CHAPTER 1

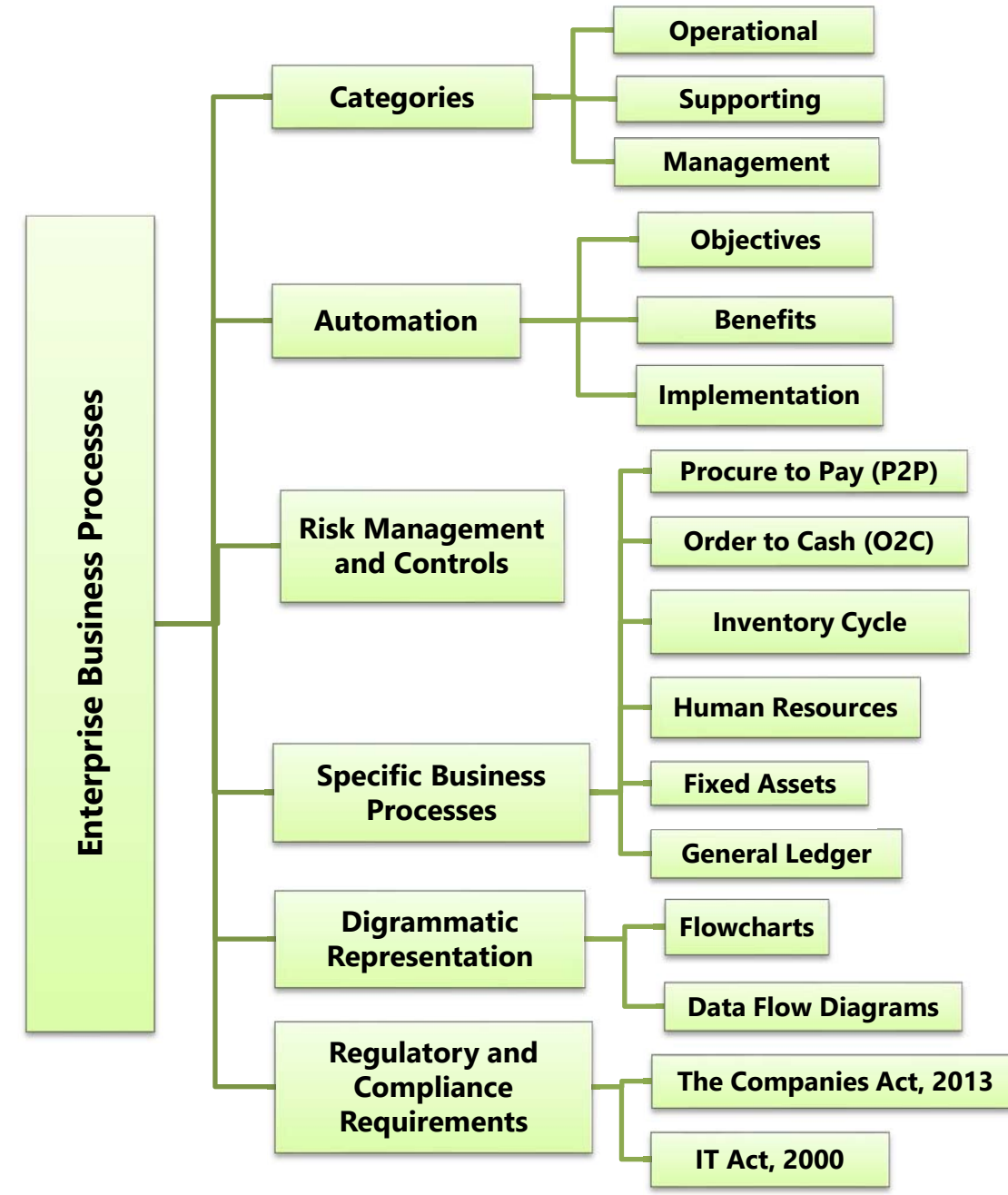
AUTOMATED BUSINESS PROCESSES

LEARNING OUTCOMES

After reading this chapter, you will be able to -

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

CHAPTER OVERVIEW



1.1 INTRODUCTION

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

The solution to this problem is provided by Enterprise Information Systems, by collecting data from numerous crucial business processes like manufacturing and production, finance and accounting, sales and marketing, and human resources and storing the data in single central data repository. An **Enterprise Information System (EIS)** may be defined as any kind of information system which improves the functions of an enterprise business processes by integration.

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

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

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

- The accounting department is notified to send the customer an invoice.
- Debtors Department keeps track of payments.
- Customer service representatives track the progress of the order through every step to inform customers about the status of their orders.

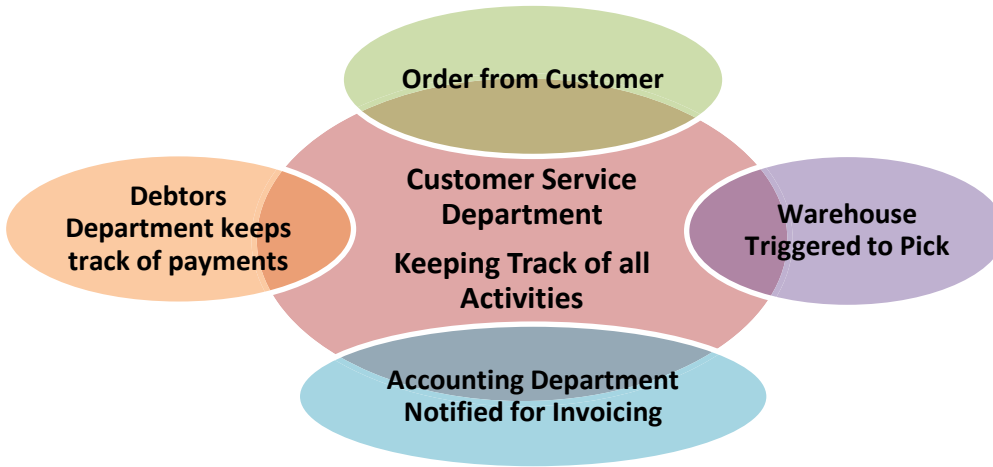


Fig. 1.1.1: Customer Service Department Activities

1.2 ENTERPRISE BUSINESS PROCESSES

A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal. Business processes are designed as per vision and mission of top management. Business processes are reflection of entities' management thought process. The success or failure of an organization is dependent on how meticulously business processes have been designed and implemented.

Business Process Management (BPM) helps an organization achieve 3E's for business processes, namely **Effectiveness**, **Efficiency** and **Economy**. BPM is a systematic approach to improving these processes. Business Process Management is an all-round activity working on a 24x7 basis to ensure improvement in all parameters all the time. The key components of business process are outlined below.

The details of these processes are shown in the Fig. 1.2.1 below:

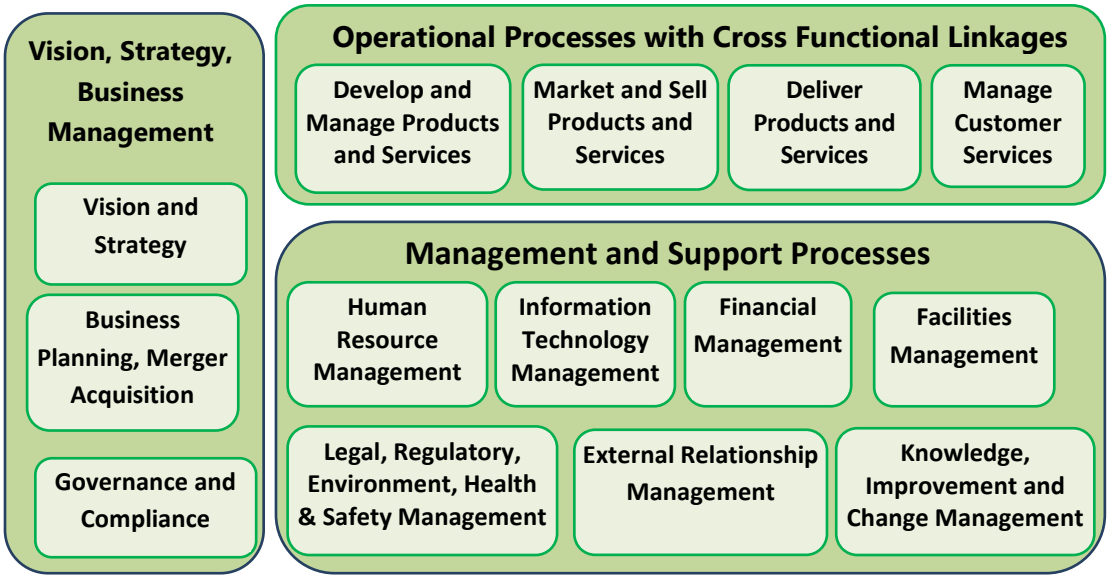


Fig. 1.2.1: Enterprise Business Process Model

The key guiding factors 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.

1.2.1 Categories of Business Processes

Depending on the organization, industry and nature of work; business processes are often broken up into different categories as shown in the Fig. 1.2.2.

Fig. 1.2.2: Categories of Business Processes

I. Operational Processes (or Primary Processes)

Operational or **Primary Processes** deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives e.g. purchasing, manufacturing, and sales. Also, Order to Cash cycle (O2C) and Purchase to Pay (P2P) cycles are associated with revenue generation.

II. Supporting Processes (or Secondary Processes)

Supporting Processes back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

Example 1.2: Human Resource Management

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

III. Management Processes

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

Example 1.3: Process of Budgeting

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

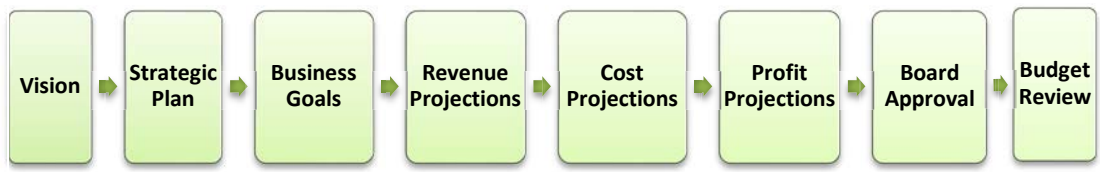


Fig. 1.2.3: Budgeting Process

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

Table 1.2.1: Examples representing all categories of Business Processes

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

1.3 AUTOMATED BUSINESS PROCESSES

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

In the days of manual accounting, most business processes were carried out manually. For example, a sales invoice would be raised manually and based on the shipment of goods, the inventory would be manually updated for reducing the stock. Subsequently, the accounting entries would be manually passed by debiting and crediting the respective accounts through journal entries. Today most of the business processes have to be automated to make enterprises more efficient and to handle the large volumes of transactions in today's world. This is what has led to **Business Process Automation (BPA)**. The manual example given above would be performed in an integrated computer system which is as follows:

- Raise invoice to customer in a computer system using relevant application software;
- The system automatically reduces the stock;
- The system instantly passes the necessary accounting entries by adding relevant transactions in relevant database tables:
  - Debit : Customer
  - Credit : Sales, Indirect Taxes
  - Debit : Cost of Goods Sold
  - Credit : Inventory

Business Process Automation (BPA) is the technology-enabled automation of activities or services that accomplish a specific function and can be implemented for many different functions of company activities including sales, management, operations, supply chain, human resources, information technology, etc. In other words, BPA is the tactic a business uses to operate efficiently and effectively. It consists of integrating applications and using software applications throughout the organization. BPA is the tradition of analyzing, documenting, optimizing and then automating business processes.

1.3.1 Factors affecting BPA Success

The success of any Business Process Automation shall only be achieved when BPA ensures the following:

- **Confidentiality:** To ensure that data is only available to persons who have right to see the same;
- **Integrity:** To ensure that no unauthorized amendments can be made in the data;

- **Availability:** To ensure that data is available when asked for; and
- **Timeliness:** To ensure that data is made available at the right time.

To ensure that all the above parameters are met, BPA needs to have appropriate internal controls put in place.

1.3.2 Benefits of Automating Business Process

A process is a repetitively used network of orderly linked activities using information and resources for transforming inputs to outputs. And the business process is the flow of information, customized by value-added tasks, that begins with the primary contact with a potential customer and continues through deliverance of a finished product. Well-developed business processes can generate a flawless link from initial customer interface through the supply chain. Automation of these processes maintains the accuracy of the information transferred and certifies the repeatability of the value-added tasks performed. Table 1.3.1 elaborates on major benefits of automating Business Processes.

Table 1.3.1: Benefits of Automating Business Processes

Quality and Consistency
♦ Ensures that every action is performed identically resulting in high quality, reliable results and stakeholders will consistently experience the same level of service.
Time Saving
♦ Automation reduces the number of tasks employees would otherwise need to do manually. ♦ It frees up time to work on items that add genuine value to the business, allowing innovation and increasing employees' levels of motivation.
Visibility
♦ Automated processes are controlled, and they consistently operate accurately within the defined timeline. It gives visibility of the process status to the organization.
Improved Operational Efficiency
♦ Automation reduces the time it takes to achieve a task, the effort required to undertake it and the cost of completing it successfully. ♦ Automation not only ensures that systems run smoothly and efficiently, but also that errors are eliminated and that best practices are constantly leveraged.

Governance and Reliability
♦ The consistency of automated processes means stakeholders can rely on business processes to operate and offer reliable services to customers, thus, maintaining a competitive advantage.
Reduced Turnaround Time
♦ Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection. This adjustment of processes distils operational performance and reduces the turnaround time for both staff and external customers.
Reduced Costs
♦ Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more. Automation allows to accomplish more by utilizing fewer resources.

1.3.3 Which Business Processes should be automated?

Technology is the enabler of Business Process Automation (BPA). BPA offers many advantages to the business. But every business process is not a good fit for automation. Companies tend to automate those business processes that are time and resource-intensive operationally or those that are subject to human error. Following are the few examples of processes that are best suited to automation:

- **Processes involving high-volume of tasks or repetitive tasks:** Many business processes such as making purchase orders involve high-volume of repetitive tasks. Automating these processes results in cost and work effort reductions.
- **Processes requiring multiple people to execute tasks:** A business process which requires multiple people to execute tasks often results in waiting time that can lead to increase in costs. For example - Help desk services. Automating these processes results in reduction of waiting time and in costs.
- **Time-sensitive processes:** Business process automation results in streamlined processes and faster turnaround times. The streamlined processes eliminate wasteful activities and focus on enhancing tasks that add value. Time-sensitive processes such as online banking system, railway/aircraft operating and control systems etc. are best suited to automation.
- **Processes involving need for compliance and audit trail:** With business process automation, every detail of a particular process is recorded. These

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

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

1.3.4 Challenges involved in Business Process Automation

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

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

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

1.3.5 BPA Implementation

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

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

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

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

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

(ii) Step 2: Understand the rules / regulation under which enterprise needs to comply with?

One of the most important steps in automating any business process is to understand the rules of engagement which include following the rules, adhering to regulations and following document retention requirements. This governance is established by a combination of internal corporate policies, external industry regulations and local, state, and central laws. Regardless of the source, it is important to be aware of their existence and how they affect the documents that drive the processes. It is important to understand that laws may require documents to be retained for specified number of years and in a specified format. Entity needs to ensure that any BPA adheres to the requirements of law.

(iii) Step 3: Document the process, we wish to automate

At this step, all the documents that are currently being used need to be documented. The following aspects need to be kept in mind while documenting the present process:

- What documents need to be captured?
- Where do they come from?
- What format are they in: Paper, FAX, email, PDF etc.?
- Who is involved in processing of the documents?
- What is the impact of regulations on processing of these documents?
- Can there be a better way to do the same job?
- How are exceptions in the process handled?

The benefit of the above process for user and entity being:

- It provides clarity on the process.
- It helps to determine the sources of inefficiency, bottlenecks, and problems.
- It allows designing the process to focus on the desired result with workflow automation.

An easy way to do this is to sketch the processes on a piece of paper, possibly in a flowchart format. Visio or even Word can be used to create flowcharts easily.

It is important to understand that no automation shall benefit the entity, if the process being automated is error-prone. Investment in hardware, workflow software and professional services, would get wasted if the processes being automated are not made error-free. Use of technology needs to be made to realize the goal of accurate, complete and timely processing of data so as to provide right information to the right people safely and securely at optimum cost.

Table 1.3.2: Steps involved in Implementing Business Process Automation

Step 1: Define why we plan to implement BPA?	• The answer to this question will provide justification for implementing BPA.
Step 2: Understand the rules/ regulation under which it needs to comply with?	• The underlying issue is that any BPA created needs to comply with applicable laws and regulations.
Step 3: Document the process, we wish to automate.	• The current processes which are planned to be automated need to be correctly and completely documented at this step.
Step 4: Define the objectives/goals to be achieved by implementing BPA.	• This enables the developer and user to understand the reasons for going for BPA. The goals need to be precise and clear.
Step 5: Engage the business process consultant.	• Once the entity has been able to define the above, the entity needs to appoint an expert, who can implement it for the entity.
Step 6: Calculate the RoI for project.	• The answer to this question can be used for convincing top management to say 'yes' to the BPA exercise.
Step 7: Development of BPA.	• Once the top management grants their approval, the right business solution has to be procured and implemented or developed and implemented covering the necessary BPA.
Step 8: Testing the BPA.	• Before making the process live, the BPA solutions should be fully tested.

(iv) Step 4: Define the objectives/goals to be achieved by implementing BPA

Once the above steps have been completed, entity needs to determine the key objectives of the process improvement activities. When determining goals, remember that goals need to be **SMART:**

- **Specific:** Clearly defined,
- **Measurable:** Easily quantifiable in monetary terms,
- **Attainable:** Achievable through best efforts,
- **Relevant:** Entity must be in need of these, and
- **Timely:** Achieved within a given time frame.

Example 1.4: Consider for the following cases-

Case 1: For vendor's offering early payment discounts, entity needs to consider:

- How much could be saved if they were taken advantage of, and if the entity has got the cash flow to do so?
- Vendor priority can be created based on above calculations, for which gets paid sooner rather than later.

Case 2: To determine the average invoice aging per customer. Entity can decide to reduce the average from 75 days to 60 days. This alone can dramatically improve cash flow.

(v) Step 5: Engage the business process consultant

This is again a critical step to achieve BPA. To decide as to which company/ consultant to partner with, depends upon the following:

- Objectivity of consultant in understanding/evaluating entity situation.
- Does the consultant have the experience with entity business process?
- Is the consultant experienced in resolving critical business issues?
- Whether the consultant can recommend and implement a combination of hardware, software and services as appropriate to meeting enterprise BPA requirements?
- Does the consultant have the required expertise to clearly articulate the business value of every aspect of the proposed solution?

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

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

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

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

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

(vii) Step 7: Developing the BPA

Once the requirements have been documented, RoI have been computed and top management approval to go ahead has been received; the consultant develops the requisite BPA. The developed BPA needs to meet the objectives for which the same is being developed.

(viii) Step 8: Testing the BPA

Once developed, it is important to test the new process to determine how well it works and identify where additional "exception processing" steps need to be included. The process of testing is an iterative process, the objective being is to remove all problems during this phase.

Testing allows room for improvements prior to the official launch of the new process, increases user adoption and decreases resistance to change. Documenting the final version of the process will help to capture all the hard work, thinking and experience which can be used to train new people.

1.3.6 Case studies on Business Processes Automation

Case 1: Automation of Purchase order generation process in a manufacturing entity

Various steps of automation are given as follows:

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

The entity has been facing the problem of non-availability of critical raw material items which is leading to production stoppages and delay in delivery. Delay in delivery has already cost company in terms of losing customer and sales.

Step 2: Understand the rules / regulation under which needs to comply with?

The item is not covered by regulation regarding quantity to be ordered or stored. To keep cost at minimum, entity has calculated economic order quantity for which orders are placed.

Step 3: Document the process, we wish to automate.

The present process is manual where the orders are received by purchase department from stores department. Stores department generates the order based on manual stock register and based on item's re-order levels. The levels were decided five years back and stores records are not updated timely.

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

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

Step 5: Engage the business process consultant.

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

Step 6: Calculate the ROI for project.

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

Step 7: Developing the BPA.

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

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

Step 8: Testing the BPA.

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

Case 2: Automation of Employees' Attendance System

Various steps of automation are given as follows:

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

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

Step 2: Understand the rules/regulation under which needs to comply with?

Numbers of regulations are applicable to employee attendance including Factories Act 1948, Payment of Wages Act 1936, State laws, etc. This is a compliance requirement and hence, any BPA needs to cater to these requirements.

Step 3: Document the process, we wish to automate.

The present system includes an attendance register and a register at the security gate. Employees are expected to put their signatures in attendance registers. The register at the gate is maintained by security staff, to mark when an employee has entered. There is always a dispute regarding the time when an employee has entered and what has been marked in the security register. The company policy specifies that an employee coming late by 30 minutes for two days in a month shall have a ½ day salary deduction. There is over-writing in attendance register, leading to heated arguments between human resource department staff and employees. As the time taken to arrive at the correct attendance is large, there is a delay in preparation of salary. The same has already led to penal action against company by labor department of the state.

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

The objective for implementing BPA is to have:

- Correct recording of attendance.
- Timely compilation of monthly attendance so that salary can be calculated and distributed on a timely basis.
- To ensure compliance with statutes.

Step 5: Engage the business process consultant.

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

Step 6: Calculate the RoI for project.

The BPA may provide tangible benefits in the form of reduced penalties and intangible benefits which may include:

- Better employee motivation and morale,
- Reduced differences between employees,

- More focus on work rather than salary, and
- Improved productivity.

Step 7: Developing the BPA.

Implementing BPA includes would result in the following:

- All employees would be given electronic identity cards.
- The cards would contain details about employees.
- The attendance system would work in the following manner:
  - Software with card reading machine would be installed at the entry gate.
  - Whenever an employee enters or leaves the company, he/she needs to put the card in front of machine.
  - The card reading machine would be linked to the software which would record the attendance of the employee.
  - At the end of month, the software would print attendance reports employee-wise. These reports would also point out how many days an employee has reported late in the month.
  - Based on this report, monthly attendance is put in the system to generate the monthly salary.

Step 8: Testing the BPA.

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

The above illustrations are of entities which have gone for business process automation. There are thousands of processes across the world for which entities have gone for BPA and reaped numerous benefits. These include tracking movement of goods, ales order processing customer services departments, Inventory management, Employee Management System, and Asset tracking systems.

1.4 RISK AND ITS MANAGEMENT

1.4.1 Introduction

Various terminologies relating to risk and its management are as follows:

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.

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

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

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

- 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'.

Exposure: An exposure is defined as an extent of loss an 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 determine the consequence of the attack.

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 counter measures may be used.

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

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

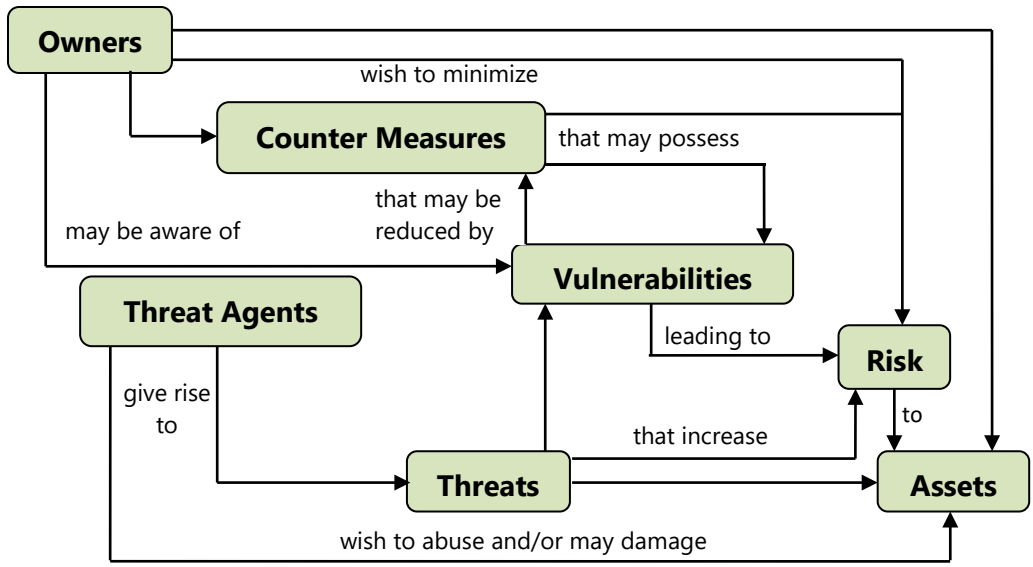


Fig. 1.4.1: Risk and Related Terms

1.4.2 Sources of Risk

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

political circumstances, technology and technical issues, management activities and controls, and individual activities.

Broadly, risk has the following characteristics:

- Potential loss that exists as the result of threat/vulnerability process. Threats have the potential to cause damage or loss. A risk is an expectation that a threat may succeed, and the potential damage can occur.
- Uncertainty of loss expressed in terms of probability of such loss. The extent of loss includes not only the immediate direct financial loss but also the loss due to its impact in the long run. Loss in the long run includes losses such as loss of business, loss of reputation, etc.
- The probability / likelihood that a threat agent may mount a specific attack against a particular system. The assessment of both the likelihood/probability of occurrence and the consequence of risk is a high probability event.

To conclude, Risk can be defined as the potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset.

1.4.3 Types of Risks

The risks can be broadly categorized as follows:

A. Business Risks: Business risk is a broad category which applies to any event or circumstances related to business goals. Businesses face all kinds of risks ranging from serious loss of profits to even bankruptcy and are discussed below:

- **Strategic Risks:** These are the risks that would prevent an organization from accomplishing its objectives (meeting its goals). Examples include risks related to strategy, political, economic relationship issues with suppliers and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs.
- **Financial Risks:** Financial risks are those risks 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) Risks:** This includes risks 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, lack of due diligence, protection of personal data in accordance with

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

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

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

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

(ii) **Frequent changes or obsolescence of technology:** Technology keeps on evolving and changing constantly and becomes obsolete very quickly. Hence, there is always a challenge that the investment in technology solutions unless properly planned may result in loss to the organization due to risk of obsolescence.

(iii) **Multiplicity and complexity of systems:** The technology architecture used for services could include multiple digital platforms and is quite complex. Hence, this requires the personnel to have knowledge about requisite technology skills or the management of the technology could be outsourced to a company having the relevant skill set.

(iv) **Different types of controls for different types of technologies/systems:** Deployment of technology often gives rise to new types of risks. These risks need to be mitigated by relevant controls as applicable to the technology/information systems deployed.

(v) **Proper alignment with business objectives and legal/regulatory requirements:** Organizations must ensure that the systems implemented cater to all the business objectives and needs, in addition to the legal/regulatory requirements envisaged.

(vi) **Dependence on vendors due to outsourcing of IT services:** In a systems environment, the organization requires staff with specialized domain skills to manage IT deployed. Hence, these services could be outsourced to vendors and there is heavy dependency on vendors and gives rise to vendor risks which should be managed by proper contracts, controls and monitoring.

(vii) **Vendor related concentration risks:** There may not be one but multiple vendors providing different services. For example, network, hardware, system software and application software services may be provided by different vendors or these services may be provided by a single vendor. Both these situations result in higher risks due to heavy dependence on vendors.

(viii) **Segregation of Duties (SoD):** Organizations may have a highly-defined organization structure with clearly defined roles, authority and responsibility. The Segregation of Duties as per organization structure should be clearly mapped. This is a high-risk area since any SoD conflicts can be a potential vulnerability for fraudulent activities. For example, if a single employee can initiate, authorize and disburse a loan, the possibility of misuse cannot be ignored.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4.4 Risk Management Strategies

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

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

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

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

1.5 ENTERPRISE RISK MANAGEMENT (ERM)

In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy.

The Sarbanes Oxley Act (SOX) in the US, which focuses on the implementation and review of internal controls as relating to financial audit, highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented. How controls are implemented would be dependent on the overall risk management strategy and risk appetite of the management.

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

The underlying premise of Enterprise Risk Management is that every entity, whether for profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty an entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. ERM provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

ERM in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM is a common framework applied by business management and other personnel to identify potential events that may affect the enterprise, manage the associated risks and opportunities, and provide reasonable assurance that an enterprise's objectives will be achieved.

1.5.1 Benefits of Enterprise Risk Management

No entity operates in a risk-free environment and ERM does not create such an environment. Rather, it enables management to operate more effectively in environments filled with risks. ERM provides enhanced capability to do the following:

- **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad-based level that an enterprise (any type of entity) is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
- **Link growth, risk and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
- **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.

- **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital:** More robust information on an entity's total risk allows management to assess more effectively overall capital needs and improve capital allocation.

1.5.2 Enterprise Risk Management (ERM) Framework

ERM provides a framework for risk management which typically involves identifying events or circumstances relevant to an organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. Various potential threats to computer system affect the Confidentiality, Integrity, and Availability of data and computer system. For successful continuity of business, it is very essential to evaluate these potential threats and control them so as to minimize the impact of these threats to an acceptable level. By identifying and pro-actively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

ERM is a risk-based approach which includes the methods and processes used by organizations to manage risks. ERM provides a framework for risk management which involves:

- identifying potential threats or risks.
- determining how big a threat or risk is, what could be its consequence, its impact, etc.
- implementing controls to mitigate the risks.

ERM framework consists of eight interrelated components that are derived from the way management runs a business and are integrated with the management process. These components are as follows:

(i) **Internal Environment:** The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any

business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

(ii) **Objective Setting:** Objectives should be set before management can identify events potentially affecting their achievement. ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.

(iii) **Event Identification:** Potential events that might have an impact on the entity should be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Opportunities are channelled back to management's strategy or objective-setting processes. Management identifies inter-relationships between potential events and may categorize events to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective.

(iv) **Risk Assessment:** Identified risks are analysed to form a basis for determining how they should be managed. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

(v) **Risk Response:** Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

(vi) **Control Activities:** Policies and procedures are established and executed to help ensure that the risk responses that management selected are effectively carried out.

(vii) **Information and Communication:** Relevant information is identified, captured and communicated in a form and time frame that enables people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective

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

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

1.6 CONTROLS

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

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

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

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

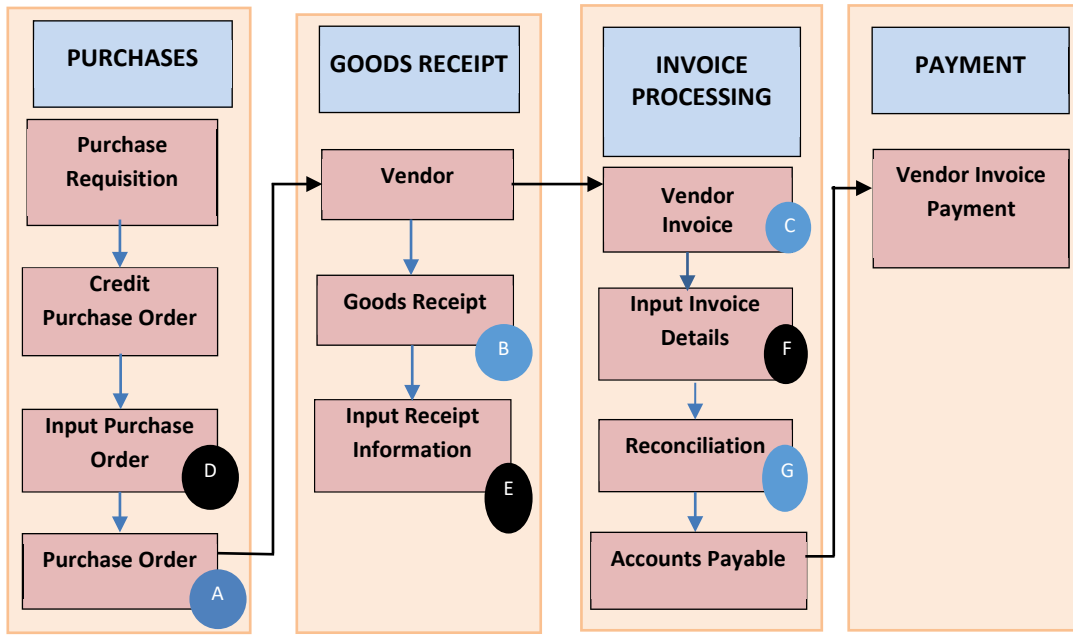


Fig. 1.6.1: Purchase Cycle – Sample Controls

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

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

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

- **Automated Control:** The above verification is done automatically by the computer system by comparing (D), (E) & (F) and exceptions highlighted.
- **Semi-Automated Control:** Verification of Goods Receipt (E) with PO (D) could be automated but the vendor invoice matching could be done manually in a reconciliation process (G).

1.6.1 Importance of IT Controls

IT Control objectives is defined as: "A statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity". Implementing right type of controls is responsibility of management. Controls provide a clear policy and good practice for directing and monitoring performance of IT to achieve enterprise objectives. IT Controls perform dual role which is as follows:

(i) They enable enterprise to achieve objectives; and

(ii) They help in mitigating risks.

Many issues drive the need for implementing IT controls. These range from the need to control costs and remain competitive to the need for compliance with internal and external governance. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. Any control that mitigates or detects fraud or cyber-attacks enhances the organization's resiliency because it helps the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls which enable a well-controlled organization-to manage challenges or disruptions seamlessly.

1.6.2 Applying IT Controls

It is important for an organization to identify controls as per policy, procedures and its structure and configure it within IT software as used in the organization.

There are different options for implementing controls as per risk management strategy. For example, the way banking is done in a nationalized bank is traditional way with rigid organization structure of managers at different levels, officers and clerks and clear demarcation between departments and functions whereas in a private sector, the organization structure is organized around customers and focused on relationship banking.

A common classification of IT controls is **General Controls** and **Application Controls**. **General Controls** are macro in nature and are applicable to all applications and data resources. **Application Controls** are controls which are specific to the application software such as payroll, accounts payable, and billing, etc.

(a) Information Technology General Controls (ITGC)

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

General controls include, but are not limited to:

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

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

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

- **User training and qualification of Operations personnel:** The personnel deployed have required competencies and skillsets to operate and monitor the IT environment. These competencies should be consistent with the competencies required by the organization of the relevant role. Moreover, training may be used as a tool to develop the competencies and skillsets to work in IT environment.

It is important to note that proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls. In later sections, detailed risk and control matrix for various types of general controls are provided.

(b) Application Controls

Application represents the interface between the user and the business functions. **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. For example: In banking, application software ensures that 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-

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

1.6.3 Key indicators of effective IT controls

The IT controls implemented in an organization are considered to be effective on the basis of following criteria:

- The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services.
- Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.
- Ability to allocate resources predictably.

- Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.
- Clear communication to management of key indicators of effective controls.
- The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently.
- The efficient use of a customer support center or help desk.
- Heightened security awareness on the part of the users and a security conscious culture.

1.6.4 Framework of Internal Control as per Standards on Auditing

A company's management team is responsible for the development of internal control policies and procedures. SA315 defines the system of Internal Control as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives regarding reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations".

An Internal Control System -

- facilitates the effectiveness and efficiency of operations.
- helps ensure the reliability of internal and external financial reporting.
- assists compliance with applicable laws and regulations.
- helps safeguarding the assets of the entity.

As per SA315, the five components of any internal control as they relate to a financial statement audit are explained below. All these components must be present to conclude that internal control is effective.

I. Control Environment

The **Control Environment** is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and Senior Management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out

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

II. Risk Assessment

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

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

Risk Assessment includes the following:

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

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

III. Control Activities

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

levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations and business performance reviews.

Broadly, the control activities include the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

IV. Information and Communication

Information is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Pertinent information must be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. **Communication** is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the enterprise, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities should be taken seriously. External communication is two-fold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

V. Monitoring of Controls

Monitoring of Controls is an ongoing cyclical process. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control including controls to affect the principles within each component is present and functioning. Ongoing evaluations built into business processes at different levels of the entity, provide timely information. Separate evaluations conducted periodically will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated

against management's criteria and deficiencies are communicated to management and the Board of Directors as appropriate.

1.6.5 Limitations of Internal Control System

Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Internal control systems are subject to certain inherent limitations, such as:

- Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.
- The fact that most internal controls do not tend to be directed at transactions of unusual nature, the reasonable potential for human error such as – due to carelessness, distraction, mistakes of judgment and misunderstanding of instructions.
- The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.
- Manipulations by management with respect to transactions or estimates and judgments required in the preparation of financial statements.

1.7 RISKS AND CONTROLS FOR SPECIFIC BUSINESS PROCESSES

1.7.1 Business Processes - Risks and Controls

Suitable controls should be implemented to meet the requirements of the control objectives. These controls can be manual, automated or semi-automated provided the risk is mitigated. Based on the scenario, the controls can be **Preventive**, **Detective** or **Corrective**. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction. In computer systems, controls should be checked at three levels, namely **Configuration**, **Masters** and **Transaction** level.

1. Configuration

Configuration refers to the way a software system is set up. Configuration is the methodical process of defining options that are provided during system setup.

When any software is installed, values for various parameters should be set up (configured) as per policies and business process work-flow and business process rules of the enterprise. The various modules of the enterprise such as Purchase, Sales, Inventory, Finance, User Access etc. must be configured. Configuration will define how software will function and what menu options are displayed.

Example 1.7: Some examples of configuration are given below:

- Mapping of accounts to front end transactions like purchase and sales.
- Control on parameters: Creation of Customer Type, Vendor Type, year-end process.
- User activation and deactivation.
- User Access and privileges - Configuration & its management.
- Password Management.

2. Masters

Masters refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, and Finance etc. These drive how the software will process relevant transactions. The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed. Examples are Vendor Master, Customer Master, Material Master, Accounts Master, Employee Master etc. Any changes to these data have to be authorized by appropriate personnel and these are logged and captured in exception reports. The way masters are set up will drive the way software will process transactions of that type. For example - The Customer Master will have the credit limit of the customer. When an invoice is raised, the system will check against the approved credit limit and if the amount invoiced is within the credit limit, the invoice will be created, if not the invoice will be put on "credit hold" till proper approvals are obtained.

Example 1.8: Some examples of Masters are given below:

- **Vendor Master:** Credit period, vendor bank account details, etc.
- **Customer Master:** Credit limit, Bill to address, Ship to address, etc.
- **Material Master:** Material type, Material description, Unit of measure, etc.
- **Employee Master:** Employee name, designation, salary details, etc.

3. Transactions

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

Implementation or review of specific business process can be done from risk or control perspective. In case of risk perspective, we need to consider each of the key sub-processes or activities performed in a business process and look at existing and related control objectives and existing controls and the residual risks after application of controls. The residual risk should be knowingly accepted by the management.

If we review this from a control objective perspective, then for each key sub-process or activity, we will consider what is sought to be achieved by implementing controls and then evaluate whether risks are mitigated by controls which are implemented at present and what are the residual risks and whether there is need to complement/add more controls.

Given below are some examples of risks and controls for a few business processes. The checklist provided below is illustrative. It is not necessary that all the sub-processes/activities given below are applicable for all enterprises. However, they are provided to build an understanding of the sub-processes, risk and related controls and control objectives. This list can be practically used for implementation/evaluation of risk/controls of business processes detailed below. However, it should be customized specifically as per the nature of business processes and how these are implemented in the enterprise. The checklist given below is categorized into Configuration, Masters and Transactions.

1.7.2 Procure to Pay (P2P) – Risks and Controls

Procure to Pay (Purchase to Pay or P2P) is the process of obtaining and managing the raw materials needed for manufacturing a product or providing a service. It involves the transactional flow of data that is sent to a supplier as well as the data that surrounds the fulfillment of the actual order and payment for the product or service. Using automation, it should be possible to have a seamless procure to pay process covering the complete life-cycle from point of order to payment.

Masters

Table 1.7.1: Risks and Control Objectives (Masters-P2P)

Risk	Control Objective
Unauthorized changes to supplier master file.	Only valid changes are made to the supplier master file.
All valid changes to the supplier master file are not input and processed.	All valid changes to the supplier master file are input and processed.
Changes to the supplier master file are not correct.	Changes to the supplier master file are accurate.
Changes to the supplier master file are delayed and not processed in a timely manner.	Changes to the supplier master file are processed in a timely manner.
Supplier master file data is not up to date.	Supplier master file data remains up to date.
System access to maintain vendor masters has not been restricted to the authorized users.	System access to maintain vendor masters has been restricted to the authorized users.

Transactions

Table 1.7.2: Risks and Control Objectives (Transactions-P2P)

Risk	Control Objective
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Purchase orders issued are not input and processed.	All purchase orders issued are input and processed.
Amounts are posted in accounts payable for goods or services not received.	Amounts posted to accounts payable represent goods or services received.
Amounts posted to accounts payable are not properly calculated and recorded.	Accounts payable amounts are accurately calculated and recorded.

Amounts for goods or services received are not input and processed in accounts payable.	All amounts for goods or services received are input and processed to accounts payable.
Amounts for goods or services received are recorded in the wrong period.	Amounts for goods or services received are recorded in the appropriate period.
Accounts payable amounts are adjusted based on unacceptable reasons.	Accounts payable are adjusted only for valid reasons.
Credit notes and other adjustments are not accurately calculated and recorded.	Credit notes and other adjustments are accurately calculated and recorded.
All valid credit notes and other adjustments related to accounts payable are not input and processed.	All valid credit notes and other adjustments related to accounts payable are input and processed.
Credit notes and other adjustments are recorded in the wrong period.	Credit notes and other adjustments are recorded in the appropriate period.
Disbursements are made for goods and services that have not been received.	Disbursements are made only for goods and services received.
Disbursements are distributed to unauthorized suppliers.	Disbursements are distributed to the appropriate suppliers.
Disbursements are not accurately calculated and recorded.	Disbursements are accurately calculated and recorded.
All disbursements are not recorded.	All disbursements are recorded.
Disbursements are recorded for an inappropriate period.	Disbursements are recorded in the period in which they are issued.
Adjustments to inventory prices or quantities are not recorded promptly and not done in the appropriate period.	Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

1.7.3 Order to Cash (O2C) – Risks and Controls

Order to Cash (OTC or O2C) is a set of business processes that involve receiving and fulfilling customer requests for goods or services. It is a set of business

processes that involve receiving and fulfilling customer requests for goods or services. Refer Fig 1.7.1.

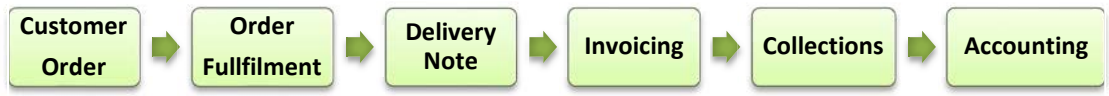


Fig. 1.7.1: Order to Cash Process

Fig. 1.7.1 depicts an O2C cycle that consists of multiple sub-processes including:

1. **Customer Order:** Customer order received is documented;
2. **Order fulfillment:** Order is fulfilled or service is scheduled;
3. **Delivery Note:** Order is shipped to customer or service is performed;
4. **Invoicing:** Invoice is created and sent to customer;
5. **Collections:** Customer sends payment /Collection; and
6. **Accounting:** Payment is recorded in general ledger.

Risks and Control Objectives (Masters-O2C) and Risks and Control Objectives (Transactions-O2C) are provided below in Tables 1.7.3 and 1.7.4 respectively.

Masters

Table 1.7.3: Risks and Control Objectives (Masters-O2C)

Risk	Control Objective
The customer master file is not maintained properly, and the information is not accurate.	The customer master file is maintained properly, and the information is accurate.
Invalid changes are made to the customer master file.	Only valid changes are made to the customer master file.
All valid changes to the customer master file are not input and processed.	All valid changes to the customer master file are input and processed.
Changes to the customer master file are not accurate.	Changes to the customer master file are accurate.
Changes to the customer master file are not processed in a timely manner.	Changes to the customer master file are processed in a timely manner.

Customer master file data is not up-to-date and relevant.	Customer master file data is up to date and relevant.
System access to maintain customer masters has not been restricted to the authorized users.	System access to maintain customer masters has been restricted to the authorized users.

Transactions

Table 1.7.4: Risks and Control Objectives (Transactions-O2C)

Risk	Control Objective
Orders are processed exceeding customer credit limits without approvals.	Orders are processed only within approved customer credit limits.
Orders are not approved by management as to prices and terms of sale.	Orders are approved by management as to prices and terms of sale.
Orders and cancellations of orders are not input accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely and accurately to the shipping and invoicing activities.	Order entry data are transferred completely and accurately to the shipping and invoicing activities.
All orders received from customers are not input and processed.	All orders received from customers are input and processed.
Invalid and unauthorized orders are input and processed.	Only valid and authorized orders are input and processed.
Invoices are generated using unauthorized terms and prices.	Invoices are generated using authorized terms and prices.
Invoices are not accurately calculated and recorded.	Invoices are accurately calculated and recorded.
Credit notes and adjustments to accounts receivable are not accurately calculated and recorded.	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.
Goods shipped are not invoiced.	All goods shipped are invoiced.
Credit notes for all goods returned and adjustments to accounts receivable are not issued in accordance with organization policy.	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.

Invoices are raised for invalid shipments.	Invoices relate to valid shipments.
Credit notes do not pertain to a return of goods or other valid adjustments.	All credit notes relate to a return of goods or other valid adjustments.
Invoices are not recorded in the system.	All invoices issued are recorded.
Credit notes issued are not recorded in the system	All credit notes issued are recorded.
Invoices are recorded in the wrong period.	Invoices are recorded in the appropriate period.
Credit notes are recorded in the wrong accounting period.	Credit notes issued are recorded in the appropriate accounting period.
Cash receipts are not recorded in the period in which they are received.	Cash receipts are recorded in the period in which they are received.
Cash receipts data are not entered correctly.	Cash receipts data are entered for processing accurately.
Cash receipts are not entered in the system for processing.	All cash receipts data are entered for processing.
Cash receipts data are not valid and are not entered in the system for processing more than once.	Cash receipts data are valid and are entered for processing only once.
Cash discounts are not accurately calculated and recorded.	Cash discounts are accurately calculated and recorded.
Collection of accounts receivable is delayed and not properly monitored.	Timely collection of accounts receivable is monitored.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

1.7.4 Inventory Cycle – Risks and Controls

The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory. The term "Inventory Cycle" means different things to companies in different verticals. For those who source, assemble and create inventory; it refers to a time-based

process which is basic to understanding how to maximize resources and cash flow. To businesses that buy, store and sell inventory; it focuses on the process of understanding, planning and managing inventory levels, from purchasing through more-efficient auditing. The typical phases of the Inventory Cycle for Manufacturers are as follows:

1. **The Ordering phase:** The amount of time it takes to order and receive raw materials.
2. **The Production phase:** The work in progress phase relates to time it takes to convert the raw material to finished goods ready for use by customer.
3. **The finished goods and delivery phase:** The finished goods that remain in stock and the delivery time to the customer. The inventory cycle is measured in number of days.

Risks and Control Objectives (Masters-Inventory) and Risks and Control Objectives (Transactions- Inventory) are provided below in Tables 1.7.5 and 1.7.6 respectively.

Masters

Table 1.7.5: Risks and Control Objectives (Masters-Inventory)

Risk	Control Objective
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.
Invalid changes to the inventory management master file are input and processed.	All valid changes to the inventory management master file are input and processed.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.
Changes to the inventory management master file are not promptly processed.	Changes to the inventory management master file are promptly processed.
Inventory management master file data is not up to date.	Inventory management master file data remain up to date.
System access to maintain inventory masters has not been restricted to the authorized users.	System access to maintain inventory masters has been restricted to the authorized users.

Transactions

Table 1.7.6: Risks and Control Objectives (Transactions-Inventory)

Risk	Control Objective
Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Raw materials received are not recorded accurately.	Raw materials received are recorded accurately.
Raw materials received are not recorded in system.	All raw materials received are recorded.
Receipts of raw materials are not recorded promptly and not in the appropriate period.	Receipts of raw materials are recorded promptly and in the appropriate period.
Defective raw materials are not returned promptly to suppliers.	Defective raw materials are returned promptly to suppliers.
Transfers of raw materials to production are not recorded accurately and are not in the appropriate period.	All transfers of raw materials to production are recorded accurately and in the appropriate period.
Direct and indirect expenses associated with production are not recorded accurately and are posted in an inappropriate period.	All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.
Transfers of completed units of production to finished goods inventory are not recorded completely and accurately and are posted in an inappropriate period.	All transfers of completed units of production to finished goods inventory are recorded completely and accurately in the appropriate period.
Finished goods returned by customers are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods returned by customers are recorded completely and accurately in the appropriate period.
Finished goods received from production are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods received from production are recorded completely and accurately in an appropriate period.

Shipments are not recorded in the system.	All shipments are recorded in the system.
Shipments are not recorded accurately.	Shipments are recorded accurately.
Shipments are not recorded promptly and are in an inappropriate period.	Shipments are recorded promptly and in the appropriate period.
Inventory is reduced when goods are not shipped and made based on unapproved customer orders.	Inventory is reduced only when goods are shipped with approved customer orders.
Costs of shipped inventory are not transferred from inventory to cost of sales.	Costs of shipped inventory are transferred from inventory to cost of sales.
Costs of shipped inventory are not accurately recorded.	Costs of shipped inventory are accurately recorded.
Amounts posted to cost of sales does not represent those associated with shipped inventory.	Amounts posted to cost of sales represent those associated with shipped inventory.
Costs of shipped inventory are not transferred from inventory to cost of sales promptly and not done in the appropriate period.	Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.
System access to process inventory related transactions has not been restricted to the authorized users.	System access to process inventory related transactions has been restricted to the authorized users.

1.7.5 Human Resources – Risks and Controls

The **Human Resources (HR)** life cycle refers to human resources management and covers all the stages of an employee's time within a specific enterprise and the role the human resources department plays at each stage. Typical stage of HR cycle includes the following:

1. **Recruiting and On-boarding:** Recruiting is the process of hiring a new employee. The role of the human resources department in this stage is to assist in hiring. This might include placing the job ads, selecting candidates whose resumes look promising, conducting employment interviews and administering assessments such as personality profiles to choose the best applicant for the position. In a small business where the owner performs these duties personally, the HR person would assist in a support role. In some organizations, the

recruiting stage is referred to as "hiring support." On-boarding is the process of getting the successful applicant set up in the system as a new employee.

2. **Orientation and Career Planning:** Orientation is the process by which the employee becomes a member of the company's work force through learning his/her new job duties, establishing relationships with co-workers and supervisors and developing a niche. Career planning is the stage at which the employee and his/her supervisors work out her long-term career goals with the company. The human resources department may make additional use of personality profile testing at this stage to help the employee determine his/her best career options with the company.

3. **Career Development:** Career development opportunities are essential to keep an employee engaged with the company over time. After an employee has established himself/herself at the company and determined his long-term career objectives, the human resources department should try to help him/her meet his/her goals, if they are realistic. This can include professional growth and training to prepare the employee for more responsible positions with the company. The company also assesses the employee's work history and performance at this stage to determine whether he has been a successful hire.

4. **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. Others will choose to move on to other opportunities or be laid off. Whatever the reason, all employees will eventually leave the company. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed, carrying out an exit interview if that is company policy and removing the employee from the system. These stages can be handled internally or with the help of enterprises that provide services to manage the employee life cycle.

Risks and Control Objectives (Configuration-Human Resources) and Risks and Control Objectives (Masters-Human Resources) are provided below in Tables 1.7.7 and 1.7.8 respectively.

Configuration

Table 1.7.7: Risks and Control Objectives (Configuration-Human Resources)

Risk	Control Objective
Employees who have left the company continue to have system access.	System access to be immediately removed from employees who leave the company.

Employees have system access in excess of their job requirements.	Employees should be given system access based on a "need to know" basis and to perform their job function.

Masters

Table 1.7.8: Risks and Control Objectives (Masters-Human Resources)

Risk	Control Objective
Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
Terminated employees are not removed from the payroll master files.	Terminated employees are removed from the payroll master files.
Employees are terminated without following statutory requirements.	Employees are terminated only within statutory requirements.
Deletions from the payroll master files do not represent valid terminations.	Deletions from the payroll master files represent valid terminations.
Invalid changes are made to the payroll master files.	Only valid changes are made to the payroll master files.
Changes to the payroll master files are not accurate.	Changes to the payroll master files are accurate.
Changes to the payroll master files are not processed in a timely manner.	Changes to the payroll master files are processed in a timely manner.
Payroll master file data is not up to date.	Payroll master file data remain up to date.
Payroll is disbursed to inappropriate employees.	Payroll is disbursed to appropriate employees.
System access to process employee master changes has not been restricted to the authorized users.	System access to process employee master changes has been restricted to the authorized users.

1.7.6 Fixed Assets – Risks and Controls

Fixed Assets process ensures that all the fixed assets of the enterprise are tracked for the purposes of financial accounting, preventive maintenance, and theft deterrence. Fixed assets process ensures that all fixed assets are tracked, and fixed

asset record maintains details of location, quantity, condition, and maintenance and depreciation status. Typical steps of fixed assets process are as follows:

1. **Procuring an asset:** An asset is most often entered into the accounting system; when the invoice for the asset is entered into the accounts payable or purchasing module of the system.
2. **Registering or adding an asset:** Most of the information needed to set up the asset for depreciation is available at the time the invoice is entered. Information entered at this stage could include acquisition date, placed-in-service date, description, asset type, cost basis, depreciable basis etc.
3. **Adjusting the Assets:** Adjustments to existing asset information is often needed to be made. Events may occur that can change the depreciable basis of an asset. Further, there may be improvements or repairs made to asset that either adds value to the asset or extend its economic life.
4. **Transferring the Assets:** A fixed asset may be sold or transferred to another subsidiary, reporting entity, or department within the company. These inter-company and intra-company transfers may result in changes that impact the asset's depreciable basis, depreciation, or other asset data. This needs to be reflected accurately in the fixed assets management system.
5. **Depreciating the Assets:** The decline in an asset's economic and physical value is called Depreciation. Depreciation is an expense which should be periodically accounted on a company's books, and allocated to the accounting periods, to match income and expenses. Sometimes, the revaluation of an asset, may also result in appreciation of its value.
6. **Disposing the Assets:** When a fixed asset is no longer in use, becomes obsolete, or is beyond repair; the asset is typically disposed. When an asset is taken out of service, depreciation cannot be charged on it. There are multiple types of disposals such as abandonments, sales, and trade-ins. Any difference between the book value and realized value is reported as a gain or loss.

Tables 1.7.9 and 1.7.10 given below provide Risks and Control Objectives (Masters-Fixed Assets) and Risks and Control Objectives (Transactions-Fixed Assets) respectively.

Masters

Table 1.7.9: Risks and Control Objectives (Masters-Fixed Assets)

Risk	Control Objective
Invalid changes are made to the fixed asset register and/or master file.	Only valid changes are made to the fixed asset register and/or master file.
Valid changes to the fixed asset register and/or master file are not input and processed.	All valid changes to the fixed asset register and/or master file are input and processed.
Changes to the fixed asset register and/or master file are not accurate.	Changes to the fixed asset register and/or master file are accurate.
Changes to the fixed asset register and/or master file are not promptly processed.	Changes to the fixed asset register and/or master file are promptly processed.
Fixed asset register and/or master file data are not kept up to date.	Fixed asset register and/or master file data remain up to date.
System access to fixed asset master file/system configuration is not restricted to the authorized users.	System access to fixed asset master file/system configuration is restricted to the authorized users.
System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has not been correctly defined.	System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has been correctly defined.

Transactions

Table 1.7.10: Risks and Control Objectives (Transactions-Fixed Assets)

Risk	Control Objective
Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
Fixed asset acquisitions are not recorded.	All fixed asset acquisitions are recorded.
Depreciation charges are not accurately calculated and recorded.	Depreciation charges are accurately calculated and recorded.

Depreciation charges are not recorded in the appropriate period.	All depreciation charges are recorded in the appropriate period.
Fixed asset disposals/transfers are not recorded.	All fixed asset disposals/transfers are recorded.
Fixed asset disposals/transfers are not accurately calculated and recorded.	Fixed asset disposals/transfers are accurately calculated and recorded.
Fixed asset disposals/transfers are not recorded in the appropriate period.	Fixed asset disposals/transfers are recorded in the appropriate period.
Records of fixed asset maintenance activity are not accurately maintained.	Records of fixed asset maintenance activity are accurately maintained.
Fixed asset maintenance activity records are not updated in a timely manner.	Fixed asset maintenance activity records are updated in a timely manner.
Accounting entries pertaining to acquisition, disposals, transfers, retirement are not recorded in the correct General Ledger(GL) account.	Accounting entries pertaining to acquisition, disposals, transfers, retirement are recorded in the correct GL account.
System access to process fixed asset transactions has not been restricted to the authorized users.	System access to process fixed asset transactions has been restricted to the authorized users.

1.7.7 General Ledger – Risks and Controls

General Ledger (GL) process refers to the process of recording the transactions in the system to finally generating the reports from financial transactions entered in the system. The input for GL Process Flow is the financial transactions and the outputs are various types of financial reports such as balance sheet, profit and loss a/c, funds flow statement, ratio analysis, etc. The typical steps in general ledger process flow are as follows:

1. Entering financial transactions into the system
2. Reviewing Transactions
3. Approving Transactions
4. Posting of Transactions
5. Generating Financial Reports

Risks and Control Objectives (Configuration-General Ledger); Risks and Control Objectives (Masters-General Ledge) and Risks and Control Objectives (Transactions-General Ledger) are provided below in Tables 1.7.11, 1.7.12 and 1.7.13 respectively.

Configuration

Table 1.7.11: Risks and Control Objectives (Configuration-General Ledger)

Risk	Control Objective
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.
System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliations to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliations to confirm accuracy of such accounts.
Systems do not generate reports of all recurring and non-recurring journal entries for review by management for accuracy.	Systems generate reports of all recurring and non-recurring journal entries for review by management for accuracy.
Non-standard journal entries are not tracked and are inappropriate.	All non-standard journal entries are tracked and are appropriate.
Out-of-balance entries are not prohibited.	Out-of-balance entries are prohibited.
Enterprise-wide consolidation including standard inter-company eliminations, is not automated and not performed.	Enterprise-wide consolidation including standard inter-company eliminations, is automated and performed.
Variance reports are not generated for use to identify posting errors/out-of-balance conditions.	Variance reports are generated for use to identify posting errors/out-of-balance conditions.
System controls are not in place for appropriate approval of write-offs.	System controls are in place for appropriate approval of write-offs.
Journal entries of exceptional amount that were posted to the general ledger during the month are not flagged by the system and not subsequently reviewed for accuracy	Journal entries of exceptional amount that were posted to the general ledger during the month are flagged by the system and subsequently reviewed for

and approved by the controller or CFO after month-end.	accuracy and approved by the controller or CFO after month-end.
Automated amortization timing, periods and methods are not appropriate and not accurately entered.	Automated amortization timing, periods and methods are appropriate and accurately entered.
Standard, recurring period-end journal entries submitted from subsidiary ledger systems are not automated, not appropriately approved and not entered accurately.	Standard, recurring period-end journal entries submitted from subsidiary ledger systems are automated, appropriately approved and entered accurately.
Transactions can be recorded outside of financial close cut-off requirements.	Transactions cannot be recorded outside of financial close cut-off requirements.
The sources of all entries are not readily identifiable.	The sources of all entries are readily identifiable.
Transactions are not rejected, accepted and identified, on exception reports in the event of data exceptions.	Transactions are rejected, or accepted and identified, on exception reports in the event of data exceptions.
Account mappings are not up to date.	Account mappings are up to date.
Adding to or deleting general ledger accounts are not limited to authorize accounting department personnel.	Adding to or deleting general ledger accounts are limited to authorized accounting department personnel.

Masters

Table 1.7.12: Risks and Control Objectives (Masters-General Ledger)

Risk	Control Objective
General ledger master file change reports are not generated by the system and are not reviewed as necessary by an individual who does not input the changes.	General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does input the changes.
A standard chart of accounts has not been approved by management and is not utilized within all entities of the corporation.	A standard chart of accounts has been approved by management and is suitably utilized within all entities of the corporation.

Transactions

Table 1.7.13: Risks and Control Objectives (Transactions-General Ledger)

Risk	Control Objective
General ledger balances are not reconciled to sub ledger balances and such reconciliation are not reviewed for accuracy and not approved by supervisory personnel.	General ledger balances reconcile to sub ledger balances and such reconciliation are reviewed for accuracy and approved by supervisory personnel.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliation to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliation to confirm accuracy of such accounts.
Account codes and transaction amounts are not accurate and not complete, and exceptions are not reported.	Account codes and transaction amounts are accurate and complete, with exceptions reported.
A report of all journal entries completed as part of the closing process is not reviewed by management to confirm the completeness and appropriateness of all recorded entries.	A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.
Actual-to-actual, actual-to-budget and yield reports are not produced from the general ledger system monthly prior to the final close of the general ledger. Reports are not distributed to and reviewed by the controller and CFO. Unusual amounts or variances are not investigated and reclassified when applicable.	Actual-to-actual, actual-to-budget and yield reports are produced from the general ledger system monthly prior to the final close of the general ledger. Reports are distributed to and reviewed by the controller and CFO. Unusual amounts or variances are investigated and re-classified when applicable.
Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.

1.8 DIAGRAMMATIC REPRESENTATION OF BUSINESS PROCESSES

1.8.1 Introduction to Flowcharts

For controlling the organization effectively, it is very important to have an understanding about its processes which can be done through business process mapping. Business process mapping refers to gathering extensive information about the current processes in an organization. This information should include description of the different activities involved in the process, the process flows, what the processes actually do, who is in charge of the process, the competence needed and how the process should be performed.

A **Flowchart** is a diagram that describes a process or operation. It includes multiple steps, through which the process "flows" from start to finish. Flowcharts are used in designing and documenting simple processes or programs. Like other types of diagrams, they help visualize what is going on and thereby help understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it.

I. Flowcharting Symbols

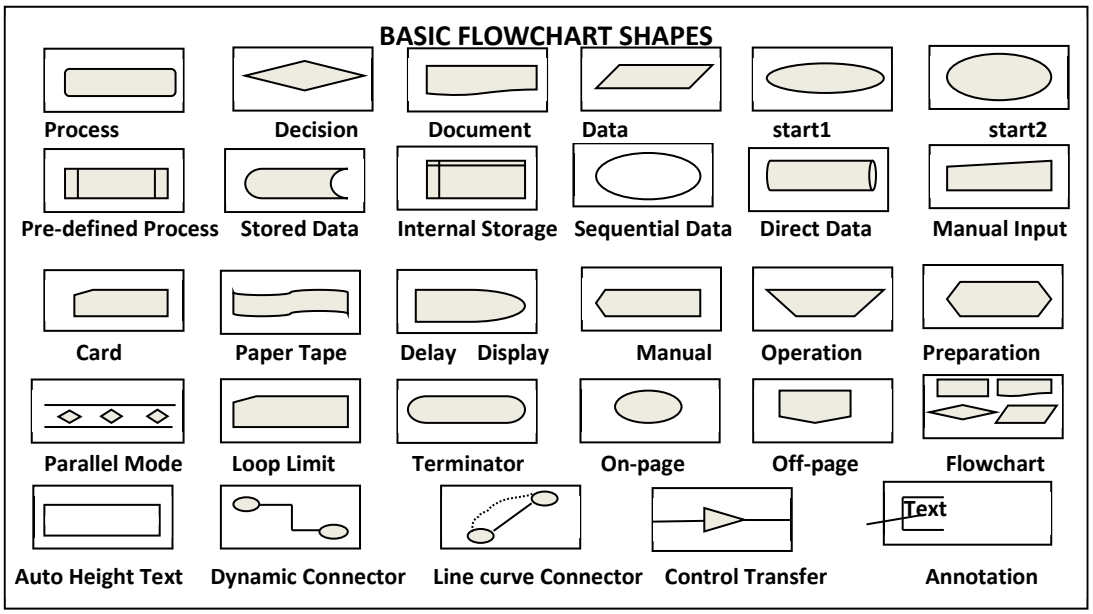


Fig. 1.8.1: Flowcharting Symbols

There are many different types of flowcharts, and each type has its own collection of boxes and notational conventions. The two most common types of boxes in a flowchart are as follows:

- A processing step, usually called **activity** and denoted as a **rectangular box**.
- A **decision** usually denoted as a **diamond**.

A Flowchart is described as "cross-functional" when the page is divided into different swimlanes describing the control of different organizational units. A symbol appearing in a particular "lane" is within the control of that organizational unit. This technique allows the author to locate the responsibility for performing an action or deciding correctly, showing the responsibility of each organizational unit for different parts of a single process.

II. Steps for creating flowcharts for business processes

- Identify the business process that is to be documented with a flowchart and establish the overall goal of the business process.
- Based on inputs from the business process, owner obtains a complete understanding of the process flow.
- Prepare an initial rough diagram and discuss with the business process owner to confirm your understanding of the processes.
- Obtain additional information about the business process from the people involved in each step, such as end users, stakeholders, administrative assistants and department heads. During this phase, you may find that some employees do not follow certain processes, or some processes are redundant. This should be highlighted so that corrective steps can be taken by the management.
- Identify the activities in each process step and who is responsible for each activity.
- Identify the starting point of the process. The starting point of a business process should be what triggers the process to action. In other words, it is the input that the business seeks to convert into an output. Starting points generally fall into one of several categories:

- **External events:** These include the initiation of a transaction or a transmitted alert from another business system. For example, creation of a purchase order in a computer system or a sales order alerting a production system that a product should be manufactured due to lack of available stock.
- **Content arrival:** For content management systems, the starting point might be the arrival of a new document or other form of content.
- **Human intervention:** This includes customer complaints and other human intervention within or outside of the business.

♦ Separate the different steps in the process. Identify each individual step in the process and how it is connected to the other steps. On the most general level, you will have events (steps that require no action by the business), activities (performed by the business in response to input), and decision gateways (splits in the process where the path of the process is decided by some qualifier). Between these objects, there are connectors, which can be either solid arrows (activity flow) or dashed (message/information flow).

♦ **Business Process Modelling Notation (BPMN)** is a flowchart based notation for defining business processes. In traditional BPMN, the steps are represented by different shapes depending on their function. For example, we would use steps such as "customer order" (an event), "process order" (an activity), "Check credit" (an action), "Credit?" (A decision gateway that leads to one of two other actions, depending on a "yes" or "no" determination), and so on.

♦ Clarify who performs each step and what is performed in each step. To make the process as clear as possible, you should determine which part of the business completes each step. For example, different parts of the process may be completed by the accounting department, customer service, or order fulfilment. Alternately, for a small business, these steps may be completed by specific individuals. In BPMN, the associated person or department for each activity is either denoted by a designator next to the step or by a horizontal division or "lanes" in the flowchart that shows which part of the business performs each step, i.e. person or department.

Fig. 1.8.2 is a very simple flowchart which represents a process that happens in our daily life.

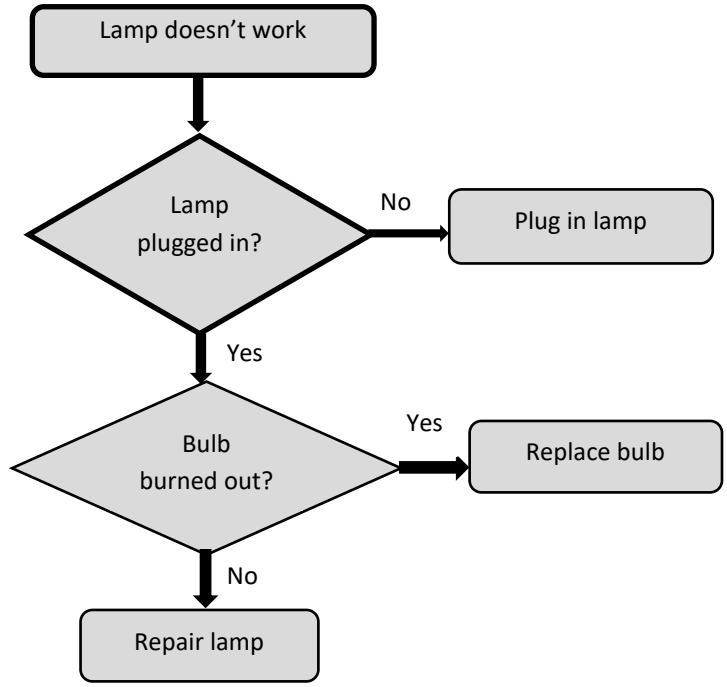


Fig. 1.8.2: Simple Flowchart

III. Advantages of Flowcharts

(i) Quicker grasp of relationships - The relationship between various elements of the application program/business process must be identified. Flowchart can help depict a lengthy procedure more easily than by describing it by means of written notes.

(ii) Effective Analysis - The flowchart becomes a blueprint of a system that can be broken down into detailed parts for study. Problems may be identified and new approaches may be suggested by flowcharts.

(iii) Communication - Flowcharts aid in communicating the facts of a business problem to those whose skills are needed for arriving at the solution.

(iv) Documentation - Flowcharts serve as a good documentation which aid greatly in future program conversions. In the event of staff changes, they serve as training function by helping new employees in understanding the existing programs.

(v) Efficient coding - Flowcharts act as a guide during the system analysis and program preparation phase. Instructions coded in a programming language may be checked against the flowchart to ensure that no steps are omitted.

(vi) Program Debugging - Flowcharts serve as an important tool during program debugging. They help in detecting, locating and removing mistakes.

(vii) Efficient program maintenance - The maintenance of operating programs is facilitated by flowcharts. The charts help the programmer to concentrate attention on that part of the information flow which is to be modified.

(viii) Identifying Responsibilities - Specific business processes can be clearly identified to functional departments thereby establishing responsibility of the process owner.

(ix) Establishing Controls - Business process conflicts and risks can be easily identified for recommending suitable controls.

IV. Limitations of Flowchart

(i) Complex logic – Flowchart becomes complex and clumsy where the problem logic is complex. The essentials of what is done can be easily lost in the technical details of how it is done.

(ii) Modification – If modifications to a flowchart are required, it may require complete re-drawing.

(iii) Reproduction – Reproduction of flowcharts is often a problem because the symbols used in flowcharts cannot be typed.

(iv) Link between conditions and actions – Sometimes it becomes difficult to establish the linkage between various conditions and the actions to be taken there upon for a condition.

(v) Standardization – Program flowcharts, although easy to follow, are neither a natural way of expressing procedures as writing in English, nor are they easily translated into Programming language.

Example 1.9: Draw a Flowchart for finding the sum of first 100 odd numbers.

Solution 1.9: The flowchart is drawn as Fig. 1.8.3 and is explained step by step below. The step numbers are shown in the flowchart in circles and as such are not a part of the flowchart but only a referencing device.

Our purpose is to find the sum of the series 1, 3, 5, 7, 9.....(100 terms). The student can verify that the 100^{th} term would be 199. We propose to set A = 1 and then go on incrementing it by 2 so that it holds the various terms of the series in turn. B is an accumulator in the sense that A is added to B whenever A is incremented. Thus, B will hold:

1

1 + 3 = 4

4 + 5 = 9,

9 + 7 = 16, etc. in turn.

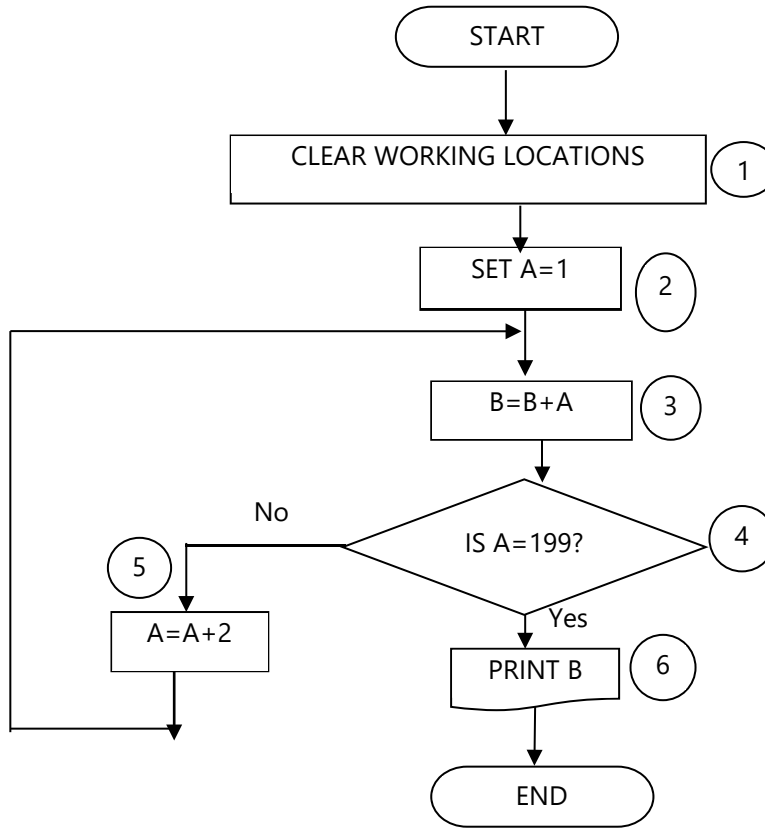


Fig. 1.8.3: Flowchart for addition of first 100 odd numbers

Step 1 - All working locations are set at zero. This is necessary because if they are holding some data of the previous program, that data is liable to corrupt the result of the flowchart.

Step 2 - A is set at 1 so that subsequently by incrementing it successively by 2, we get the wanted odd terms: 1,3,5,7 etc.

Step 3 - A is poured into B i.e., added to B. B being 0 at the moment and A being 1, B becomes 0 + 1 = 1.

Step 4 - Step 4 poses a question. "Has A become 199?" if not, go to step 5, we shall increment A by 2. So, that although at the moment A is 1, it will be made 3 in step 5, and so on. Then go back to Step 3 by forming loop.

Since we must stop at the 100^{th} term which is equal to 199. Thus, A is repeatedly incremented in step 5 and added to B in step 3. In other words, B holds the cumulative sum up to the latest terms held in A.

When A has become 199 that means the necessary computations have been carried out so that in Step 6 the result is printed.

Example 1.10: An E-commerce site has the following cash back offers.

(i) If purchase mode is via website, an initial discount of 10% is given on bill amount.

(ii) If purchase mode is via phone app, an initial discount of 20% is given on bill amount.

(iii) If done via any other purchase mode, the customer is not eligible for any discount.

Every purchase eligible to discount is given 10 reward points.

(a) If the reward points are between 100 and 200 points, the customer is eligible for a further 30% discount on the bill amount after initial discount.

(b) If the reward points exceed 200 points, the customer is eligible for a further 40% discount on the bill amount after initial discount.

Taking purchase mode, bill amount and number of purchases as input; draw a flowchart to calculate and display the total reward points and total bill amount payable by the customer after all the discount calculation.

Solution 1.10: Let us define the variables first:

PM: Purchase Mode **BA:** Bill Amount **TBA:** Total Bill Amount

NOP: Number of Purchases **TRP:** Total Reward Points **IN_DISC:** Initial Discount

ET_DISC: Extra Discount on purchases eligible to Initial Discount

N: Counter (to track the no. of purchases)

Refer Fig. 1.8.4 for the desired flowchart.

Example 1.11: A bank has 500 employees. The salary paid to each employee is sum of his Basic Pay (BP), Dearness Allowance (DA) and House Rent Allowance (HRA). For computing HRA, bank has classified his employees into three classes A, B and C. The HRA for each class is computed at the rate of 30%, 20% and 10% of the BP Pay respectively. The DA is computed at a flat rate of 60% of the Basic Pay. Draw a flow chart to determine percentage of employee falling in the each of following salary slabs:

(i) Above ₹ 30,000

(ii) ₹ 15,001 to ₹ 30,000

(iii) ₹ 8,001 to ₹ 15,000

(iv) Less than or equal to ₹ 8,000

Solution 1.11: Abbreviations used in the flowchart are as follows:

P_1, P_2, P_3 and P_4: Percentage of employees falling in salary slab (salary<=8,000); salary slab (8,001<= salary<=15,000); salary slab (15,001<= salary<=30,000) and salary slab (salary >=30,000) respectively;

C_1, C_2, C_3 and C_4 are the number of employees falling in salary slab (salary<=8,000); salary slab (8,001<= salary<=15,000); salary slab (15,001<= salary<=30,000) and salary slab (salary >=30,000) respectively;

I: Count of number of employees

The required flowchart is given in Fig. 1.8.5.

Solution 1.10 (Ctd.)

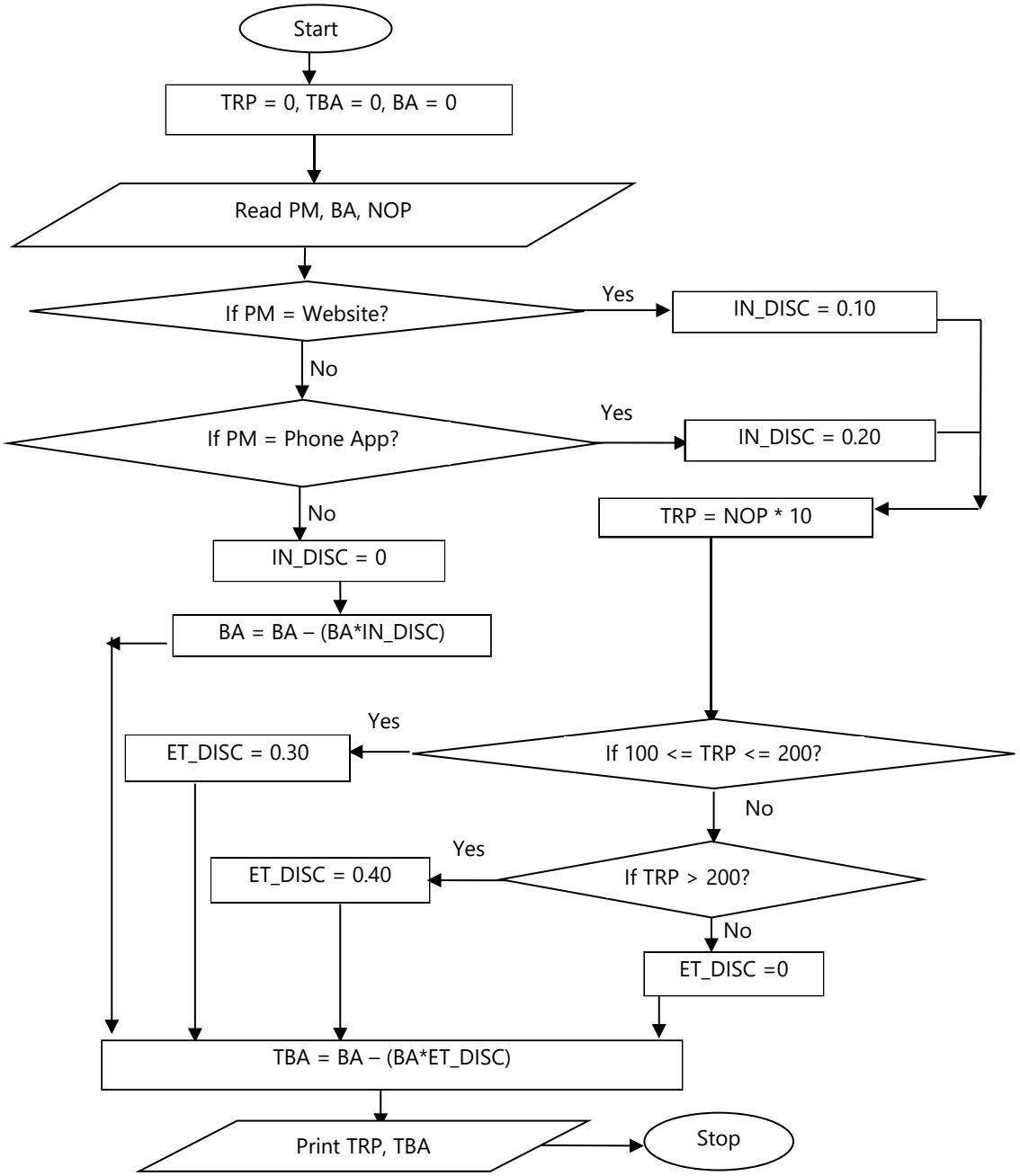


Fig. 1.8.4: Flowchart for Example 1.10

Solution 1.11 (Ctd.)

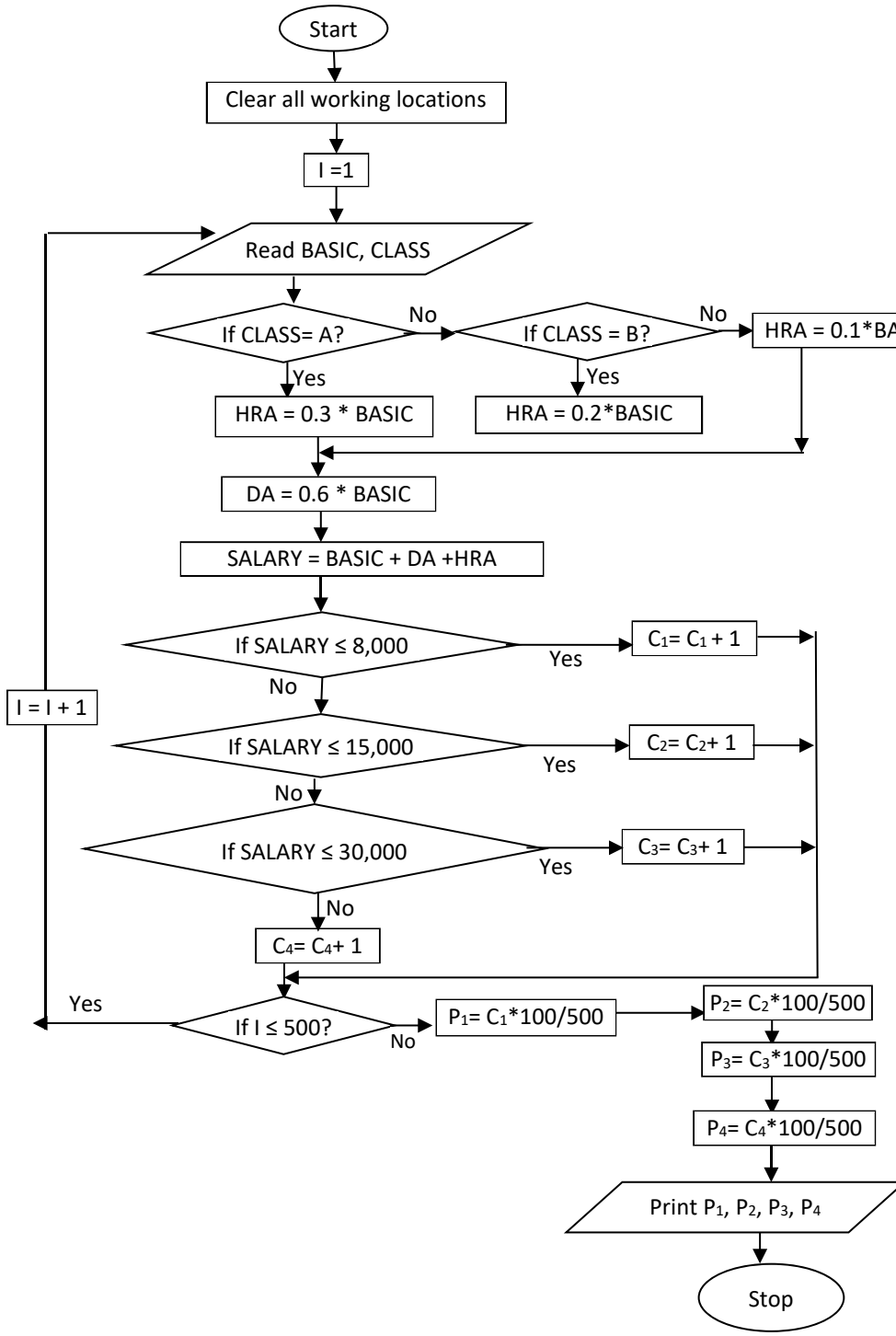


Fig. 1.8.5: Flowchart for Example 1.11

Example 1.12: Consider the following flowchart in the Fig. 1.8.6.

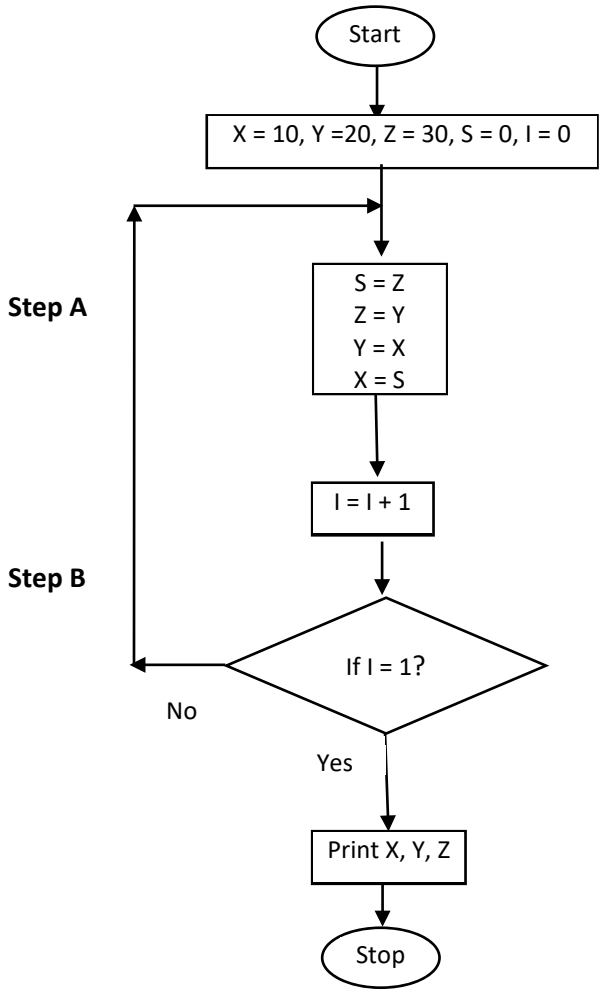


Fig. 1.8.6: Example 1.12

(a) What is the output of the flowchart?

(b) In Step B, put I = 3 in place of I = 1; what will be the output then?

(c) In Step B, put I = 6 in place of I = 1; what will be the output then?

(d) In the given flowchart if I = 0 is replaced by I = 1 at Step A, what will be the output?

Solution 1.12: Refer to the Table 1.8.1.

(a) X = 30, Y = 10, Z = 20

(b) For I = 3; X = 10, Y = 20, Z = 30

(c) For I = 6; X = 10, Y = 20, Z = 30

(d) For I = 1 at Step A; the flowchart will enter into an Infinite Loop as the condition I = 1 will never be true.

Table 1.8.1: Working of Example 1.12

Working of the Flowchart							
Initial Values	**Sequence of Steps**	**Output 1**	**Output 2**	**Output 3**	**Output 4**	**Output 5**	**Output 6**
I = 0							
S = 0	S = Z Z = Y Y = X X = S I = I + 1	S = 30	S = 20	S = 10	S = 30	S = 20	S = 10
Z = 30		Z = 20	Z = 10	Z = 30	Z = 20	Z = 10	Z = 30
Y = 20		Y = 10	Y = 30	Y = 20	Y = 10	Y = 30	Y = 20
X = 10		X = 30	X = 20	X = 10	X = 30	X = 20	X = 10
I = 0		I = 1	I = 2	I = 3	I = 4	I = 5	I = 6
		Ans. (a)		**Ans. (b)**			**Ans. (c)**

Example 1.13: A company is selling three types of products namely A, B and C to two different types of customers viz. dealers and retailers. To promote the sales, the company is offering the following discounts. Draw a flowchart to calculate the discount for the below mentioned policy.

(i) 10% discount is allowed on product A, irrespective of the category of customers and the value of order.

(ii) On product B, 8% discount is allowed to retailers and 12% discount to dealers, irrespective of the value of order.

(iii) On product C, 15% discount is allowed to retailers irrespective of the value of order and 20% discount to dealers if the value of order is minimum of ₹10,000.

Solution 1.13: The required flowchart is given in Fig. 1.8.7:

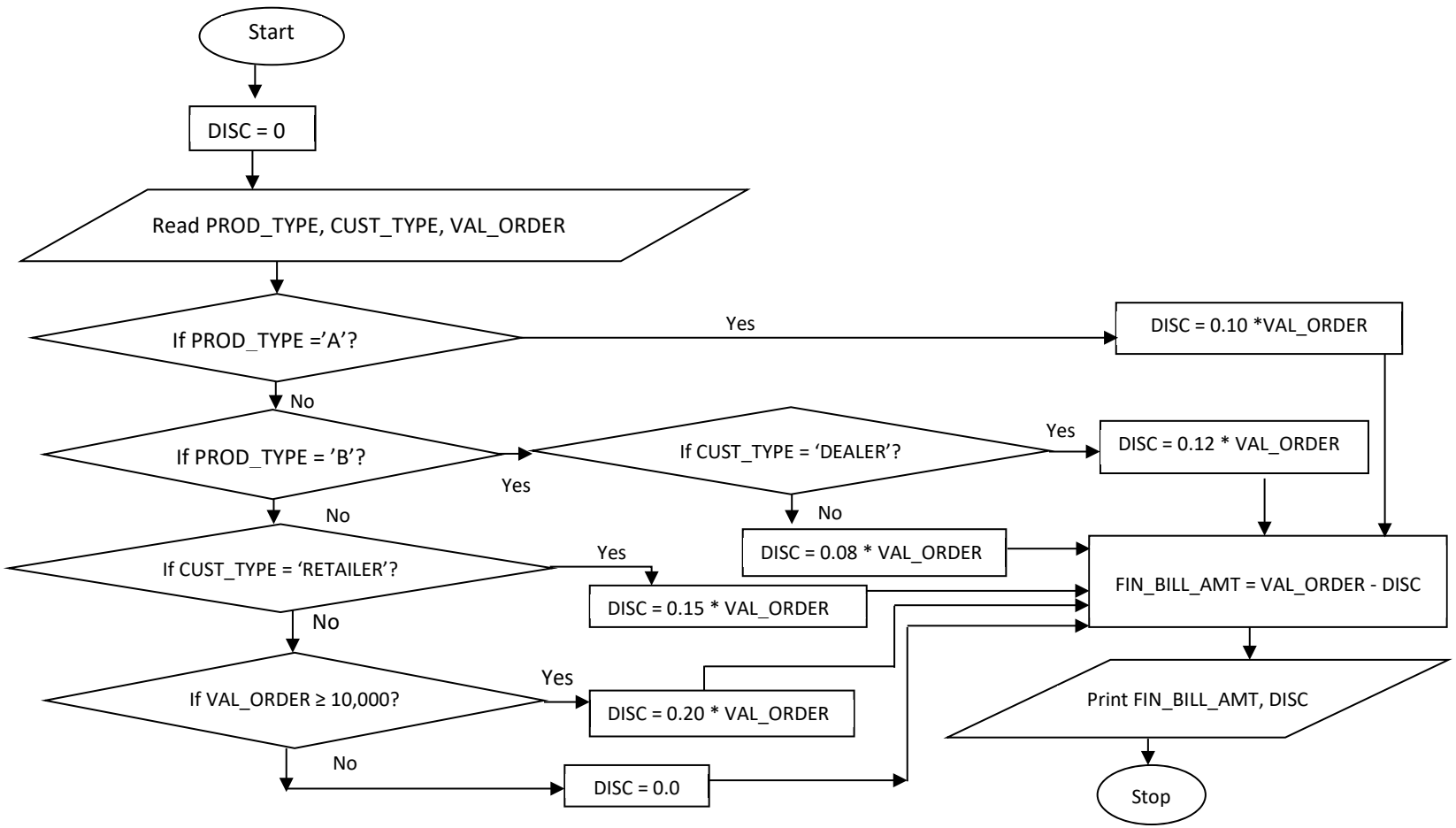


Fig. 1.8.7: Flowchart for Example 1.13

1.8.2 Data Flow Diagrams (DFDs)

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

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

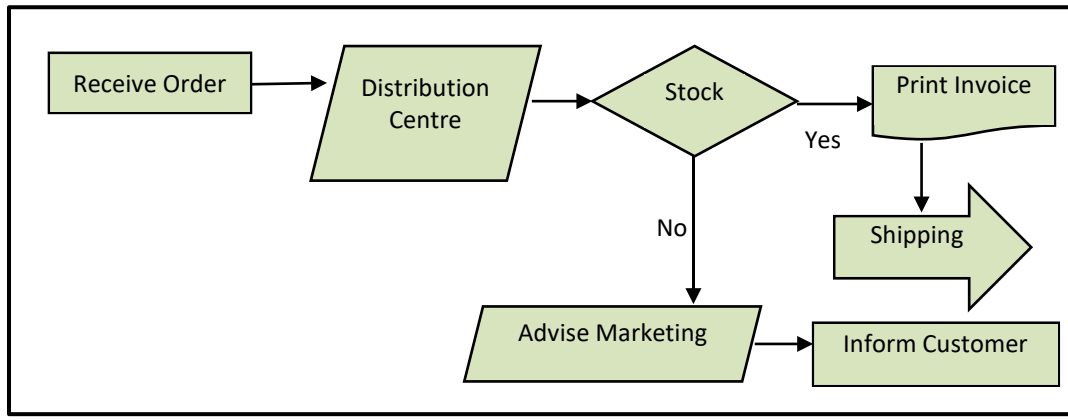


Fig. 1.8.8: Simple Flow chart of Sales (Example: 1.14)

DFD basically provides an overview of:

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

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

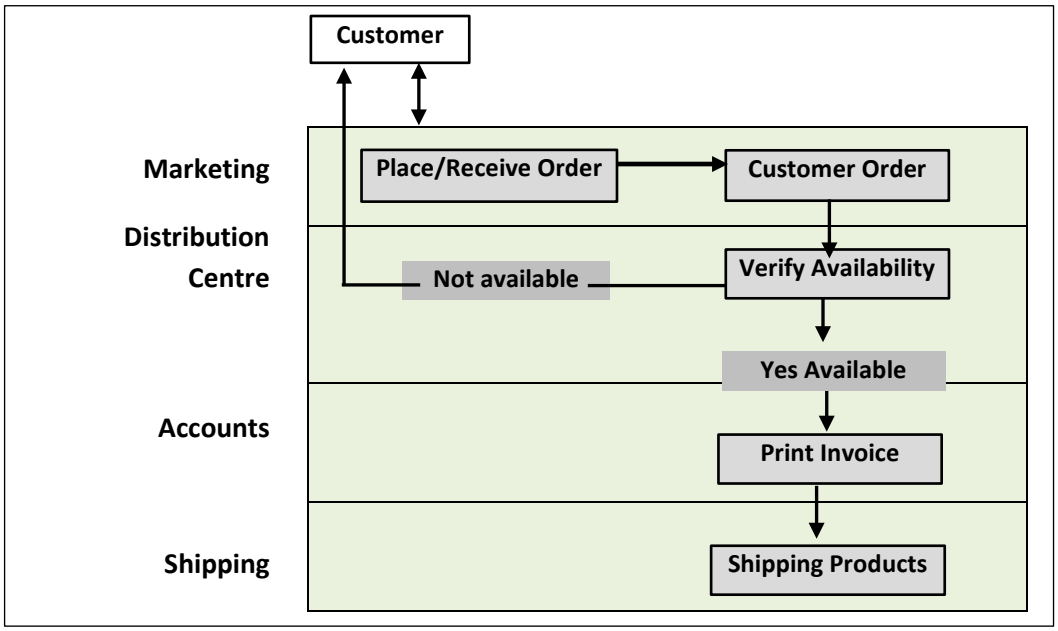
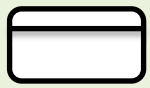


Fig. 1.8.9: Process flow of Sales (Example)

DFD is mainly used by technical staff for graphically communicating between systems analysts and programmers. Main symbols used in DFD are provided in Table 1.8.2.

Table 1.8.2: Main symbols used in DFD

	**Process**	Step-by-step instructions are followed that transform inputs into outputs (a computer or person or both doing the work).
	**Data flow**	Data flowing from place to place, such as an input or output to a process.
	**External Agent**	The source or destination of data outside the system. The people and organizations that send data to or receive data from are represented by this symbol called external agent.
	**Data Store**	Data at rest, being stored for later use. Usually corresponds to a data entity on an entity-relationship diagram.
	**Real-time link**	Communication back and forth between an external agent and a process as the process is executing (e.g. credit card verification).

Example 1.16: Given below in Fig. 1.8.10 is a simple scenario depicting a book borrowed from a library being returned and the fine calculated, due to delay.

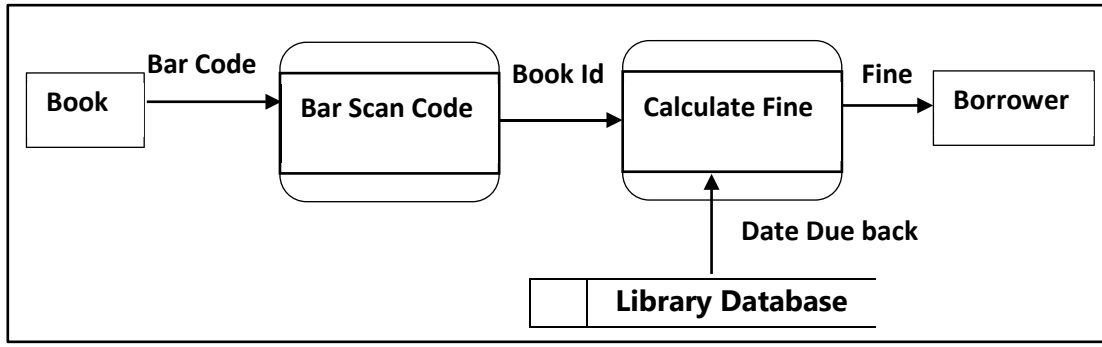


Fig. 1.8.10: Simple DFD (Example1.16)

- The book is represented as an external entity and the input is the bar code.
- The process is the scanning of the bar code and giving an output of the Book ID.
- The next process calculates the fine based on accessing the "library database" and establishing the "due back" date.
- Finally, the fine is communicated to the borrower who is also shown as an external entity.

1.8.3 Diagrammatic Representation of Specific Business Processes

Example 1.17: Customer Order Fulfilment (Refer Fig. 1.8.11)

- The process starts with the customer placing an order and the sales department creating a sales order.
- The sales order goes through the Credit & Invoicing process to check credit (an activity) is it OK? (a decision gateway).
- If the customer's credit check is not OK, you would move to the step "credit problem addressed" (an activity), followed by a decision "OK?". If, "No" the order will be stopped.
- If the customer's "credit check" response is "yes", and if stock is available, an invoice is prepared, goods shipped and an invoice is sent to the customer. If the stock is not available, the order is passed to "production control" for manufacture and then shipped to customer with the invoice.
- The process ends with the payment being received from customer.

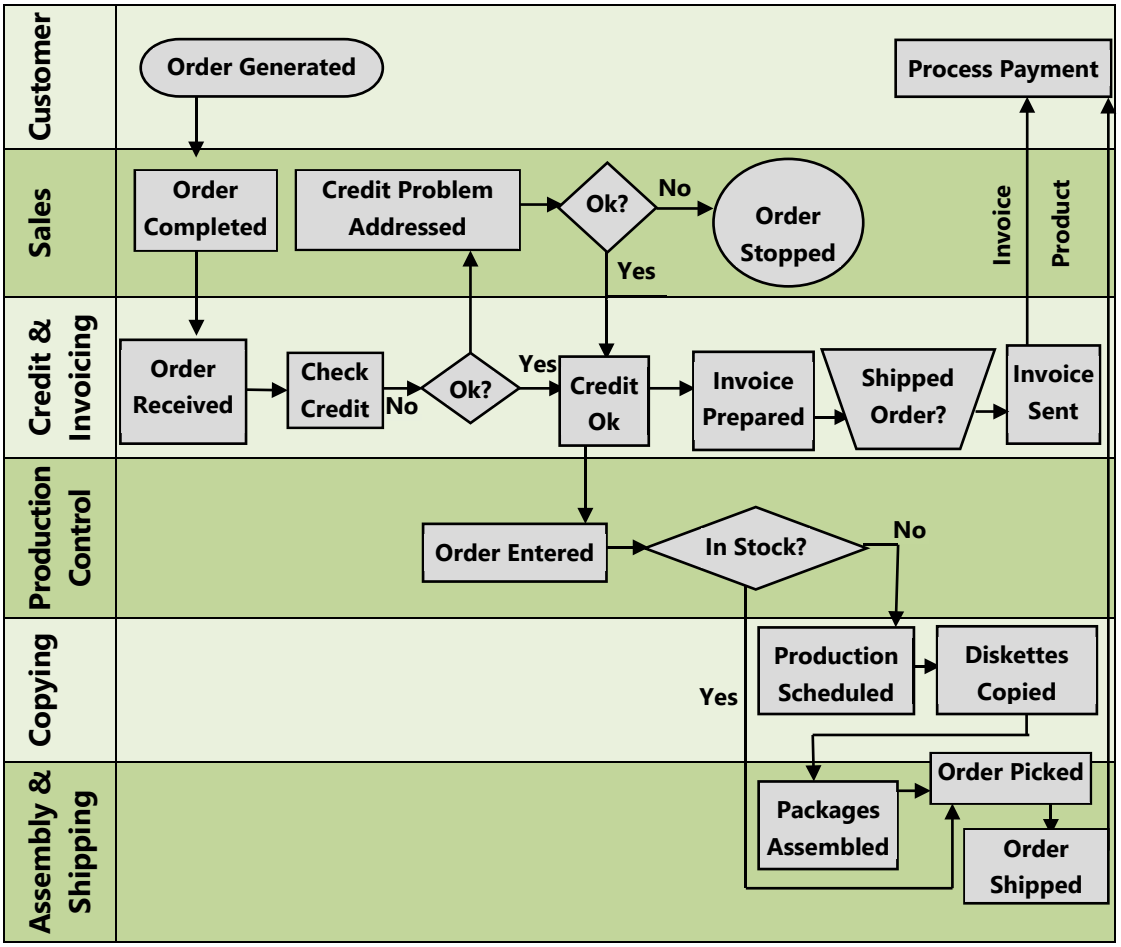


Fig. 1.8.11: Customer Order Fulfilment (Example 1.17)

Example 1.18: Order to Cash (Refer Fig. 1.8.12)

Fig. 1.8.12 indicates the different sub processes within the main processes in the Order to Cash cycle. It should be noted that this is only a simple example to illustrate the concept. However, in large enterprises the main processes, sub processes and activities could be much more.

(i) Sales and Marketing (SM)

- Advertises and markets the company's products and books sales orders from customers.

(ii) Order Fulfillment

- Receives orders from SM.

- Checks inventory to establish availability of the product. If the product is available in stock, transportation is arranged, and the product is sent to the customer.

(iii) Manufacturing

- If the product is not available in stock, this information is sent to the manufacturing department so that the product is manufactured and subsequently sent to the customer.

(iv) Receivables

- The invoice is created, sent to the customer, payment received and the invoice closed.
- It should be noted that under each sub process, there could be many activities. For example:
  - **Main Process –** Order Fulfilment
  - **Sub Process –** Receive Orders
  - **Other Activities –** Check correctness and validity of information in order, enter order in computer system, check credit worthiness of customer, check credit limit, obtain approval for any discrepancy etc.

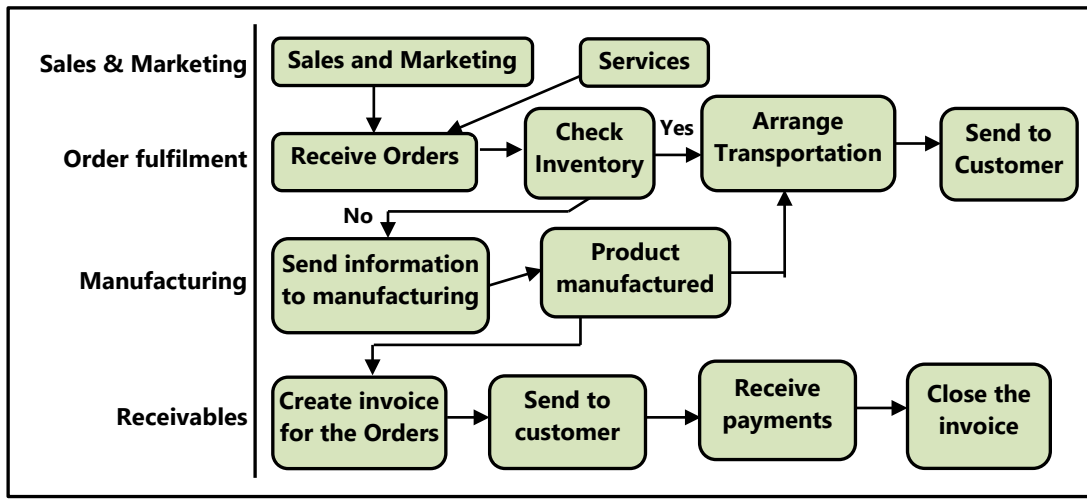


Fig. 1.8.12: Order to Cash (Example 1.18)

Example 1.19: Procure to Pay (Refer Fig. 1.8.13)

The **Purchase to Pay/Procure to Pay** process in Fig. 1.8.13 indicates the different processes identified specifically to department/entity through "swimlanes" so that

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

(i) User Department

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

(ii) Procurement Department (PD)

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

(iii) Vendor

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

(iv) Stores

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

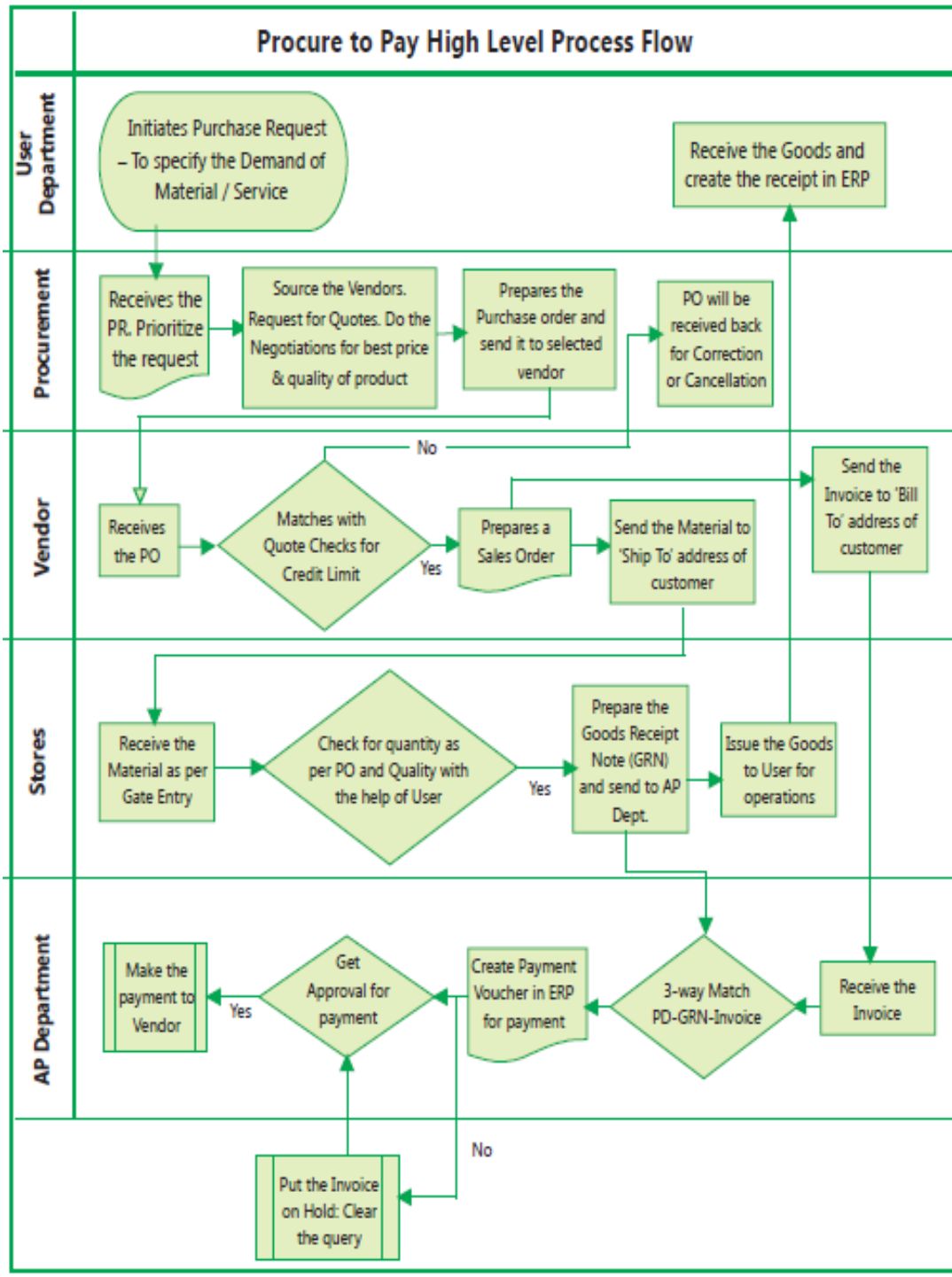


Fig. 1.8.13: Procure to Pay (Example 1.19)

(v) Accounts Payable (AP)

AP will do a "Three-way match" of PO/GRN/VI. This is to ensure that the price, quantity and terms indicated in the VI matches with the PO and the quantity received in the PO matches with the GRN quantity. This check establishes that what has been ordered has been delivered.

- If there is no discrepancy, the payment voucher is prepared for payment and the necessary approvals obtained.
- If there is a discrepancy, the VI is put "on hold" for further clarification and subsequently processed.
- Finally, the payment is made to the vendor.

1.9 REGULATORY AND COMPLIANCE REQUIREMENTS

Major corporations worldwide have used Information Technology (IT) to stay ahead in business. The competitive edge in terms of fast information flow, to support the business, can be an important factor between success and failure.

The efficiency of an enterprise depends on the quick flow of information across the complete supply chain i.e. from the customer to manufacturers to the suppliers. With the globalization of the marketplace coupled with competition and increasing customer expectations, enterprises should address certain fundamental areas like lowering costs in the supply chain, reducing throughput times, optimizing stock levels, improving product quality and service to the customers, efficiently handling cross border data flow etc. Today's IT systems achieve all this.

The core to any enterprise's success is to have an efficient and effective financial information system to support decision-making and monitoring. The risks, controls and security of such systems should be clearly understood to pass an objective opinion about the adequacy of control in an IT environment.

1.9.1 The Companies Act, 2013

The Companies Act, 2013 has two very important Sections - **Section 134** and **Section 143**, which have a direct impact on the audit and accounting profession.

(i) Section 134

Section 134 of the Companies Act, 2013 on "Financial statement, Board's report, etc." states inter alia:

The **Directors' Responsibility Statement** referred in clauses (c,e) of sub-section (3) shall state that:

(c) the Directors had taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of this Act for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities;

(e) the Directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

Explanation: For the purposes of this clause, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

(ii) Section 143

Section 143, of the Companies Act 2013, on "Powers and duties of auditors and auditing standards" states inter alia:

Section 143(3)(i) contains the **Auditor's Report** which shall state that:

"Whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls";

When we talk in terms of "adequacy and effectiveness of controls"; it refers to the adequacy of the control design and whether the control has been working effectively during the relevant financial year.

Example 1.20: Let us assume that a company has a sales invoicing control wherein all sales invoices raised by the salesman which is greater than ₹ 50,000/- are reviewed and approved by the sales manager. In terms of the control, design this control may seem adequate. However, if during audit, it was found that during the year, there were many invoices raised by the salesman which was greater than ₹ 50,000/- and not reviewed and approved by the sales manager. In such a case, although the control design was adequate, the control was not working effectively, due to many exceptions without proper approval.

I. Management's Responsibility

1. The Companies Act, 2013 has significantly expanded the scope of internal controls to be considered by the management of companies to cover all aspects of the operations of the company.

   Clause (e) of Sub-section 5 of Section 134 to the Act requires the Directors' responsibility statement to state that the directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

   Clause (e) of Sub-section 5 of Section 134 explains the meaning of the term, "internal financial controls" as "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information."

2. Rule 8(5)(viii) of the Companies (Accounts) Rules, 2014 requires the Board of Directors' report of all companies to state the details in respect of adequacy of internal financial controls with reference to the financial statements.

The inclusion of the matters relating to internal financial controls in the directors' responsibility statement is in addition to the requirement for the directors to state that they have taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of the 2013 Act, for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities.

II. Auditors' Responsibility

As per ICAI's "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting":

Clause (i) of Sub-section 3 of Section 143 of the Companies Act, 2013 ("The 2013 Act" or "The Act") requires the Auditors' report to state whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls.

The auditor's objective in an audit of internal financial controls over financial reporting is to express an opinion on the effectiveness of the company's internal financial controls over financial reporting and the procedures in respect thereof

are carried out along with an audit of the financial statements. Because a company's internal controls cannot be considered effective if one or more material weakness exists, to form a basis for expressing an opinion, the auditor should plan and perform the audit to obtain sufficient appropriate evidence to obtain reasonable assurance about whether material weakness exists as of the date specified in management's assessment. A material weakness in internal financial controls may exist even when the financial statements are not materially misstated.

III. Corporate Governance Requirements

Corporate Governance is the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with its all stakeholders (financiers, customers, management, employees, government, and the community). The directors of a company are responsible to the shareholders for their actions in directing and controlling the business of the company. Good corporate governance requires establishment of sound internal control practices, risk management, and compliance with relevant laws and standards such as corporate disclosure requirements. Good management practices are one of the important elements of corporate governance. The major elements of corporate governance include management's commitment, good management practices, functional and effective control environment, transparent disclosure and well-defined shareholder rights.

The Corporate Governance framework consists of:

(i) explicit and implicit contracts between the company and the stakeholders for distribution of responsibilities, rights, and rewards.

(ii) procedures for reconciling the sometimes-conflicting interests of stakeholders in accordance with their duties, privileges, and roles, and

(iii) procedures for proper supervision, control, and information-flows to serve as a system of checks-and-balances.

1.9.2 Information Technology Act, 2000 (IT Act)

Cyber Crime: The term 'Cyber Crime' finds no mention either in The Information Technology Act, 2000 or in any legislation of the Country. Cyber Crime is not different than the traditional crime. The only difference is that in Cyber Crime the computer technology is involved and thus it is a computer related crime. This can be explained by the following instance:

- **Traditional Theft:** Thief 'A' enters into B's house and steals an object kept in the house.
- **Hacking:** Many business organizations store their confidential information in computer system which is often targeted by rivals, criminals and disgruntled employees. Hacking generally refers to unauthorized intrusion into a computer or a network. This may be done by either altering system or security features to accomplish a goal that differs from the original purpose of the system. For example - Mr. A, a cyber-criminal while sitting in his own house, through his computer hacks the computer of Mr. B and steals the data saved in Mr. B's computer without physically touching the computer or entering in B's house.

The IT Act, 2000 aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what the various perspectives of the IT Act 2000 (as amended in 2008) are and what it offers.

The Act also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract maybe expressed by electronic means of communication and the same shall have legal validity and enforceability.

A. Computer Related Offences

Let us look at some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in Information Technology Act, 2000 (amended via 2008).

- **Harassment via fake public profile on social networking site:** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim. Section 67 of the IT Act, 2000 is applicable here.
- **Email Account Hacking:** If victim's email account is hacked and obscene emails are sent to people in victim's address book. Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act, 2000 are applicable in this case.
- **Credit Card Fraud:** Unsuspecting victims would use infected computers to make online transactions. Sections 43, 66, 66C, 66D of IT Act, 2000 are applicable in this case.

- **Web Defacement:** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days. Sections 43 and 66 of IT Act and Sections 66F and 67 of IT Act, 2000 also apply in some cases.
- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, and Bugs:** All these are some sort of malicious programs which are used to destroy or gain access to some electronic information. Sections 43 and 66 of IT Act, 2000 are applicable in this case.
- **Cyber Terrorism:** Cyber terrorism is the terrorism conducted in cyberspace, where the criminals attempt to damage or disrupt computer systems or telecommunication services. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via electronic communication. Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business. Sections 43, 66, 66A of IT Act, 2000 are applicable in this case.
- **Online sale of illegal Articles:** Where sale of narcotics, drugs, weapons and wildlife is facilitated by the Internet.
- **Cyber Pornography:** Among the largest businesses on Internet, pornography may not be illegal in many countries, but child pornography is. Sections 67, 67A and 67B of the IT Act, 2000 are applicable in this case.
- **Phishing and Email Scams:** Phishing involves fraudulently acquiring sensitive information through masquerading oneself as a trusted entity (e.g. usernames, Passwords, credit card information). Sections 66, 66C and 66D of IT Act, 2000 are applicable in this case.
- **Theft of Confidential Information:** Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees. Sections 43, 66 and 66B of IT Act, 2000 are applicable in this case.
- **Source Code Theft:** A Source code generally is the most coveted and important "crown jewel" asset of a company. Sections 43, 65, 66 and 66B of IT Act, 2000 are applicable in this case.

B. Key Provisions of IT Act

I. Some Definitions in IT Act

The IT Act, 2000 defines the terms **Access** 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 programmes, software and databases or microfilm or computer generated microfiche;

In a cyber-crime, computer or the data are the target or the object of offence or a tool in committing some other offence. The definition of term computer elaborates that computer is not only the computer or laptop on our tables, as

per the definition computer means any electronic, magnetic, optical or other high speed data processing devise of system which performs logical, arithmetic and memory function 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. Thus, the definition is much wider to include mobile phones, automatic washing machines, micro-wave ovens etc.

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 incharge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network 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 thereunder;

(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.

Explanation - For the purposes of this section -

(i) **"computer contaminant"** means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) **"computer database"** means a representation of information, know-ledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) **"computer virus"** means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) **"damage"** means to destroy, alter, delete, add, modify or rearrange any computer resource by any means;

(v) **"computer source code"** means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

[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.

Explanation - For the purposes of this section -

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[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 two lakh rupees, or with both. The explanation clarifies that 'Computer Source Code'' means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

[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 66B] 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 66C] 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 66D] Punishment for cheating by personation by using computer resource

Whoever, by means for any communication device or computer resource cheats by personating, 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 66E] 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.

[Section 66F] Punishment for cyber terrorism

(1) Whoever -

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or

services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

[Section 67] Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever, -

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online; or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

PROVIDED that provisions of Section 67, Section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form -

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation - For the purposes of this section, "children" means a person who has not completed the age of 18 years.

II Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber-crimes. We need such laws so that people can perform purchase

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

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

III. Privacy of Online Data

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

different. Therefore, in a globalized world it becomes very challenging for these companies to ensure uniform standards of privacy.

The main principles on data protection and privacy enumerated under the IT Act, 2000 are as follows:

- defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.
- creating civil liability if any person accesses or secures access to computer, computer system or computer network.
- creating criminal liability if any person accesses or secures access to computer, computer system or computer network.
- declaring any computer, computer system or computer network as a protected system.
- imposing penalty for breach of confidentiality and privacy.
- setting up of hierarchy of regulatory authorities, namely adjudicating officers, the Cyber Regulations Appellate Tribunal etc.

Example 1.21: A sample **privacy policy** is given below which highlights key aspects of how and what type of information is collected from the customer, how it is used and secured and options for user providing the information:

"At ABC Ltd., we take your privacy very seriously. Because of this, we want to provide you with explicit information on how we collect, gather and identify information during your visit to our site. This information may be expanded or updated as we change or develop our site. For this reason, we recommend that you review this policy from time-to-time to see if anything has changed. Your continued use of our site signifies your acceptance of our privacy policy."

Personally, identifiable information refers to information that tells us specifically who you are, such as your name, phone number, email or postal address. In many cases, we need this information to provide the personalized or enhanced service that you have requested. The amount of personally identifiable information that you choose to disclose to ABC Ltd. is completely up to you. The only way we know something about you personally is if you provide it to us in conjunction with one of our services.

What information do we collect and how do we use it?

- ABC Ltd. collects information on our users by your voluntary submissions (e.g., when you sign up for a white paper or request product information).

We also collect, store and accumulate certain non-personally identifiable information concerning your use of this web site, such as which of our pages are most visited.

- The information ABC Ltd. collects is used in a variety of ways: for internal review; to improve the content of the site, thus making your user experience more valuable; and to let you know about products and services of interest.

Email

- If you have provided us your email address, ABC Ltd. periodically sends promotional emails about products offered by us. If you do not wish to receive email information from ABC Ltd., please let us know by emailing us.
- ABC Ltd. does not sell, rent, or give away your personal information to third parties. By using our web site, you provide consent to the collection and use of the information described in this by Privacy Policy of ABC Ltd.

IV. Sensitive Personal Data Information (SPDI)

Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under Section 43A of the Information Technology Act 2000 define a data protection framework for the processing of digital data by Body Corporate.

Scope of Rules: Currently the Rules apply to Body Corporate and digital data. As per the IT Act, Body Corporate is defined as "Any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."

The present scope of the Rules excludes from its purview several actors, that do or could have access to Big Data or use Big Data practices. The Rules would not apply to government bodies or individuals collecting and using Big Data. Yet, with technologies such as IoT (Internet of Things) and the rise of Smart Cities across India – a range of government, public, and private organizations and actors could have access to Big Data.

Definition of Personal and Sensitive Personal data: Rule 2(i) of 2011 Rules defines "Personal information as information that relates to a natural person which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."

Rule 3 of 2011 Rules defines "Sensitive personal data" as passwords; Financial information; Physical/physiological/mental health condition; Sexual orientation; Medical records and history and Biometric information.

The present definition of personal data hinges on the factor of identification (data that is capable of identifying a person). Yet this definition does not encompass information that is associated to an already identified individual - such as habits, location, or activity.

The definition of personal data also addresses only the identification of 'such person' and does not address data that is related to a particular person but that also reveals identifying information about another person - either directly - or when combined with other data points. By listing specific categories of sensitive personal information, the Rules do not account for additional types of sensitive personal information that might be generated or correlated using Big Data analytics.

Importantly, the definitions of sensitive personal information or personal information do not address how personal or sensitive personal information - when anonymized or aggregated – should be treated.

Consent to collect: Rule 5(1) of Rule 2011 requires that Body Corporate should, prior to collection, obtain consent in writing through letter or fax or email from the provider of sensitive personal data regarding the use of that data.

In a context where services are delivered with little or no human interaction, data is collected through sensors, data is collected on a real time and regular basis, and data is used and re-used for multiple and differing purposes - it is not practical, and often not possible, for consent to be obtained through writing, letter, fax, or email for each instance of data collection and for each use.

Consent to Disclosure: Rule 6 of the 2011 Rules provides that disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

ILLUSTRATION 1.1

ABC Ltd. is engaged in the business of producing consumer durable products. It is facing the problem of poor customer service due to its broken, inefficient, and

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

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

Answer the following Questions:

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

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

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

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

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

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

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

(b) There may not be one but multiple vendors providing different services.

(c) The system environment provides access to customers anytime, anywhere using internet.

(d) The dependence on technology is insignificant.

3. The management of ABC Ltd. adopted a holistic and comprehensive approach of Enterprise Risk Management (ERM) framework by implementing controls across the company. Identify the false statement w.r.t. components of ERM framework.

(a) As a part of event identification, potential events that might have an impact on the entity should be identified.

(b) As a part of risk assessment component, identified risks are analyzed to form a basis for determining how they should be managed.

(c) As a part of monitoring, the entire ERM process should be monitored with no further modifications in the system.

(d) As a part of control activities, policies and procedures are established and executed to help ensure that the risk responses that management selected are effectively carried out.

4. The management of ABC Ltd. implemented different Information Technology General Controls (ITGCs) across different layers of IT environment with an objective to minimize the impact of risks associated with automated processes. Which of the following is not an example of ITGC?

(a) Information Security Policy

(b) Processing Controls

(c) Backup, Recovery and Business Continuity

(d) Separation of key IT functions

SOLUTION

Question No.	Answer	Question No.	Answer
1.	(c) The documentation of all the automated	**2.**	(c) The system environment

		business processes is not done properly.			provides access to customers anytime, anywhere using internet.
3.	(c)	As a part of monitoring, the entire ERM process should be monitored with no further modifications in the system.	**4.**	(b)	Processing Controls

ILLUSTRATION 1.2

DXN Ltd. is engaged in manufacturing consumer products for women. The company released a new product recently which met with unexpected success. The company was established as a market leader in that product. The growing volume of sales transactions started to put a strain on company's internal processes. The company employed 300 more employees to ensure that the customers are served better and faster. But with the increase in number of monthly transactions to 1.5 million, the manual processes which were being followed by the company at present, were holding it back. The company was not able to meet consumer demands even after employing addition 300 employees. The management consultant Mr. X of DXN Ltd. advised to automate the key business processes of the company to handle large volume of transactions to meet the expectations of its customers and maintain its competitive edge in the market.

Mr. X gathered extensive information about the different activities involved in the current processes followed by DXN Ltd. like what the processes do, the flow of various processes, the persons who are in-charge of different processes etc. The information so collected helped him in understanding the existing processes such as flaws, bottlenecks, and other less obvious features within the existing processes. Based on the information gathered about the current processes, Mr. X prepared various flowcharts depicting how various processes should be performed after automation and submitted his report to the management covering the following points:

- The major benefits of Business Process Automation.
- The processes that are best suited to automation.
- Challenges that DXN Ltd. may face while implementing automated processes.

- Risks involved in Business Process Automation and how the management should manage these risks.

Answer the following Questions

1. As the DXN Ltd. was implementing the automated processes for the first time, the consultant suggested not to automate all the processes at a time and automate only critical processes which would help the company to handle large volume of transactions. Which of the following business processes are not best suited to automation?

   (a) Processes involving repetitive tasks

   (b) Processes requiring employees to use personal judgment

   (c) Time sensitive processes

   (d) Processes having significant impact on other processes and systems

2. While understanding the criticality of various business processes of DXN Ltd., the consultant Mr. X documented the current processes and identified the processes that needed automation. However, documentation of existing processes does not help in _____.

   (a) providing clarity on the process

   (b) determining the sources of inefficiency, bottlenecks, and problems

   (c) controlling resistance of employees to the acceptance of automated processes

   (d) designing the process to focus on the desired result with workflow automation

3. When DXN Ltd. decided to adopt automation to support its critical business processes, it exposed itself to number of risks. One risk that the automated process could lead to breakdown in internal processes, people and systems is a type of _____.

   (a) Operational Risk

   (b) Financial Risk

   (c) Strategic Risk

   (d) Compliance Risk

4. Mr. X of DXN Ltd. prepared various flowcharts depicting how various processes should be performed after automation and submitted his report

to the management. The flowcharting symbol that he used to depict processing step is _____.

(a) Rectangular Box

(b) Diamond

(c) Oval

(d) Line

Solution

Question No.	Answer	Question No.	Answer
1.	(b) Processes requiring employees to use personal judgment	**2.**	(c) controlling resistance of employees to the acceptance of automated processes
3.	(a) Operational Risk	**4.**	(a) Rectangular Box

SUMMARY

Technology is the enabler of business process automation (BPA), and it can automate business processes to the point where human intervention is unnecessary. Automation can save time and money, delight customers who no longer must wait in line for a person to assist them with a transaction and avoid human errors.

But not every business process is a good fit for automation, so it's incumbent upon companies to determine which processes are best suited to automation and which ones are best handled manually. How do companies select which business processes to automate? Companies start by looking at the strategic and operating drivers for process improvement in their organizations and industries. For instance, in today's global market, nearly every company is feeling pressure to get goods to market quickly and to be first to market whenever possible. In a highly price-competitive environment, companies are also under great pressure to economize their operations to improve their profitability. Consequently, companies look to automate business processes that are time and resource intensive operationally, that are subject to human error, and that can be accelerated with automated process improvements achievable through computers and technology. If automating business processes speeds product to market,

improves revenue, reduces operating expenses so margins can improve and brings efficiency and effectiveness in the enterprise, the case for automation is substantiated.

Enhanced automated controls within accounting and transaction recording applications can control risk much before they can actually materialize. In addition, companies are under added pressure as regulators, rating agencies and stock exchanges drive improved standards of risk management at an enterprise level, with special emphasis on good corporate governance. Enterprises are therefore in the process of adopting a variety of automated controls to help them combat risk and advance to a proactive approach that reduces the incidence of errors or focuses on them well before the point of impact.

By definition, an automated control is a mechanism or device inside an application, interface or appliance that enforces or controls a rule-set or validation on one or more conditions inside a process. A very simple example of an automated control in accounting parlance is a "drop-down list" of vendors to ensure that the user selects one of the multiple choices provided therein. This would ensure that the transaction is conducted with the authorized set of vendors, which have been set elsewhere by another team that is responsible for vendor on-boarding. Similarly, there are several applications of automated controls in accounting with the prime objective of:

- Mitigating/Eliminating Frauds through enforced segregation of duties and ensuring adherence to a set of delegation of financial powers.
- Business Process Improvement through elimination of manual controls thereby enhancing efficiency and reducing costs.
- Reduced Audit Costs by shifting from "transaction" audit to "controls" audit.
- Adherence to Regulatory Compliance requirements such as Companies Act 2013, IT Act, and the likes, entailing testing of key controls through sampling techniques, which again can be reduced substantially by monitoring the effectiveness of automated controls.

IT is primary driver for enterprises to survive and thrive in this digital age. Regulators have recognized critical importance of IT and hence facilitate digital economy by providing legislative framework and mandating compliances as required. The IT Act, 2000 and Companies have been updated to meet the needs of digital economy. Protection of privacy and personal information is also mandated. Cyber-crime is a reality of digital world when operates without geographical boundaries. Various types of computer related defines have been

defined and penalties specified for these offences. Digitization of business processes should for modern enterprises and this leads to new risks which should be mitigated by implementing appropriate controls.

TEST YOUR KNOWLEDGE

Theoretical Questions

1. In an enterprise, explain various categories of business processes - Operational Processes, Supporting Processes and Management Processes with examples. **(Refer Section 1.2.1)**

2. BPA is the tactic used by a business to operate efficiently and effectively. Explain the parameters that should be met to conclude that success of any business process automation has been achieved. **(Refer Section 1.3.1)**

3. Through automation, a business organization intends to increase the accuracy of its information transferred and certifies the repeatability of the value-added task. Being a management consultant, identify major benefits that an organization would reap out of BPA. **(Refer Table 1.3.1)**

4. Every business process is not a good fit for automation. Explain four examples of business processes that are best suited for automation.

   (Refer Section 1.3.3)

5. Automated processes are susceptible to challenges. Explain the major challenges involved in business process automation. **(Refer Section 1.3.4)**

6. The increased availability of choice to customers about products / services makes it very important for businesses to keep themselves updated with new technology and delivery mechanisms. Being a consultant, briefly explain the steps involved in BPA implementation. **(Refer Section 1.3.5)**

7. As an entrepreneur, your business may face all kinds of risks related from serious loss of profits to even bankruptcy. What could be the possible Business Risks? **(Refer Section 1.4.3 [A])**

8. Automated processes are technology driven. The dependence on technology in BPA for most of the key business processes has led to various challenges. Explain the technology related risks involved in BPA.

   (Refer Section 1.4.3 [B])

9. Effective risk management begins with a clear understanding of an enterprise's risk appetite and identifying high-level risk exposures. Explain the different risk management strategies which the Board or senior management may take up. **(Refer Section 1.4.4)**

10. ERM provides a framework for risk management, which typically involves identifying events or circumstances relevant to the organization's objectives. Discuss the main components of Enterprise Risk Management Framework.

(Refer Section 1.5.2)

11. SA315 provides the definition of Internal Control that are required to facilitate the effectiveness and efficiency of business operations in an organization. Explain all components of Internal Control as per SA315.

(Refer Section 1.6.4)

12. Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Explain the inherent limitations of internal control systems. **(Refer Section 1.6.5)**

13. As a part of his project work submission, Mr. X, a student of ABC university needs to prepare and present a PowerPoint presentation on the topic "Advantages and limitations of Flowcharts" during his practical examination. What shall be the relevant content? **(Refer Section 1.8.1 III,IV)**

14. Give two examples each of the Risks and Control Objectives for the following business processes:

    a. Procure to Pay at Master Level **(Refer Section 1.7.2)**

    b. Order to Cash at Transaction Level **(Refer Section 1.7.3)**

    c. Inventory Cycle at Master Level **(Refer Section 1.7.4)**

15. Explain the salient features of Section 134 & Section 143 of the Companies Act 2013. **(Refer Section 1.9.1 I,II)**

16. Give five examples of computer related offences that can be prosecuted under the IT Act 2000 (amended via 2008). **(Refer Section 1.9.2[A])**

17. Corporate Governance is defined as the framework of rules and practices by which Board of Directors ensures accountability, fairness and transparency

in a company's relationship with all its stakeholders. List the rules and procedures that constitute corporate governance framework.

(Refer Section 1.9.1[III Corporate Governance])

18. Explain the following terms in brief:

    (a) Data Flow Diagram **(Refer Section 1.8.2)**

    (b) Flowchart **(Refer Section 1.8.1)**

    (c) Risk Assessment **(Refer Section 1.5.2[iv])**

19. "Enterprise Risk Management (ERM) does not create a risk-free environment; rather it enables management to operate more effectively in environment filled with risks". In view of this statement, explain the various benefits, which Board of Directors and Management of an entity seek to achieve by implementing the ERM process within the entity.

(Refer Section 1.5.1)

20. State the required characteristics of goals to be achieved by implementing Business Process Automation (BPA). **(Refer Section 1.3.5 [Step 4])**

21. Give some examples of the Risks and Control objectives for Human Resource Process at configuration level. **(Refer Table 1.7.7)**

22. As a cyber-expert, you have been invited in a seminar to share your thoughts on data protection and privacy in today's electronic era. In your PowerPoint presentation on the same, you wish to incorporate the main principles on data protection and privacy enumerated under the IT Act, 2000. Identify them. **(Refer Section 1.9.2[III Privacy of Online Data])**

23. Explain the positive aspects contained in the IT Act 2000 and its provisions from the perspective of e-commerce in India.

(Refer Section 1.9.2[II Advantages of Cyber Laws])

24. General Controls are pervasive controls and apply to all the components of system, processes and data for a given enterprise or systems environment. As an IT consultant, discuss some of the controls covered under general controls which you would like to ensure for a given enterprise.

(Refer Section 1.6.2 [a])

25. Data that is waiting to be transmitted are liable to unauthorized access called 'Asynchronous Attack'. Explain various types of Asynchronous attacks on data. (Refer Section 1.4.3 Point C)21. Draw a Flowchart for the following process:

Leebay is a new e-commerce web site that is setting up business in India. Leebay and their partner bank Paxis have come up with a joint promotion plan for which the following offers are proposed. Customers can either login through a mobile app or directly from the website:

(i) If the payment mode chosen is 'Paxis Credit', then a 20% discount is given to the user.

(ii) If the payment mode chosen is 'Paxis Debit', then a 10% discount is given to the user.

(iii) If other payment modes are used, then no discount is given.

Also, to promote the downloads of its new smart phone app, the company has decided to give the following offer:

(i) If the purchase mode is 'Mobile App', then no surcharge is levied on the user.

(ii) If any other purchase mode is used, then additional 5% surcharge is levied on the user. This surcharge is applied on the bill after all necessary discounts have been applied.

With bill amount, payment mode and purchase mode as inputs, draw a flowchart for the billing procedure for Leebay.

Solution: The variables used are defined as follows:

PU_MODE: Purchase Mode **BILL_AMT:** Initial Bill Amount

TOT_BILL_AMT: Bill Amount after Discount **SCHG:** Surcharge

FIN_BILL_AMT: Final Bill Amount after Surcharge **DISC:** Discount

PMT_MODE: Payment Mode