure completeness, accuracy, authorization and validity of data capture and transaction processing.**

  Example: In banking, application software ensures automatic calculation of interest based on pre-defined rates, only transactions of the day are accepted by the system, Withdrawals are not allowed beyond limits, etc.

Some examples of Application controls are as follows:

Sr. No.	Example-Application control	Purpose/Example
I.	Data edits	Editing of data is allowed only for permissible fields
II.	Separation of business functions	Transaction initiation and authorization done by separate individuals
III.	Balancing of processing totals	Debit and credit of all transactions are tallied
IV.	Transaction logging	All transactions are identified with unique id and logged
V.	Error reporting	All errors in processing are reported
VI.	Exception Reporting	All exceptions are reported

CHAPTER-2

ERP System

Benefits of an ERP System

Benefits of an ERP System		
Sr. No.	**Benefit**	**Description**
1.	**Information integration**	ERP **integrates all processes and functions of enterprise as a result it automatically updates data** between related business functions and components.
2.	**Reduction of lead-time**	Lead-time is basically **time involved in placing an order and receiving it.** Since ERP is an integrated system having several modules like Finance, Manufacturing, Material Management Module etc and use of technologies like **EFT** (Electronic Fund Transfer), **EDI** (Electronic Data Interchange) reduce the lead times.
3.	**On-time Shipment**	ERP **integrates various functions involved in the timely delivery of the finished goods to the customers like purchasing, material management production, production planning, plant maintenance, sales and distribution etc** and hence ensure on-time delivery of goods to the customers.
4.	**Reduction in Cycle Time**	Cycle time is the **total time elapsed between placement of the order and delivery of the product.** ERP reduces cycle time as all data are stored in **centralized database**, are **updated in real time** and **procedure are automated** which doesn't need human intervention
5.	**Improved Resource utilization**	ERP systems help the organization in drastically improving the capacity and resource utilization by **keeping inventory at minimum level, minimizing machine down time, producing goods as per demand and delivering goods to customer in most efficient way.**

6.	**Better Customer Satisfaction**	ERP enables customers **to place the order, track the status of the order and make the payment sitting at home** which improves the customer satisfaction level.
7.	**Improved Supplier Performance**	**ERP systems provide vendor management and procurement support tools designed to coordinate all aspects of the procurement process which is helpful in negotiation, monitoring, and control procurement costs and schedules while assuring superior product quality** and also help the organization in managing supplier relations, monitoring vendor activities and managing supplier quality.
8.	**Increased Flexibility**	ERP Systems **addresses departmental barriers and make information available across departments** which organization flexible and adaptive to market conditions.
9.	**Reduced Quality Costs**	ERP system **provides tools to implement TQM** and it helps to ensure that a single change to standard procedure is implemented throughout the organization. Hence ERP system helps to maintain quality keeping cost as low as possible
10.	**Better Analysis and Planning Capabilities**	ERP system enables the comprehensive and unified management of related business functions and their data which helps 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.
11.	**Improved information accuracy and decision-making capability**	ERP Systems **helps in integration and automation which ultimately improves the information accuracy** and help **in better decision-making.**
12.	**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**

ERP IMPLEMENTATION, ITS RISKS AND RELATED CONTROLS

There are certain issues which arises during implementation namely People, Process, Technological, other implementation and post implementation issues. To manage these issues appropriate controls should be adopted so to avoid failure or underperformance of project.

Various issues and related controls are discussed below;

1. **People Issues:** Here people include **employees, management, implementation team, consultants and vendors.** These players play vital role in success or failure of an ERP System

Risks and corresponding Controls related to People Issues

Sr. No.	Aspect	Risk Associated	Control Required
1	**Change Management**	Change 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 and Practical hands on training of the ERP System helps in smooth and hassle free transition.
		Change in **organization functions, improvement in planning,** forecasting and decision-making capabilities 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.	This requires clear **defining of change control procedures** and holds everyone to them.
2	**Training**	Management may **curtail the training due to increase in the overall cost budget.**	**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.
3	**Staff Turnover**	**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.	Creating **match between employee's aptitude and job assigned,** fixing of **compensation package etc** thus **keeping the employees happy and content** and minimizing the staff turnover.
4	**Top Management Support**	**Lack or inadequate support** and grant permission for the availability of the huge **resources** that are required during the transition.	The ERP implementation shall be started only after the **top management is fully convinced and assure of providing the full support.**
5	**Consultants**	**Consultant might not be**	Assignment of a **liaison officer**

		familiar with the internal workings and organizational culture.	**from senior management to familiarize consultant with company's inner workings.**

2. **Process Risks:** ERP system is applied to integrate and improve business process and make it more efficient, effective and productive. Meanwhile various types of risks also arise.

Risks and corresponding Controls related to Process Risks

Sr. No.	Aspect	Risk Associated	Control Required
1	**Program Management**	Possibility of **information gap between day-to-day program management activities and ERP-enabled functions** like materials and procurement planning, logistics and manufacturing.	Using **applications for bridging the information gap** between traditional ERP-based functions and high value operational management functions to enable reliable real-time information linkages to enable high-quality decision Making.
2	**Business Process Reengineering (BPR)**	BPR is applied **to achieve dramatic improvement by affecting dramatic change.**	This requires **overhauling of organizational structures, management systems, job descriptions, performance measurements, skill development, training and use of IT.**

3. **Technological Risks:** Adapting new technology is one of the pre-requisite to survive and thrive in this highly dynamic IT environment.

Risks and corresponding Controls related to Technological Risks

Sr. No.	Aspect	Risk Associated	Control Required
1	**Software Functionality**	ERP systems consist of huge number of functions and features. **Implementing all features and functions may be disastrous** if not needed in	Incorporate **only those features which are required by the organization** and supporting additional features and functionality that might be required at a future date.

		true sense.	
2	**Technological Obsolescence**	Rapid growth in technology may cause ERP system to becomes **obsolete with time.**	Proper **care while selecting technology,** architecture of the product, ease of enhancements, ease of upgrading, quality of vendor support.
3	**Enhancement and Upgrades**	ERP Systems are **not upgraded and kept up-to-date.**	**Care must be taken while selecting the vendor** and **upgrade/support contracts should be signed** to minimize the risks.
4	**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:** There are various others risks besides people, process and technology which may cause withdrawal of ERP implementations. Those are discussed below;

Risks and corresponding Controls related to some other implementation issues

Sr. no.	Aspect	Risk Associated	Control Required
1.	**Lengthy implementation time**	ERP projects are lengthy that takes anywhere between **1 to 4 years** depending upon the size of the organization.	Care must be taken to **keep the momentum high** and enthusiasm live amongst the employees, so as to minimize the risk.
2.	**Insufficient Funding**	**Not allocating budget by consulting expert** may cause project to stop due to lack of fund.	**Allocate necessary funds** and also keep some more funds for contingencies.
3.	**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** and strict physical control is needed for data.
4.	**Speed of Operation**	As **data is maintained centrally,** gradually the data size becomes more and more and it may reduce the speed of operation.	**Remove redundant data** using techniques like data warehousing and updating hardware on a continuous basis.
5.	**System Failure**	**Failure of system being centralized the whole business may come to stand still may**	Have proper and **updated back up of data** as well as **alternate hardware** / internet arrangements. In case of failure

		get affected badly.	of primary system, secondary system may be used.
6.	**Data Access**	Data is **stored centrally** and **accessed by all the departments** which gives rise to possibility of access to non-relevant data.	Access rights need to be defined on **"Need to know"** and **Need to do"** basis only.

5. **Post Implementation issues:** After implementation of ERP operation and maintenance starts. The management and users commitment should not be limited to implementation phase only but it should be continued during operations and maintenance as well. There may be various post-implementation issues discussed below;

Risks and corresponding Controls related to post- implementation issues

Aspect	Risk Associated	Control Required
Lifelong commitment	Post implementation there is always need of **adding new modules, training to new staff, introducing new technologies etc.**	There should be **strong level of commitment and consistency** by the management and users of the system.

2. Controlling Module:

- This module facilitates coordinating, monitoring, and optimizing all the processes in an organization.
- It controls the business flow in an organization.
- This module helps in analyzing the actual figures with the planned data and in planning business strategies.
- Two kinds of elements are managed in Controlling –**Cost Elements** and **Revenue Elements**. These elements are stored in the Financial Accounting module.

Key features of Controlling Module are:

Key features of this module are as under:

Key features of controlling module;		
Sr. No.	**Feature**	**Description**
1.	**Cost Element Accounting**	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** like Cost Centers, Internal Orders, WBS etc.

2.	**Cost Centre Accounting**	This component provides information on the **costs incurred by the business.** **Cost Centers** can be created for functional areas like **Marketing, Purchasing, Human Resources, Finance, Facilities, and Information Systems etc.** This component **helps managers in setting budget/cost Centre targets; Planning; Availability of Cost allocation methods; and Assessments/Distribution of costs to other cost objects.**
3.	**Activity-Based-Accounting**	This component helps to **analyses cross-departmental business processes** and allows for a **process-oriented and cross- functional view of the cost centers.**
4.	**Internal Orders**	Internal Orders provide a means of **tracking costs of a specific job, service, or task.** It allows management the ability to review Internal Order activity for better- decision making purposes.
5.	**Product Cost Controlling**	This component is used to calculate 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.
6.	**Profitability Analysis**	This component allows the management to **review information with respect to the company's profit or contribution margin by individual market segment.**
7.	**Profit Centre Accounting**	This component **evaluates the profit or loss of individual, independent areas within an organization.**

5. Production Planning (PP) Module

Production Planning (PP) Module is designed specifically for production planning and management. This module like other also consists of configuration, master data, and transaction.

It collaborates with Master data, SOP, DRP, MRP, capacity planning, product cost planning, and production planning. These are discussed in table below;

Sr. No.	Elements	Description
1.	**Master Data**	This includes the **material master, work centres, routings and bill of materials.**
2.	**SOP**	Sales and Operations Planning (SOP) provides the **ability to forecast sales and production plans based on historical, current and future data.**
3.	**DRP**	Distribution Resource Planning (DRP) allows companies the ability to **plan the demand for distribution centres.**
4..	**Production Planning**	This includes **material forecasting, demand management, long term planning** and **master production scheduling** (MPS).
5.	**MRP**	Material Requirements planning **relies on demand and supply elements** with the calculation parameters to calculate the net requirements from the planning run.
6.	**Capacity Planning**	This **evaluates the capacity utilized** based on the work centres available capacity to show capacity constraints.
	Product Cost Planning	This is the process of **evaluating all the time values and value of component materials to determine the product cost.**

Process in Production Planning Module

1. Quality Management Module

- **Quality Management Module** helps in management of quality in productions across processes in an organization.
- This quality management module helps an organization to accelerate their business by adopting a structured and functional way of managing quality in different processes.

- Quality Management module collaborates in procurement and sales, production, planning, inspection, notification, control, audit management and so on.
    - **Quality Planning**: Quality planning is the process of **planning the production activities to achieve the goals of meeting the customer requirements in time, within the available resources.**
    - **Quality Control**: It is a system for **checking and monitoring of the process and products with an intention of preventing non-conforming materials from going to the customer.**
    - **Quality Assurance**: Quality assurance **concentrates on identifying various processes, their interactions and sequence, defining the objectives of each process, identifying the key result areas and measures to measure the results, establishing the procedures for getting the required results, documenting the procedures** to enable everyone to follow the same, **educating the people** to implement the procedures, **preparing standard operating instructions** to guide the people on work spot, **monitoring and measuring the performance**, **taking suitable actions on deviations and continuously improving the systems.**
    - **Quality Improvement**: **The customer's needs and expectations are continuously changing depending on the changes in technology, economy, political situation, ambitions and dreams, competition, etc.**

Process in Quality Management Module

Quality Management process includes the following:

- Master data and standards are set for quality management;
- Set Quality Targets to be met;
- Quality management plan is prepared;
- Define how those quality targets will be measured;
- Take the actions needed to measure quality;
- Identify quality issues and improvements and changes to be made;
- In case of any change is needed in the product, change requests are sent;
- Report on the overall level of quality achieved; and

- Quality is checked at multiple points, e.g. inwards of goods at warehouse, manufacturing, procurement, returns.

2. Plant Maintenance Module

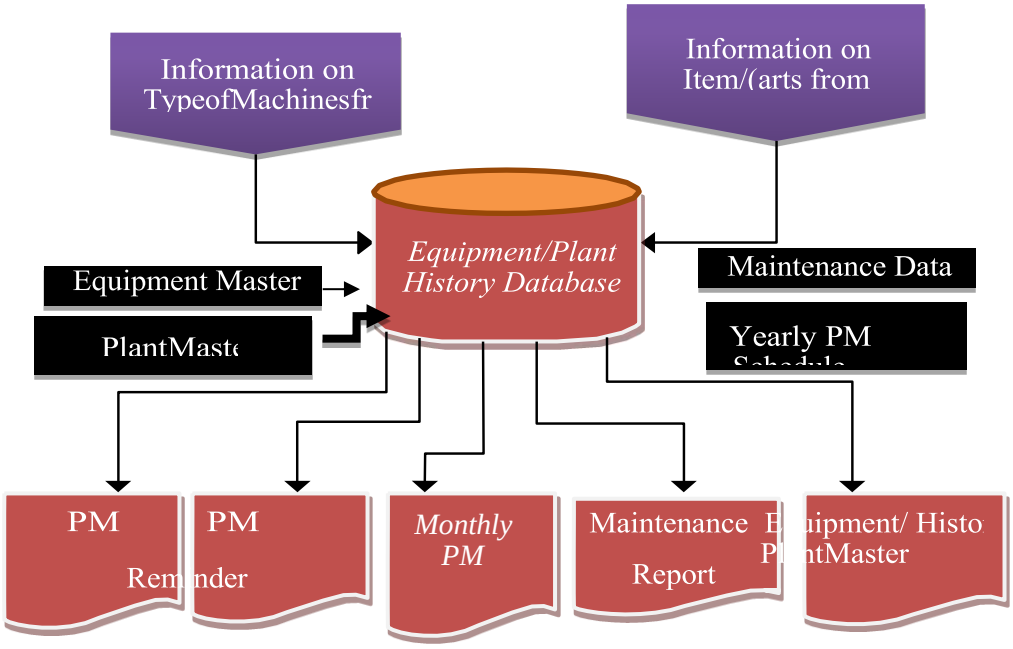
- This is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules.
- **Plant Maintenance (PM)** application component provides you with a comprehensive software solution for all maintenance activities that are performed within a company.
- It supports cost-efficient maintenance methods, such as risk-based maintenance or preventive maintenance, andprovidescomprehensiveoutageplanningandpowerfulworkordermanagement.

Objectives of Plant Maintenance Module

Objectives of Plant Maintenance Module		
Sr. No.	**Objectives**	**Memory Hint (For self)**
1.	To achieve **minimum breakdown** and to keep the plant in good working condition at the lowest possible cost.	**Minimize breakdown**
2.	To keep machines and other facilities in a condition that permits them to be used at their **optimum (profit making) capacity** without any interruption or hindrance.	**Optimum capacity utilization**
3.	To ensure the **availability of the machines,** buildings and services required by other sections of the factory for the performance of their functions at optimum return on investment whether this investment be in material, machinery or personnel. • **Equipment Master:** It is a repository of the **standard information** that one needs related to a **specific piece of equipment.** • **Equipment/Plant Maintenance**: It provides a **variety of reports** to help us to review and manage information about our equipment and its maintenance. • **Plant Maintenance (PM) Reports**: These are used to **review and manage information about preventive maintenance schedules and service types within any maintenance organization.** **Different PM reports are required to review PM information, such as:**	**Availability of machines and services etc.** **+** **Equipment master, Plant maintenance, PM reports**

	• **Status of service types for a piece of equipment;** • **Maintenance messages;** • **The frequency of occurrence for selected service types** • **All equipment transactions.**	

Process in Plant Maintenance



Reasons for Business Intelligence

Some important reasons for business intelligence are;

- BI enables organizations to make **well-informed business decisions** and thus can be the source of competitive advantages.
- BI gives **understanding of external environment** and makes accurate forecasts about future trends or economic conditions which help in decision making.
- The ultimate objective of business intelligence is to **improve the timeliness and quality of information. Business intelligence reveals to us:**
  - The **position of the firm in comparison to its competitors**
  - **Changes in customer behavior and** spending patterns

- The **capabilities of the firm**
- **Market conditions future trends, demographic** and **economic information**
- The **social, regulatory** and **political environment**
- **What the other firms in the market are doing ?**

CHAPTER-3

Big Data

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 are enabling organizations to fine tune their business strategies.
- **Early identification of risk to the product/services**, if any

b) Improved customer service

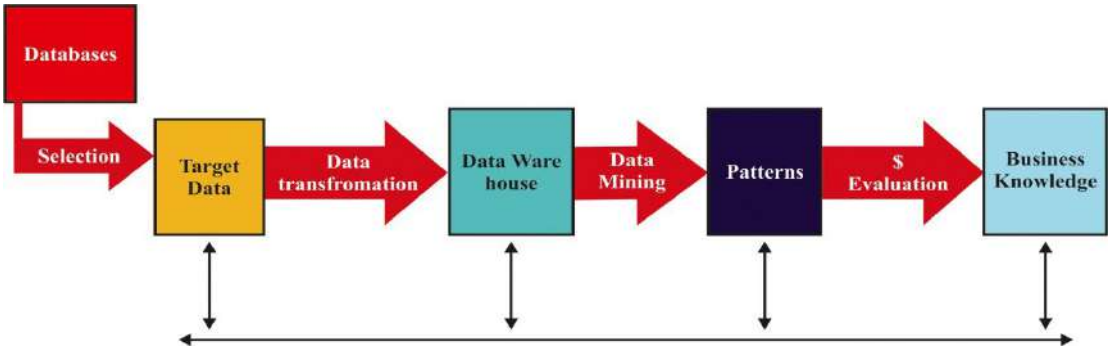
- Traditional customer feedback systems are getting replaced by **new systems designed with Big Data technologies.** In these new systems, **Big Data and natural language processing technologies** are being used to read and **evaluate consumer responses.**

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.

Data Mining:

Data Mining is the **process of analyzing data to find previously unknown trends, patterns, and associations to make decisions.** Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse.



Steps involved in Data Mining

Steps involved in data mining:

A. **Data Integration:** This is the first step and involves **collecting and integrating data** from different sources.
B. **Data selection:** This step involves **selecting that data which is useful** for data mining.
C. **Data cleaning:** It involves **removing anomalies from data like errors, inconsistent data** etc.
D. **Data transformation**: It involves **transforming data into appropriate form** for mining using different techniques like smoothing, aggregation, normalization etc.
E. Data Mining: It involves applying data mining techniques to **extract pattern from data.**
F. **Pattern evaluation and knowledge presentation**: This step **involves visualization, transformation, removing redundant pattern etc. from generated pattern.**
G. **Decision/use of discovered knowledge:** This step helps users to **make use of acquired knowledge in decision making.**

Some of the critical control lacking in a computerized environment are as follows:

Lack of management understanding of IS risks and related controls; Absence or inadequate IS control framework;

- **Absence of general controls and IS controls;**
- **Lack of awareness and knowledge of IS risks and controls** amongst the business users and even IT staff;
- **Complexity of implementation of controls** in **distributed computing environments** and extended enterprises;
- **Lack of control features** or their implementation in highly technology driven environments; and
- **Inappropriate technology implementations** or inadequate security functionality in technologies implemented.

The control objectives serve two main purposes:

- ✓ Outline the policies of the organization as laid down by the management; and
- ✓ A benchmark for evaluating whether control objectives are met.

CHAPTER-4

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

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 info me diaries 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**

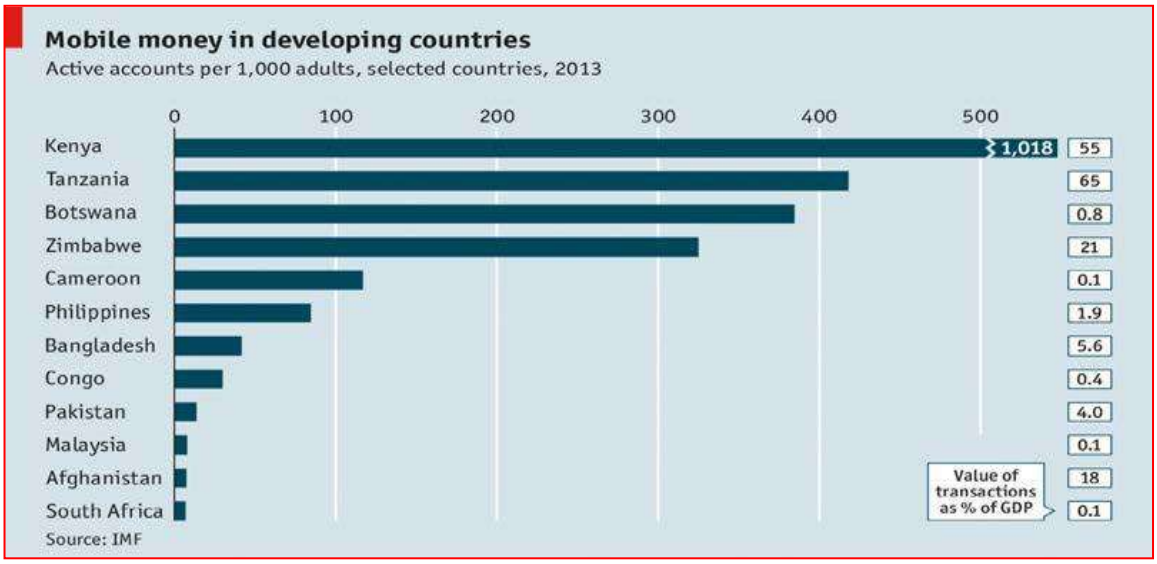
		tracking through each point in the supply chain. An example of a firm specializing in e- distribution is wipro.com (www.wipro.com) who use the internet to provide fully integrated e-business- enabled solutions that help to unify the information flows across all the major distribution processes including sales and marketing automation, customer service, warehouse logistics, purchasing and Inventory management, and finance.

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 beseen as a commercial extension of community activities.	**e-auctions, virtual communities** etc.	www.eBay.com

E-Commerce Future

From 1997 till date there has been huge growth in e-commerce. Data by The Economist magazine for 2013 indicates that E-commerce vide mobiles is not only limited to developed world but developing/third world countries have adopted is faster as well.



Introduction to Web 4.0

Web 4.0 is **next step** in the evolution which is bringing lot of capabilities.

It is **proposed to be Autonomous, Proactive, Context-exploring, Collaborative, Content generating agent based on semantic and reasoning technologies and artificial intelligence.**

These services will support adaptive content presentation that will use the web database via an intelligent agent.

Possible examples:

- **Services interacting with sensors and implants**
- **Virtual reality services**
- **Natural language services etc.**

Internet of Things (IoT)

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

For example:

India's living legend of cricket appearing in an Advertisement for water purifier informs that, the water purifier is Wi-Fi enabled. When the purifying agents deplete in the machine it connects to home Wi-Fi and informs the service agents of the company.

Future: Gartner, the technology researcher has projected that by 2020 the IOT business across the world would increase to USD 1.9 Trillion.

Applications: Some of the applications are as follows:

1. All home appliances to be connected and that shall create a virtual home.
    a. Home owners can keep track of all activities in house through their hand held devices.
    b. Home security CCTV is also monitored through hand held devices.
2. Office machines shall be connected through net.
    a. Human resource managers shall be able to see how many people have had a cup of coffee from vending machine and how many are present.
    b. Now many printouts are being generated through office printer?
3. Governments can keep track of resource utilisations / extra support needed.
    a. Under SWACHH mission government can tag all dustbins with IOT sensors. They (dustbins) generate a message once they are full. Being connected to wifi, they can intimate the cleaning supervisor of Municipal Corporation so that BIN can be emptied.
4. As a research study, individuals have got themselves implanted with electronic chips in their bodies. This chip allows him / her to connect to home / office wifi. Once connected person can enter home / office and perform designated function. This chip becomes individual's authentication token.
5. **Wearables:** Just like smart homes, wearables remain another important potential IoT application like **Apple smartwatch.**
6. **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.**
7. **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.**
8. **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.**

9. **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.**

10. **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.

11. **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.**

12. **Smart Supply Chain:** 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.**

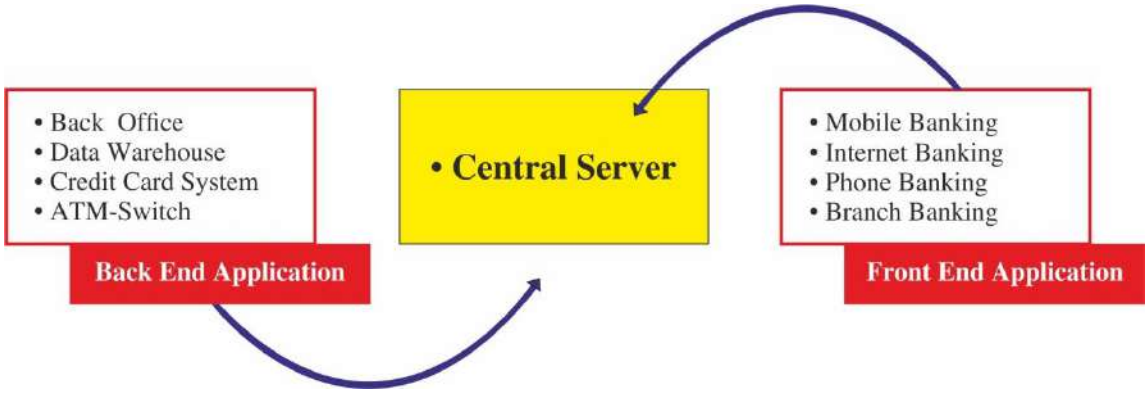
CHAPTER-5

MAJOR PRODUCTS AND SERVICES OFFERED BY BANK

3	**Remittances**	Remittances: It **involve transfer of funds from one place to another.** Two of the most common modes of remittance of funds are demand drafts and **Telegraphic/ Mail Transfers (TT/ MT).** **Drafts:** Drafts are issued by one branch of the Bank and are payable by another branch of the Bank. If there is no branch of the Bank at the place of destination, then branch of another Bank with which the issuing Bank has necessary arrangements makes the payment. The drafts are handed over to the applicant. **TT/MT:** In TT/MT no instrument is handed over to the applicant but the branch transmits it. Usually the payee of both the TT and the MT is an account holder of the paying branch. **EFT:** Electronic Funds Transfer facilitates instant fund transfer from one account to another without involvement of any paper work. This method is very popular now a day and is used widely. **Some new modes of money transfer are:** **(a) Real Time Gross Settlement (RTGS)** : It is an electronic form of funds transfer where the transmission takes place on a real-time basis. • **In India, transfer of funds with RTGS is done for high value transactions, the minimum amount being ` 2 lakh. The beneficiary account receives the funds transferred, on a real- time basis.** **(b) National Electronic Funds Transfer (NEFT)**: It is a nation-wide payment system facilitating **one-to-one funds transfer**. • Under this Scheme, individuals can electronically transfer funds **from any bank branch to any individual having an account with any other bank branch in the** country participating in the Scheme. **(c) Immediate Payment Service (IMPS)**: It is an **instant payment inter- bank electronic funds transfer system** in India. IMPS offers an inter- bank electronic fund transfer service through mobile phones. Unlike NEFT and RTGS, the service is available **24/7 throughout the year including bank holidays.**

Overview of Core Banking System:

Key modules of CBS are:



Key Modules of CBS

In the case of a CBS, at the **core is Central server**. **All key modules of banking** such as **back office, branch, data warehouse, ATM Switch, mobile banking, internet banking, phone banking and credit-card system are all connected** and related transactions are interfaced with the central server ad 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:** 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 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: 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:** The **screens have changes,** the **sizes have become smaller** and banking has **become simpler.**

  - **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** etc.

  - **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. App is Provided by Bank.

  - **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 perquisite 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 branc**hes in a bank and thus facilitate information across the delivery channels.

- **The branch confines itself to the following key functions:**

  - Creating manual documents capturing data required for input into software;
  - Internal authorization;
  - Initiating Beginning-Of-Day (BOD) operations;
  - End-Of-Day (EOD) operations; and
  - Reviewing reports for control and error correction.

CBS RISKS, SECURITY POLICY AND CONTROLS

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.**

• People risk arises from lack of trained key personnel, tampering of records, unauthorized access to dealing rooms and nexus between front and back end offices. Processing risk arises because faulty reporting of important market developments to the bank management may also occur due to errors in entry of data for subsequent bank computations. 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.

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: Once the complete business is captured by technology and processes are automated in CBS; the Data Centre (DC) of the bank, customers, management and staff are completely dependent on the DC. From a risk assessment and coverage point of view, it is critical to ensure that the Bank can impart advanced training to its permanent staff in the core areas of technology for effective and efficient technology management and in the event of outsourcing to take over the functions at a short notice at times of exigencies. Some of the common IT risks related to CBS are as follows:

i) **Ownership of Data/ process:** Data resides at the Data Centre. Establish clear ownership.

ii) **Authorization process:** Anybody with access to the CBS, including the customer himself, can enter data directly. What is the

authorization process? **If the process is not robust, it can lead to unauthorized access to the customer information.**

iii) **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.

iv) **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.

v) **Maintaining response time:** Maintaining the **interfacing software and ensuring optimum response time** and up time can be challenging.

vi) **User Identity Management:** This could be a serious issue. Some Banks may have more than **5000 users interacting with the CBS at once.**

vii) **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.

viii) **Incident handling procedures:** Incident handling procedures are used to **address and manage the aftermath of a security breach** or cyber attack. However, these at times, may not be adequate considering the need for real-time risk management.

ix) **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.**

BANKING REGULATION ACTS

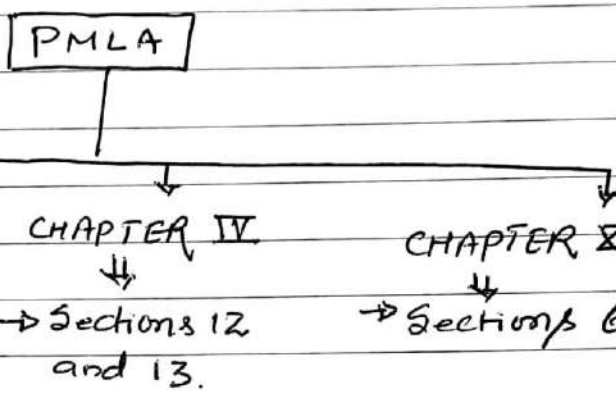
I) Negotiable Instruments Act-1881 (NIAct)

II) RBI Regulations

Some of the key functions of RBI are given here.

Topic: Prevention of Money Laundering Act: [PMLA]:

In our syllabus of EFS-SM, some sections of prevention of money laundering act are discussed.



CHAPTER II - OFFENCE OF MONEY-LAUNDERING

Section 3 : Offence of money-laundering

Whosoever,

* Acquires, owns, possesses or transfer any proceeds of crime directly or indirectly.
* Knowingly enters into any transactions related to proceeds of crime.
* Conceal, or aids/assist in concealment of proceeds of crime —

Shall be guilty of offence of money-laundering.

Chapter IV : Obligations of banking companies, financial institutions and intermediaries :

Section 12 : Reporting entity to maintain record

(1) Every reporting entity shall :-

transaction record maintain

(a) Maintain a record of all transactions, including information relating to transaction in such manner as it to enable it to reconstruct individual transaction.

nature & value of transaction as prescribed

(b) Furnish info. of transaction mentioned in clause(a) whether executed or attempted within such time as may be prescribed.

(c) Omitted.

(d) Omitted.

maintain identity record

(e) Maintain the records of the identity of all its beneficial owners and clients as well as related account files and business correspondance.

confidentiality of info maintained

(2) Every information maintained, furnished, verified, or provided under any law for time being, shall be kept confidential.

Topic _____ Date _____

5 years → Transaction records

(3) Records (Clause(a) of Subsection(1)) shall be maintained for a period of 5 years from the date of transaction.

5 years → Identity records

(4) Records (Identity records – clause(c) Subsection(1)) shall be maintained for period of 5 years after ending of business relationship between client and reporting entity or account has been closed, whichever is later.

Exemption → As notified.

(5) Central govt may exempt any reporting entity or class of reporting entity from any obligation through notification.

Section 13: Powers of Director to impose fine –

Inquiry by director

(1) Director may make inquiry or cause such inquiry to be made either on his own motion or on an application made by an authority, officer or person.

Direct (concerned Authority for records)

1(A) Director may direct concerned authority to get it's records at any stage of inquiry, as may be specified, audited by an accountant from panel of accountant mainted by central govt. for this purpose.

Topic _____ Date _____

Expenses of Audit

1(3) Expenses of any audit under sub-section 1(A) shall be borne by the central govt.

In case of failure to comply with obligation

(2) If Director finds that reporting entity or it's designated director or any employee fails to comply with obligations under this chapter then without prejudice and ignoring all other provisions of this Act he may -

warning

(a) Issue a warning in writing.

or

comply to specific instruction

(b) Direct reporting entity, director or employee to comply with specific instruction

or

Reports

(c) Direct to send reports at such interval as may be prescribed on the measures it is taking

or

Impose penalty

(d) By an order, impose penalty, not less than ten thousands which may extend upto 1 Lacs for each failure.

Order passed under sub-section (2)

(3) Director shall forward copy of order to all parties to proceedings.

Topic _____ Date _____

Chapter X Miscellaneous

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

False info to cause search or arrest.

(1) Any person willingly and maliciously giving false information and causing arrest or search made under this act shall be liable for imprisonment for a term upto 2 years or with fine which may extend upto 50 thousands rupees or both.

(2) If any person –

Refuse to answer

(a) Refuse to answer any question put to him by authority empowered by this Act, besides being legally bound to state truth of any matter relating to an offence under section 3.

or

Refuse to sign

(b) Refuse to sign any statement made by him, which an authority may legally require to sign

or

Refuse to attend

(c) Omits to attend or produce documents or accounts at the place or time besides being summoned under section 50 either to attend to give evidence or produce books of accounts or other documents.

Topic

he shall pay, by way of penalty –

* A sum not less than ₹500 which may extend to ₹10,000 for each failure.

No penalty without hearing

(3) No order → sub-section (2) under this section shall be passed unless the person on whom penalty is proposed to be imposed is given opportunity of being heard by authority.

Disobey to direction attracts IPC sec 174

(4) Notwithstanding anything contained in clause (c) of sub-section (2) –
A person who intentionally disobeys any direction issued under section 50 shall be proceeded under section 174 of IPC.

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 for 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.

INFORMATION TECHNOLOGY ACT (IT ACT)

• The Information Technology Act was passed in 2000 and amended in 2008.

• The ITA Rules were passed in 2011.

• The Amendment Act 2008 provides stronger privacy data protection measures as well as implementing reasonable information security by implementing ISO 27001 or equivalent certifiable standards to protect against cyber-crimes.

• For the banks, the Act exposes them to both civil and criminal liability.

• The civil liability could consist of exposure to pay damages by way of compensation up to 5 crores.

• There may also be exposure to criminal liability to the top management of the banks and exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions which will impact banks.

• The IT Act recognizes risks of information technology deployment in India, various types of computer- related offences and provides a legal framework for prosecution for these offences.

Some Definitions in IT Act

• The IT Act, 2000 defines the terms Access in computer network in Section 2(a), computer in Section 2(i), computer network in Section (2j), data in Section 2(o) and information in Section 2(v).

• These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime.

• **2(a) "Access"** with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

• **2(i) "Computer"** means any electronic, magnetic, optical or other high- speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

• **2(j) "Computer Network"** means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) Terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

• **2(o) "Data"** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any

form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

• **2(v) "Information"** includes data, message, text, images, sound, voice, codes, computer programmers, software and databases or micro film or computer generated micro fiche;

A. Key Provisions of IT Act

Some of key provisions of IT related offences as impacting the banks are given here.

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

If any person without permission of the owner or any other person who is in- charge of a computer, computer system or computer network -

(a) **accesses or secures access to such computer**, computer system or computer network 1[or computer resource];

(b) **downloads, copies or extracts any data,** computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) **introduces or causes to be introduced any computer contaminant or computer virus** into any computer, computer system or computer network;

(d) **damages or causes to be damaged any computer,** computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) **disrupts or causes disruption of any computer,** computer system or computer network;

(f) **denies or causes the denial of access to any person authorized to access any computer,** computer system or computer network by any means;

(g) **provides any assistance to any person to facilitate access to a computer, computer** system or computer network **in contravention of the provisions of this Act,** rules or regulations made there under;

(h) **charges the services availed of by a person to the account of another person by tampering with or manipulating any computer,** computer system, or computer network;

(i) **destroys, deletes or alters any information** residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) **steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code** used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

Section 43A: Compensation for failure to protect data.

Where a **body corporate, possessing, dealing or handling any sensitive personal data** or information in a computer resource which it owns, controls or operates, **is negligent in implementing and maintaining reasonable security practices and procedures** and thereby **causes wrongful loss or wrongful gain** to any person, such body corporate shall be **liable to pay damages by way of compensation to the person so affected.**

Section 65: Tampering with Computer Source Documents

Whoever **knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code** used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, **shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.**

Section 66: Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable **with imprisonment for a term which may extend to three years** or **with fine which may extend to 5 lakh rupees or with both.**

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

Whoever dishonestly **receives or retains any stolen computer resource or communication device knowing or having reason to believe** the same to be stolen computer resource or communication device, shall be punished with **imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.**

Section 66-C: Punishment for identity theft

Whoever, **fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person,** shall be punished with imprisonment of either description for a term which may **extend to three years** and shall also **be liable to fine which may extend to rupees one lakh.**

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

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may **extend to three years** and shall also be liable to fine which may **extend to one lakh rupees.**

Section 66-E: Punishment for violation of privacy

Whoever, **intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent,** under circumstances violating the privacy of that person, shall be punished with imprisonment which may **extend to three years or** with fine **not exceeding two lakh rupees, or with both.**

IT ACT - Comp; Comp. Syst, Comp Net.

Sections	Offence	Punishment
43	Damage	Compensation
43A	Failure to Protect Data	Compensation
65	Tampering with source document	Imp - Upto 3 Year Fine - Upto 2 Lakh or both
66	Computer related offences Section 43	Imp - Upto 3 Year Fine - Upto 5 Lakh or both
66 B	Dishonestly receiving Stolen Comp.	Imp - Upto 3 Year Fine - Upto 1 Lakh or both
66 C	Identity theft	Imp - Upto 3 Year Fine - Upto 1 Lakh
66 D	Cheating by Personation	Imp - Upto 3 Year Fine - Upto 1 Lakh
66 E	Violation of Privacy	Imp - Upto 3 Year Fine - Upto 2 Lakh or both