IN THIS CHAPTER, WE WILL LEARN

- **Understanding of automation**
- **Enterprise Business Processes**
- **Automated Business Processes**
- **Enterprise Risk Management**
- **Controls**
- **Presentation of Business Processes**
- **Risk & controls for specific Business processes**
- **Regulatory & Compliance Requirements**

"Failure will never overtake me if my determination to succeed is strong enough"

Chapter 1

AUTOMATED BUSINESS PROCESSES

1. Introduction:

A company has several type of information systems built in and around diverse functions and business processes that automatically exchange information. However, due to size of the business it is rather difficult for a company person to gather all information. It is imperative to know the availability of a product, stock status of the product etc.

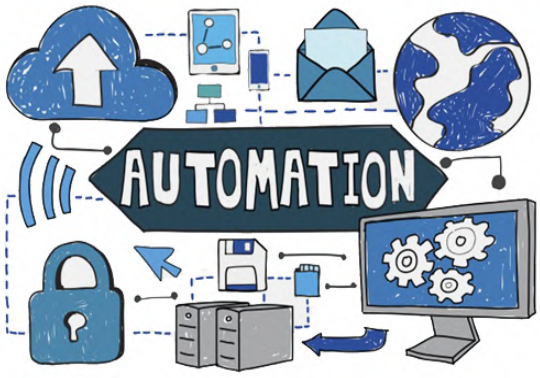


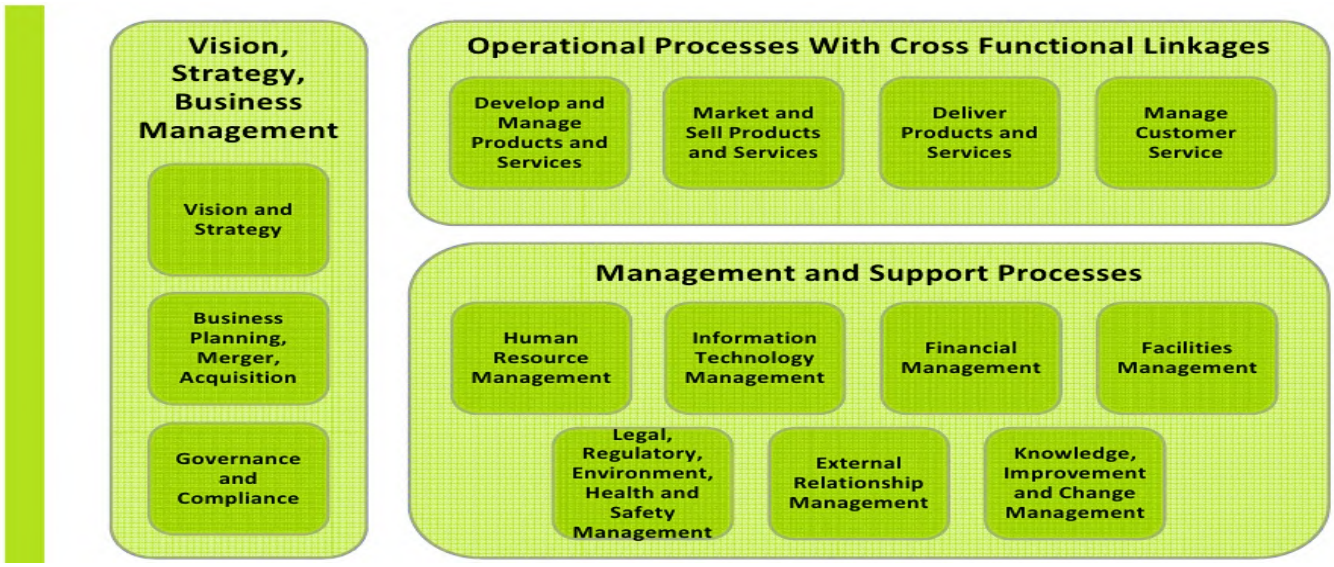
Figure 1

In order to solve this problem, EIS (Enterprise Information system) plays an important role. This system collects the data from various verticals of the business i.e. finance, production, manufacturing, sales and marketing and **storing the data in single central data repository.** As such EIS helps in smooth functioning of business processes by integrating these processes.

EIS provides platform to the organisation to integrate and coordinate their business processes on a robust (मजबूत) foundation. An EIS provides a single system that is central to the organisation that ensures information can be shared all across all functional level of organisation.

2. Enterprise Business Processes:

A business process is an activity that will accomplish a specific business goal. Business process management (BPM) is a systematic approach to improvise all the business processes.



2.1 Categories of Business Processes:

A business process is activity or a set of activities that will accomplish specific organizational goals. **Business Process Management** is a systematic approach to improvise various business activities.

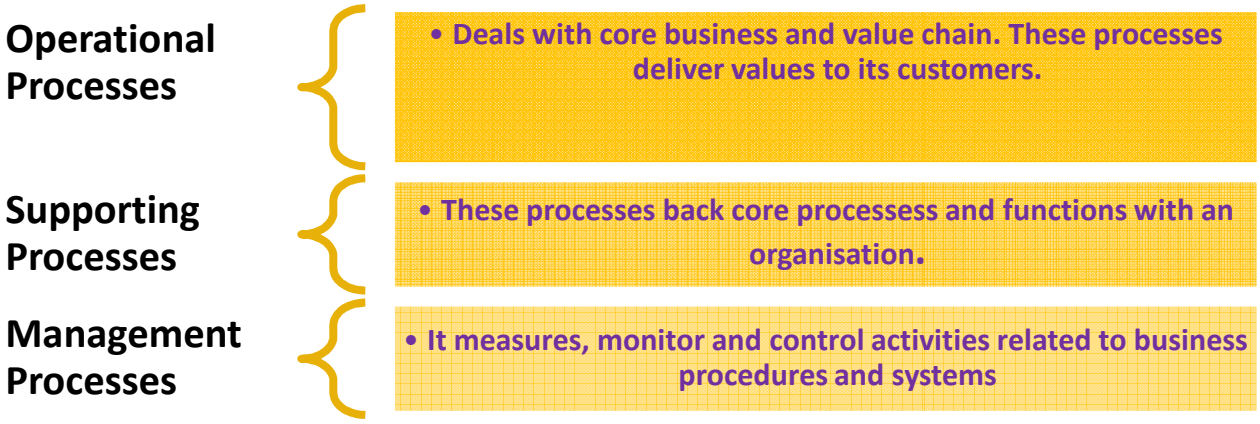


Figure 2

- **Operational Processes→**

  Deals with core business and value chain. These processes deliver values to its customers. It represents essential business activities that accomplish business objectives. For instance, order to cash cycle, purchase to pay cycle etc.

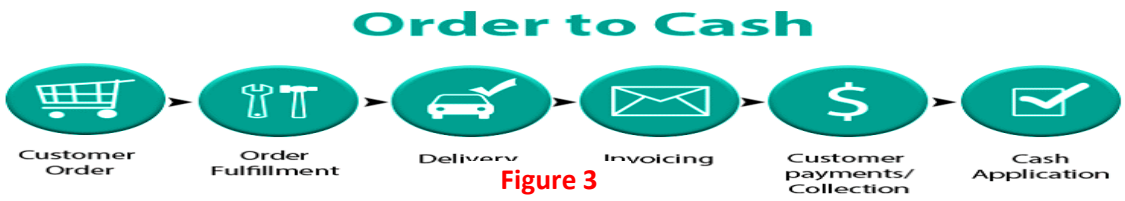


Figure 3

Customer Order	**:**	**Customer order received is documented.**
Order Fulfillment	**:**	**Order is fulfilled or service is scheduled.**
Delivery Note	**:**	**Order is shipped to customer or service is provided.**
Invoicing	**:**	**Invoice is created and sent to customer.**
Collections	**:**	**Customer sends payment/collection.**
Accounting	**:**	**Collection is accounted for in general ledger & applied.**

- **Supporting Processes→**

  These process backs **core processes and functions with an organisation.** One of the major difference between operational & supporting process is that **supporting process don't provide the values to the customer.** Some of the support processes are **HRM (Human Resource Management), accounting and workplace safety.**

Recruitment & Staffing → Goal setting → Training & development → Compensation & benefits → Performance Management → Career Development → Leadership Development

- **Management Processes→**

  These processes **monitor and control activities related to business procedures and systems.** Example of management processes includes internal communications, governance, strategic planning, budgeting, infrastructure etc.

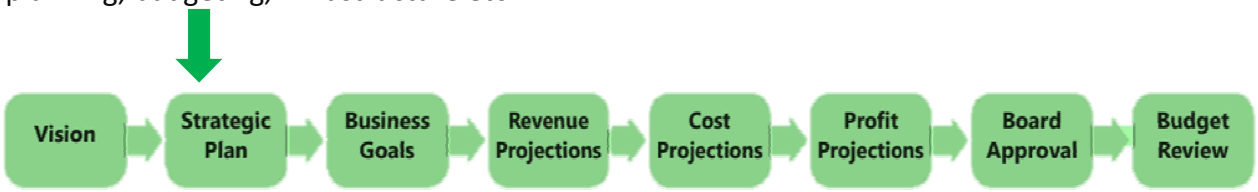


Figure 4

3. Automated Business Processes:

In the days of manual accounting, all the activities related to sales of product or service were done manually. Right from raising invoices till the accounting of the transactions. But with the introduction of technology, now-a-days almost all the processes of business have become automated. This helps enterprises to handle voluminous data.

Business process automation (BPA) is technology enabled automation of activities or services that accomplish a specific person and can be implemented for different business functions. It consists of integrating applications and using software applications throughout the organisation.

Objectives of BPA: **(Code to Remember → I. - C.A.T.)**

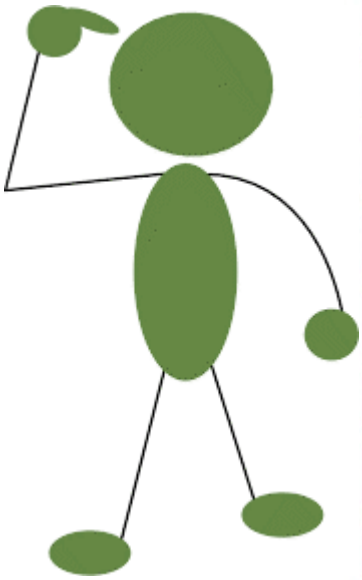
- **Integrity:** To ensure that no un-authorized amendments can be made in the data/information.
- **Confidentiality:** To ensure that data is only visible to persons who are authorized to see the same.
- **Availability:** To ensure that data is available when asked for.
- **Timeliness:** o ensure that data is made available in at the right time.

Benefits of BPA: **(Code to Remember → Q. - T.V. – R.R.I.G.)**

- **Quality & Consistency:** Ensure that every transaction is performed identically.
- **Time Saving:** Automation reduces **number of tasks employees** would otherwise need to do manually.
- **Visibility:** Automated processes are controlled & consistently operating accurately within timeline.
- **Reduce Costs:** Manual tasks cost more. Hence automation allows to accomplish tasks faster.
- **Reduce Turnaround Times:** Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection.
- **Improved Operational Efficiency:** Automation reduces time it takes to achieve a task. By automation, errors are eliminated and that best practices are constantly leveraged.
- **Governance & Reliability:** Consistency of automated process means stakeholders can rely on business processes to operate & offer reliable processes to customers.

Implementation of BPA:

Following are the steps involved in implementing business process automation. However before proceeding further it is to be noted that not all processes can be automated at a time. It involves a series of thoughts that will ultimately lead to complete 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 grant 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.

Above diagram depicts the steps involved in implementing business process automation:

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

The purpose for which an enterprise implements automation may vary from one company to another. Following are good reason to go for BPA→

Code to Remember: L. - E. P. I. C.

- **L**ack of management understanding of business processes.
- **E**rrors in manual processes leading to higher cost.
- **P**oor debtor management leading to high invoices aging and poor cash inflows.
- **I**neffective audit since documents are not easily traceable and available when needed.
- Poor **C**ustomer services.

(b) Step 2 → Understand the rules/regulations under which enterprise needs to comply with:

This is one of the most important step to be kept in mind. This includes understanding and following the rules and regulations, & document retention requirement. This governance is formulated by a combination of internal corporate policies, external industry regulations, and local laws. In this case it is imperative to understand the requirement of law in respect of retention of records for specified number of years.

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

At this step, all documents that are currently being used need to be documented. Considerable aspects:

1. What documents to be captured?
2. Where do they come from?
3. What format are they in: pdf, excel, word etc.
4. Who process the documents?
5. Impact of regulations on processing of the documents.
6. Can there be a better way to the job?

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

Once the above steps have been completed, entity needs to determine key objectives of 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 those;
- Timely : Achieved within a given time frame.

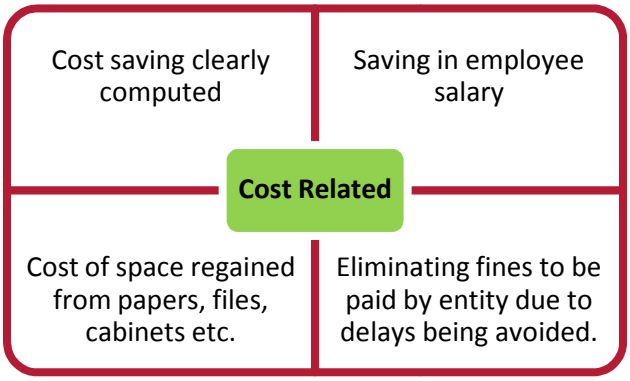
(e) Step 5 → Engage the business process consultant:

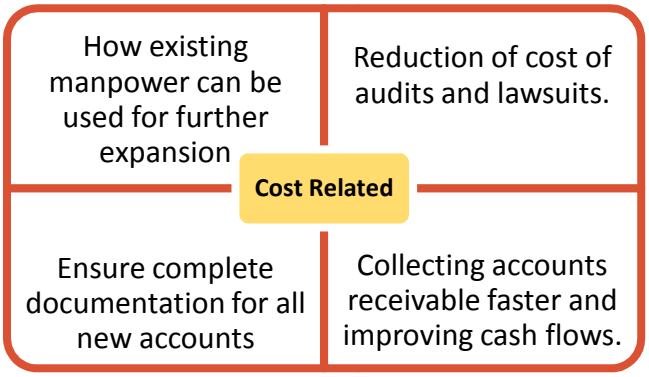
This is again critical step to achieve BPA. In order to ascertain with whom to partner with, following things to be kept in mind:

- Consultant's objective in understanding the entity.
- Does consultant have experience with entity business process?
- Is the consultant experienced?
- Whether consultant is capable of recommending & implementing a combination of hardware, software and services.
- Does consultant have required expertise to clearly articulate (स्पष्ट) business value of every aspect.

(f) Step 6→ Calculate the ROI for project:

The right stakeholders need to be engaged and involved to ensure that the benefits of BPA are clearly communicated and implementation is successful. However, it is Hercules effort to convince the senior management about the implementation of BPA. Some of justification points to be kept in mind→





(g) Step 7→ Developing the BPA:

Once the documentation of requirement, ROI has been computed and top management approval to go ahead has been received, consultant develops the requisite BPA.

(h) Step 8 → Testing the BPA:

Once developed, it is important to test the new process to determine how well it works. The process of testing is an iterative (चलने का) process, the objective being to remove all problems. Benefit of testing:

- Provide room for improvements prior to final launch.
- It helps in increasing user acceptance and decrease in resistance to change.
- Documentation final version of process will help in training people and also for quick reference.

4. Enterprise Risk Management:

Before implementing controls, it is imperative to consider the overall objectives, processes, organisation structure; technology deployed and risk appetite of the business. Based on this overall **risk management strategy** is to be formulated.

The Sarbanes Oxley Act (SOX)→

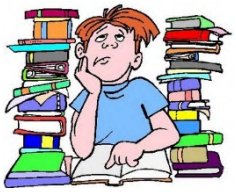
This act focus on implementation and review of internal controls related to financial statement. In an IT environment it is important to understand whether the relevant IT controls are implemented. Degree of control desired depends in the risk appetite of the business.

Enterprise Risk Management (ERM)→

This may be defined as a process, effected by entity's board of director, management and other personnel. The underlying premise of ERM is that every **entity (Profit or non-profit)** or **a governmental body** exists to provide value for its stakeholders.

ERM provides framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build values.

BENEFITS OF ENTERPRISE RISK MANAGEMENT:



Code to Remember: R^3 - M. - C. O. L. A.

- **Risk Response Decision:**
  ERM provides the rigor to identify & select among alternative risk responses – risk avoidance, reduction, sharing & acceptance.
- **Rationalize capital:**
  More robust information on entity's risk allows management to access capital requirement more effectively and also improvise capital allocation.
- **Response to multiple risks:**
  Business processes carry many inherent risks and ERM enables to provide integrated solution to manage it.
- **Minimize operational surprises & Losses:**
  Entities have capabilities to identify potential threats, assess risk and to put controls to mitigate or eliminate them. Such proactive actions help in reducing losses or cost if such risks remain undetected.
- **Cross-Enterprise risk identification & management:**
  Management not only needs to manage individual risks but also understand interrelated impacts.
- **Opportunities:**
  Business processes carry many inherent risks and ERM enables to provide integrated solution to manage it.
- **Link growth, risk and return:**
  Entities accept risk as part of value creation and they expect return commensurate (अनुरूप) with the risk.
  ERM provides framework which indicates the organisation with acceptable levels of risks.
- **Align risk appetite & strategy:**
  Risk appetite is the degree of risk acceptable by an entity. Management considers the risk appetite first in evaluating **strategic alternatives**, then **setting objectives,** aligned with **selected strategy.**

COMPONENTS OF ENTERPRISE RISK MANAGEMENT:

Code to Remember: I^2 -R^2 – C.O.M.E

- **Internal Environment:**
  This encompasses tone of an organisation & sets the basis of how risk is viewed and addressed by an entity's people **including risk management, risk appetite, integrity and ethical values.**
- **Information and communication:**
  Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out the responsibilities. Such information is required at all levels of management.
- **Risks Assessment:**
  Risks which are identified are analyzed to form basis of determining how they should be managed. Risks are assessed on both an inherent and a residual basis and assessment considers both risk likelihood and impact.
- **Risks Response:**
  Management selects an approach to align assessed risk with entity's risk tolerance and risk appetite. Personnel identify and evaluate possible response to risks (**Avoidance, accepting, reduction & sharing**)
- **Control Activities:**
  Policies and procedures that are established by the company ensures that risk responses that management selected are effectively carried out.
- **Objective Setting:**
  ERM should ensure that management has a process in place to set objectives and that chosen objectives support and align with overall objectives of the company.
- **Monitoring:**
  Entire ERM process should be monitored and modified wherever necessary. This ensures that the system can react dynamically. Monitoring is accomplished through ongoing management activities.
- **Event Identification:**
  Potential events that might have an impact on entity should be identified. This includes – **internal and external factors** that influence how potential events may affect strategy implementation and achievement of objectives.

5. Risks:

It is an event that may result in significant deviation from a planned objective which may result in unwanted negative consequences. The degree of risk associated with an event is determined by the likelihood of the event. However, following are the **RISKS ASSOCIATED WITH AUTOMATION**:

(a) Input and Access: Incomplete & inaccurate input transactions.
(b) Files and data transmission: All files & data may not be processed correctly due to network errors.
(c) Processing: Valid input data may not be processed due to bug.
(d) Output: It might be incomplete & inaccurate due to error or bug and is distributed to unauthorized personnel due to weak access control.
(e) Data: Master data may be changed by any unauthorized person(s).
(f) Infrastructure: In case of improper back up, data could be lost.

TYPES OF BUSINESS RISKS:

Strategic:
Risk that would prevent an organisation from meeting its goals.

Financial:
Risk that could result in negative financial impact to entity.

Regulatory:
Risk that expose organisation to fines and penalties from a regulatory agency due to non-compliance of laws and rules.

Reputational:
Risk that could expose organisation to negative publicity.

Operational:
Risk that could prevent organisation from operating in most effective and efficient manner or be disruptive to other operations.

6. Controls:

Controls are defined as policies, procedures, practices and organizational structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

The system of internal control extends beyond those matters which relates directly to the functions of the accounting system. The system of internal control is said to be well designed and properly operated when:

(a) All transactions are executed as per management's approval.
(b) All transactions are recorded at correct amount, in correct account and in accounting period to which it is relates.
(c) Assets are safeguarded from unauthorized access, use or disposition.
(d) The recorded assets are compared with existing assets at reasonable intervals and necessary actions are taken to reconcile the differences.

Now the same can be explained with the help of the example. Below is the diagrammatic representation of **purchase to pay** controls. There are 4 stages:

(a) Purchases.
(b) Good Receipt.
(c) Invoice Processing.
(d) Payment.

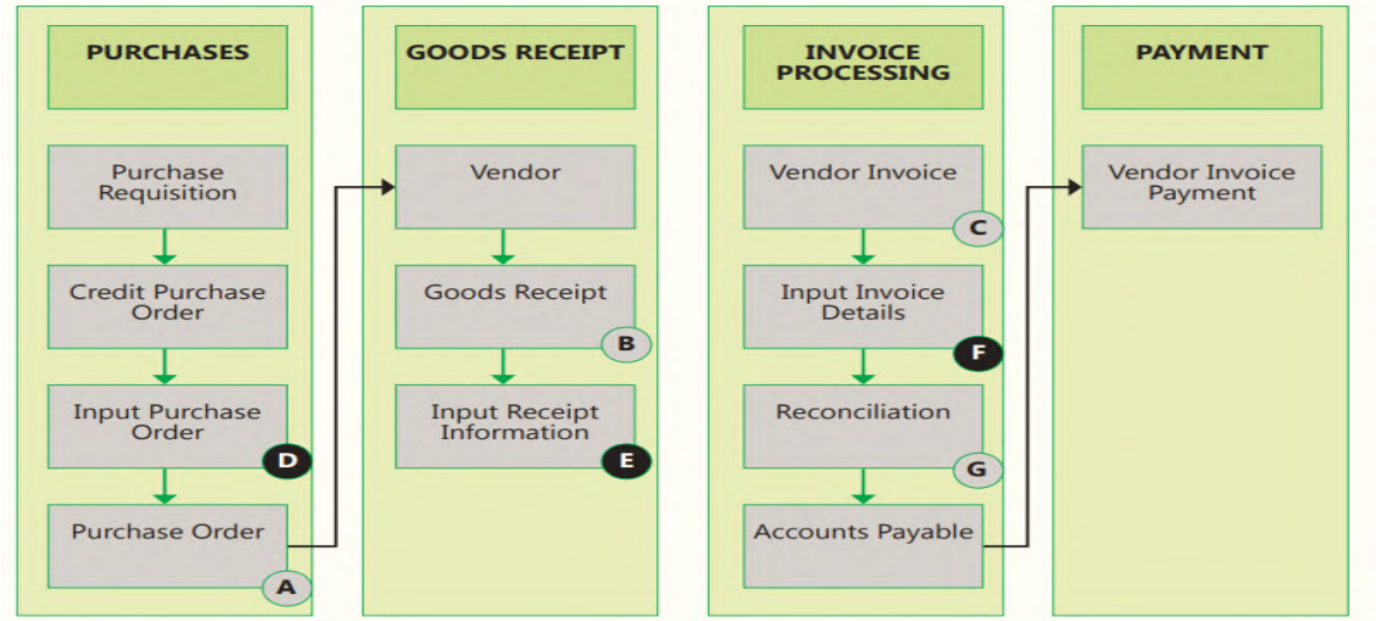


Figure 5

Purchases

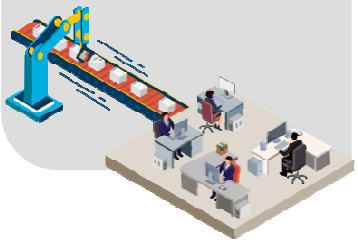
Employee of the company shall submit a purchase requsition to manager for approval. Upon approval, Purchase order is raised. PO may be raised manually or by system.

Good Receipt

PO is sent to vendor who will deliver the goods as per the terms of PO. When goods are received staff **checks the delivery note, PO number and acknowledges** receipt of material. A Good receipt number (GRN) is raised

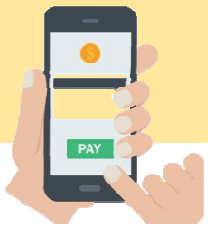
Invoice Processing

Vendor sends the invoice to the accounts payable department who will punch in the system. Checking of invoice with PO is done for the rates & with the GRN for the quantity.



Payment

If there is no mismatch between invoice, PO and GRN, payment is released to vendor based on the credit period decided



Based on the implementation of the above controls, it can be categorized under manual, semi-automated and automated. The objective of these controls is to mitigate the risk associated with the business.

Referring figure 5, the 3 categories can be explained:

Manual : Manual verifying the goods received as per PO and checking with vendor invoice.

Semi-Automated : Verification of goods receipt (E) with PO (D) could be automated, but the vendor invoice could be done manually in reconciliation process.

Automated : Automation can be done by the computer system by comparing D, E and F.

We will study the below topics in the INTERNAL CONTROL:

What is Internal Controls?

Internal control comprises of policies and procedures which are designed to provide the management reasonable assurance that overall goals of the business are achieved. **Following are the features of an internal control system**:

Code to Remember: **C.O.R.A.**

1. **C**ompliance to applicable laws and regulations.
2. **O**peration's efficiency and effectiveness facilitation.
3. **R**eliability of internal/external financial reporting.
4. **A**sset safeguarding of the business.

Effective Internal control

Control environment sets the tone of every organisation. It includes governance and management functions and attitudes, awareness and actions of those charged with governance and management concerning entity's internal control.

An entity's internal control system includes both automated and manual control. The nature of controls indeed effect the way the transactions initiated, recorded, processed and reported. **Manual element in control is required in following circumstances:**

(a) Large, unusual and non-recurring transactions.

(b) Errors prone circumstances.(Where error are difficult to predict).

(c) In monitoring the effectiveness of automated controls.

COMPONENT OF INTERNAL CONTROL SYSTEM

- Monitoring of functioning of all the 5 components.
- Going or separate evaluation or combination of both may be required for monitoring.
- Findings are evaluated by management & shared.

- Information is necessary for every business.
- Mgmt. collects information for external & internal sources to support functioning of internal controls.
- Such information's' are vital.

Figure 6

General Controls:-

- Control over Information technology management.
- Software acquisition, develop, maintenance.

Application Controls:-

- Ensures completeness, accuracy and validity of data captured & processing.
- Supporting applications are available.

Control Activities:-

- Actions established through policies that help ensure that management directives to mitigate risks. Performed at all level of entity.

Segregation of Duties:-

- Assigning responsibilities.
- This includes recording, custody of assets etc.
- Prevents control of complete process by one person.

- Risk may be defined as the possibility that an event will occur and adversely effects the organisation.
- **Risk assessment** involves a dynamic and iterative process for identifying & assessing risks.
- **Such assessment** forms basis for determining how risks are managed.
- **Risk assessment** requires management to consider impact of possible changes in external environment.

- Set of standards & Processes that provides basis for carrying out internal controls across the business.
- Control environment comprises integrity & ethical values of organisation.
- Helps top management in carrying out its governance responsibilities.

LIMITATIONS OF INTERNAL CONTROL SYSTEM

Code to Remember: U -C – M.A.P.

1. Most of the internal controls do not tend to detect **U**nusual transactions. There is possible of human error.
2. Management's consideration that **C**ost doesn't exceed benefits.
3. Manipulations by **M**anagement with respect to transactions & judgments.
4. A person may **A**buse the responsibilities for exercising an internal control.
5. **P**ossibility of circumvention of internal controls through collision with the employees or with parties outside the entity.

7. Diagrammatic representation of business processes:

7.1 FLOWCHARTS→

Flowcharts are used to design and document simple processes or programs. There are different types of flowcharts and each one has its different boxes. The most 2 common types of boxes in flowchart are as follows:

- A processing step; **usually called ACTIVITY and denoted as RECTANGULAR BOX.**
- A decision; **usually denoted as .**

A flowchart is described as "cross-functional" when pages are divided into different swimlanes* describing controls of different organizational unit.

(*A **swim lane** (or **swim lane** diagram) is used in process flow diagrams, or flowcharts, that visually distinguish job sharing and responsibilities for sub-processes of a business process. Swim lanes may be arranged either horizontally or vertically**)**

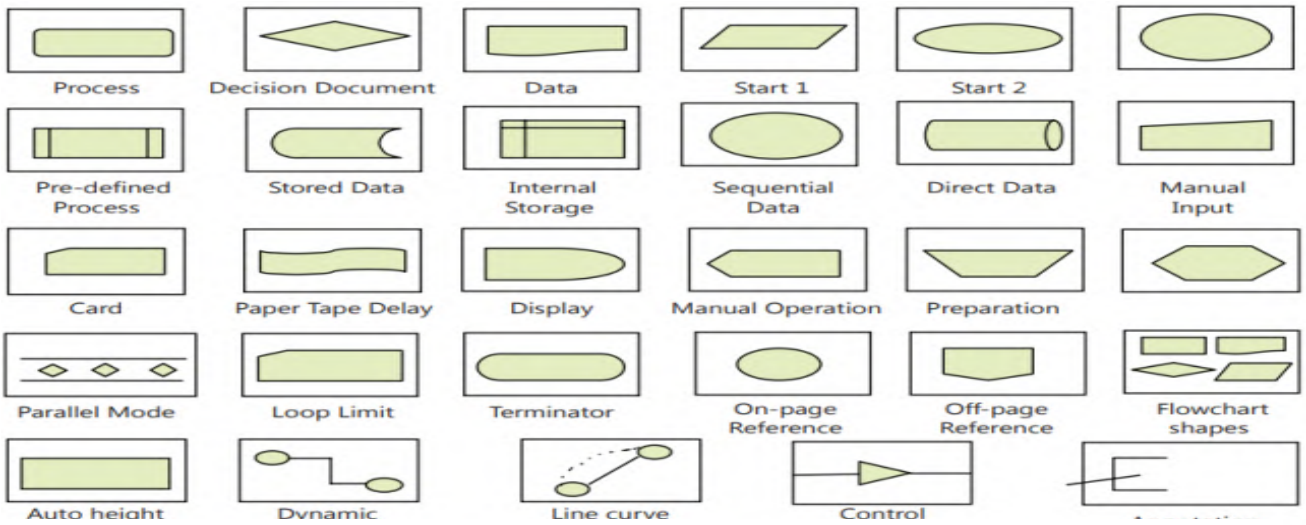
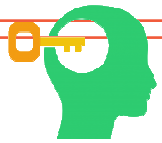


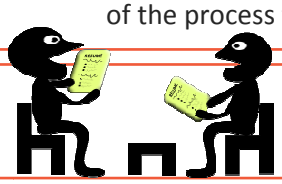
Figure 7

Flowchart Symbols:

Identify the business processes that are to be documented with a flowchart and establish the overall goals of business processes.



Based on the inputs from the business process, owner obtain a complete understanding of the process flow.



Prepare initial rough diagram & discuss with business process owner to confirm your Understanding of the process flow.

Obtain additional information from other stakeholders about the business processes. Any deviation should be highlighted and corrective steps to be taken.

Identify activities in each step and who is responsible for each activity.

Identify the starting point of the process. It means to ascertain the trigger point when the process is in action. Starting point generally falls under below 3 categories:

(a) External Events:

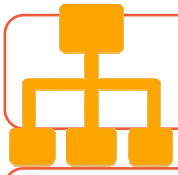
This includes initiation of transaction from other business system. For instance, if a persc purchase order in the system, the same will hit the production system to produce that material.

(b) Content Arrival:

For this starting point will be arrival of new document or other form of content.

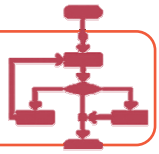
(c) Human Intervention:

Includes customer complaint and other human intervention from inside or outside organisation.



Separate the different steps in the process. Analyze how one step is connected to next step. Generally, we have events, activities & decision gateways which are showed using connectors, arrows.

In traditional business process model notation, steps are represented by different shapes depending on their functionalities i.e. events (Customer order), activity (process order), action & decision.



NOW, WILL STUDY ADVANTAGE AND DISADVANTAGE OF FLOWCHARTS:-

Advantages of Flowchart

Code to Remember
D.M.R.C. - C.A.D.R.E.

- **(a) Documentation:** Flowchart serves a good documentation which helps in reference and training new staff.
- **(b) Maintenance of program:** Flowcharts help programmer to concentrate attention on that part of information which is to be modified.
- **(c) Responsibilities Identification:** Business process can be identified to functional department thereby fixing responsibilities.
- **(d) Communication:** Flowchart communicates facts of business problem to solution seekers.
- **(e) Control Establishment:** Business process conflicts & risks can be easily identified for recommending solutions.
- **(f) Analysis:** Flowchart becomes blueprint of a system that is broken into parts for detailed study.
- **(g) Debugging of program:** Flowcharts help in detecting, locating and removing mistakes.
- **(h) Relationship understanding:** Flowchart helps in identification of relationship between program/processes.
- **(i) Effective Coding:** Flowcharts act as a guide during system analysis & program preparation phase.

Disadvantages of Flowchart

Code to Remember
C.M. - L.S.R.

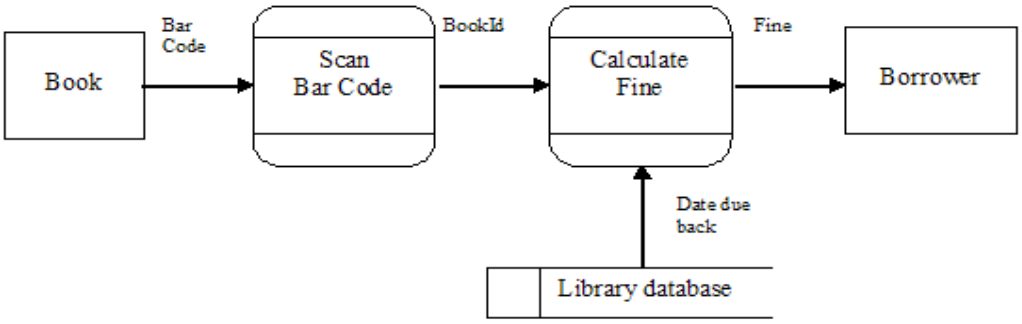
- **(a) Complex Logics:** Where problem logic is complex, flowchart usage becomes difficult.
- **(b) Modifications:** If modifications to a flowchart are required, it may require complete re-drawing.
- **(c) Link B/w condition & Actions:** It is difficult to establish conditions & actions to be taken for a condition, sometimes.
- **(d) Standardization:** Flowcharts, though easy to understand are not natural way of expressing problems and obtaining solutions.
- **(e) Reproduction:** Reproduction of flowcharts is a problem since symbols used in flowchart cannot be typed.

7.2 DATA FLOW DIAGRAM →

Data FLOW Diagram shows the flow of data from one place to another DFDs' describe the process showing how these processes are linked through data stores and how processes relates to the user and the outside world.

	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.
	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).

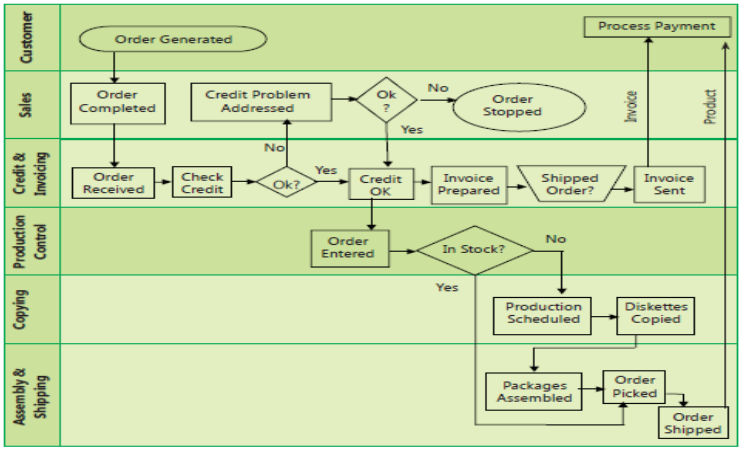
Example, book is borrowed from the library which is returned and fine collects due to delay.



- A library loans system identifies each book in its stock by a unique BookID.
- The BookID is encoded in a barcode attached to the book.
- When a borrower returns a book it is scanned and any fine that is due is calculated by extracting from the library database the date that the book was due back.

Diagrammatic represenation of specific business processes:

Customer Order Fulfilment



(A) Process start with the customer placing the order and the sales department creating sales order.

(B) The sales order goes through the credit and invoicing proces to check is it OK?

(C) If customer's credit check found to be NOT OK, will move to next step " credit problem addressed" followed by decision "OK". If "NO" order will stop.

(D) If customer's credit check found to be OK and if stock is available, **an invoice is prepared, goods are shipped & an invoice is sent to customer.** If stock not available, order is passed to "production" for manufacture & then goods shipped and invoices send to customer.

Order To cash

Below illustration indicates a complete process that happens when a product/service is sold and amount is received from the customer.

(a) Sales and Marketing:

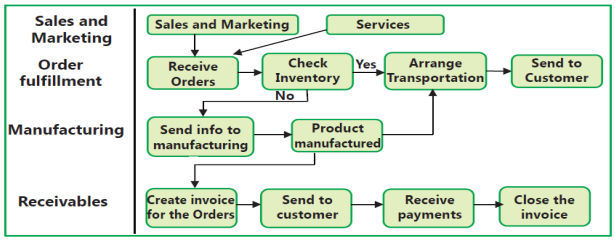
- Advertise and markets the compnay's product and book sales orders from the customer.

(b) Order Fulfilment:

- Receive order from SM (sales & Marketing).
- Check inventory level to confirm availibility of the product. If available, transportation is arranged and is sent to customer.

(c) Manufacturing:

- In case product is not available, this inforamtion is sent to manufacturing department so that product is manufactured and subsequently sent to customer.



(d) Receivables:

- Invoice raised, sned to customer. Amount received and that invoice get closed.

Procure to Pay

Below illustration indicates different processes identified specially to department/entity through "swimlanes" so that responsibilities are clearly defined.

(a) User Department:

- A user in an enterprise may require some material/service. Based on requirement, he/she rasie a PR (Purchase Requsition) to the procurement department.

(b) Procurement Department (PD):

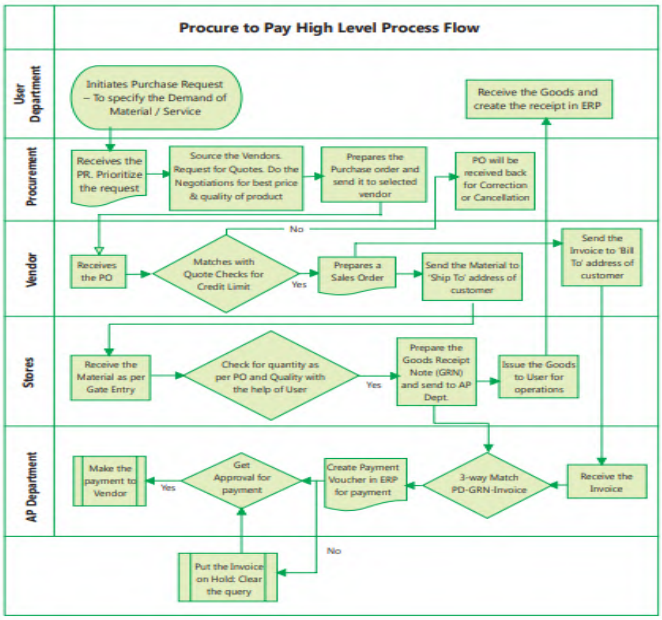
- PD receives PR and accordingly priortise request based on the need of the user.
- It is responsibility of PD to choose the best supplier of material for the material or services requested. PD calls for quotes from the potential vendors and negotiate thereafter.
- PO wil be realeased to selected vendor.

(c) Vendor:

- Vendor receives PO and carries out his own internal checks.
- Matches PO with the quotation sent and in case of discrepancy, seek clarification.
- If no discrepanices, vendor will raise sales order p& material is shipped to buyer.
- Vendor invoice is them send to accounts payable department, based on the address indicated in PO.

(d) Stores:

- Receive the material.
- Checks the quantity of material received with PO and qaulity with the user.
- Goods Received Notes (GRN) is prepared based on actual receipt of material & stores update stock . Then GRN is sent to accounts department for payment.



(e) Account Payable:

- AP will do the necessary checking at their end. This will ensure that material received is matching with PO quantity.
- If there is discrepancy, the same is sent for further clarification. In case no discrepancy, payment process starts.
- Finally payment is made to vendor.

8. Risk and controls for specific Business Processes:

8.1 Business Processes – Risk and Controls→

Suitable controls should be implemented to meet the requirement of the control objectives. These controls may be manual, automated or semi-automated. There is further categorization of controls based on the scenario. These are **preventive, detective or corrective.**

In computer system, controls should be checked at 3 levels namely **configuration, master and transaction level.**

CONFIGURATION

MEANING

It refers to a way software system is set up. It is the methodological process of defining options that are provided.

When any software is updated, values for various perimeters should be set up & business process work flow and business process rules of the enterprise.	Various modules of enterprise are purchase, sales, inventory, finance, user access etc. have to be configured. Some examples of such configurations are given in next tab	Mapping of accounts to front end transactions. Controls on parameter i.e. creation of customer type, vendor type etc. User Activation & De-activation Password Management

MASTERS

MEANING

Refers to way various parameters are set up for all the modules of software like purchase, inventory, finance etc.

The masters are first set up during installation and these are changed whenever business process rules or parameters are changed. Examples vendor master, customer master, account master etc.	The way master are set up will drive the way software will process transactions of that type.	**Examples of masters:** **Vendor Master** : Credit period **Customer Master** : Credit Limit **Material Master** : Measure Unit **Employee Master** : Name, Salary

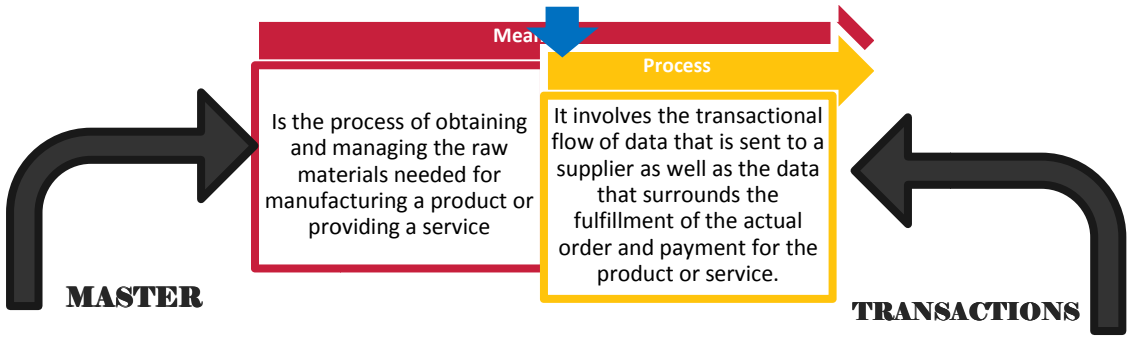
TRANSACTION MEANING

Refers refer to the actual transactions entered through menus and functions in the application software, through which all transactions for specific modules are initiated, authorized or approved

Sales transactions Purchase transactions Stock transfer transactions Journal entries 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.	Given below are some examples of risks and controls for a few business processes. The checklist provided below are illustrative

Given below are some examples of risks and controls for a few business processes. The checklist provided below is illustrative. Here we will study what is included in configuration, masters and transactions for various types of process.

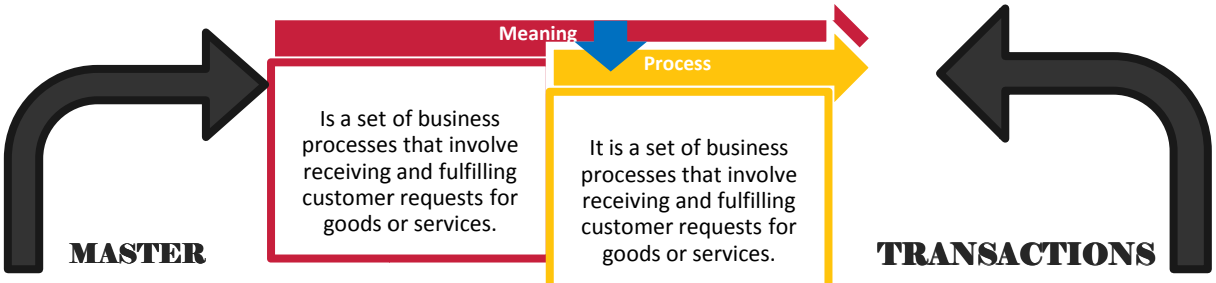
Procure to Pay (P2P)



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 & processed.	All valid changes to the supplier master file are input & processed.
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 remain 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.

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.

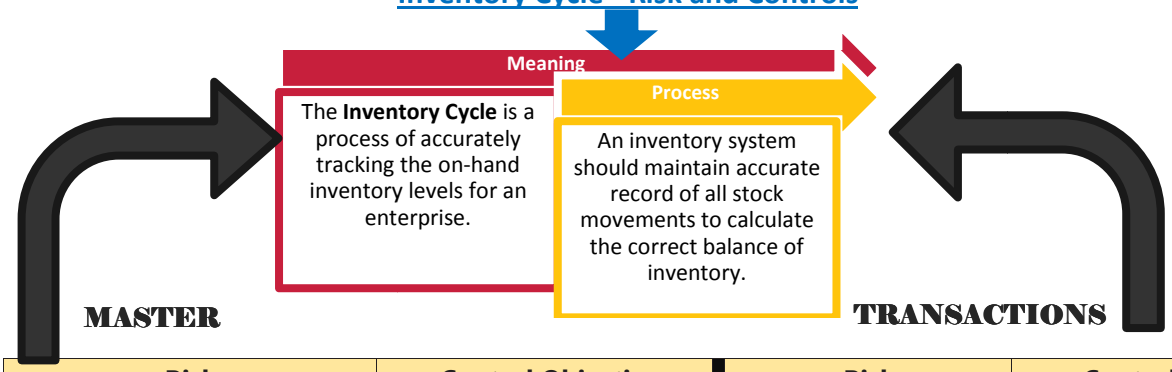
Procure to Pay (P2P)



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.

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 & cancellations of orders not input accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely.	Order entry data are transferred completely

Inventory Cycle - Risk and Controls



Risk	Control Objective	Risk	Control Objective
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.	Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
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.	Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.	Raw materials received are not recorded accurately.	Raw materials received are recorded accurately.
Inventory management master file data is not up to date.	Inventory mgmt. master file data remain up to date.	Raw materials received are not recorded in system.	All raw materials received are recorded

Typical phases of Inventory Cycle

- **The ordering phase:** The amount of time it takes to order and receive raw material.
- **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.
- **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.

HUMAN RESOURCES – RISKS AND CONTROLS

The **Human Resources** life cycle refers to human resources management and covers all the stages of an employee's time within a specific enterprise. Typical stage of HR cycle:

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.
2. **Orientation and Career Planning:** Orientation is the process by which the employee becomes a member of the company's work force through learning 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 her supervisors work out her long-term career goals 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 at the company and determined his long-term career objectives.
4. **Termination or Transition:** Some employees will leave company through retirement after a long & successful career. 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 system.

Risk	Control Objective	Risk	Control Objective
Employees who have left the company continue to have system access.	System access to be immediately removed when employees leave the company.	Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
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.	New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
		Invalid changes are made to the payroll master files.	Only valid changes are made to the payroll master files.
		Payroll master file data is not up to date.	Payroll master file data remain up to date.

FIXED ASSETS– RISKS AND CONTROLS

The 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, conditions and maintenance. Fixed assets process includes:-

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 maybe 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, 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.

MASTER		TRANSACTION	
Risk	**Control Objective**	**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.	Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
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.	Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
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.	Depreciation charges are not accurately calculated & recorded.	Depreciation charges are accurately calculated and recorded.
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.	Fixed asset maintenance activity records are not updated in a timely manner	Fixed asset maintenance activity records are updated in a timely manner.

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. Following steps in general ledger process:

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

CONFIGURATION		MASTERS	
Risk	**Control Objective**	**Risk**	**Control Objective**
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.	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 not input the changes.
System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.	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 not utilized within all entities of the corporation.
Non-standard journal entries are not tracked and are inappropriate.	All non-standard journal entries are tracked and are appropriate.	**TRANSACTIONS**	
Out-of-balance entries are not prohibited.	Out-of-balance entries are prohibited.	Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.
System controls are not in place for appropriate approval of write-offs.	System controls are in place for appropriate approval of write-offs.	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.

9. REGULATORY AND COMPLIANCE REQUIREMENT:

Companies Act 2013 | **Information Technology Act**

9.1 Companies Act 2013:

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 market place 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, improving service to the customer, efficiently handling cross border data flow etc.

An entity should have an efficient and effective financial information system to support decision-making and monitoring. In order to set up objectives for company about the adequacy of control in an IT environment, the risks and related controls should be clearly understood. Below are some of the regulatory requirements that need to be fulfilled by an entity:

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

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

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

Section 143(3) contains the **auditor's report** which states:

"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. The impact of this statement is that it involves continuous control monitoring during the year and not a review "as at" a particular date.

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.

MANAGEMENT RESPONSIBILITES

AUDITORS RESPONSIBILITES

CORPORATE GOVERNANCE REQUIREMENT

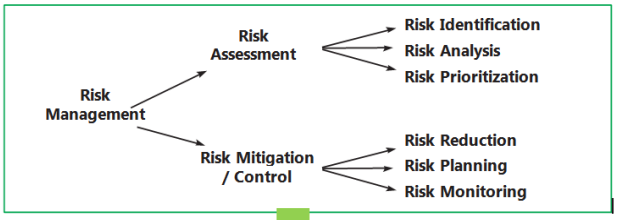
ENTERPRISE RISK MGMT. FRAMEWORK

MANAGEMENT'S RESPONSIBILITY

- The 2013 Act 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. Section 134(5)(e) 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.
- "Internal financial controls" are 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."
- 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.

AUDITORS' RESPONSIBILITY

- 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.
- 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.



CORPORATE GOVERNANCE REQUIREMENT

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

- 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.

AUDITORS' RESPONSIBILITY

Enterprise Risk Management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives.

- By identifying and pro-actively addressing risks and opportunities, business enterprises protect and create value for their stakeholders.
- Risk response strategy may include:-
  - **Avoidance**: exiting the activities resulting in risk.
  - **Reduction:** taking action to reduce the likelihood or impact related to the risk.
  - **Alternative Actions:** deciding and considering other feasible steps to minimize risks.
  - **Share or Insure:** transferring or sharing a portion of the risk, to finance it.
  - **Accept:** no action is taken, due to a cost/benefit decision.

9.2 Information Technology Act:

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 may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Advantages of Cyber Laws

The Act has also proposed a legal framework for the authentication and origin of electronic records/ communications through digital signature. From the perspective of e-commerce in India, the IT Act 2000 offers many positive aspects which are as follows. In order to remember points, below may be referred:

From company point of view:

- E-mail would now be a valid and **legal form of communication** in India that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out **electronic commerce** using the legal infrastructure provided by the Act
- Enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

From government point of view:

- The Act now allows Government to issue notification on the web thus heralding e-governance.
- IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions

Computer related Offences:

Code to Remember: V. - F.I.N.D. - P.A.T.H.

- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs:**
  These are malicious programs which are used to destroy or gain access to some electronic information.
- **Credit Card Fraud:**
  Unsuspecting victims would use infected computers to make online transactions
- **Hiding illicit business:**
  Terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business
- **Negative Image i.e. Harassment:**
  A fake profile of a person in social media to harness image of that person.
- **Web Defacement:**
  The homepage of a website is replaced with a defamatory (Bad) page.
- **Phishing and Email Scams:**
  Phishing involves fraudulently acquiring sensitive information through masquerading.
- **Sale of illegal Article:**
  Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet.
- **Theft of Confidential Information:**
  Information stored in computers is targeted by rivals, criminals and disgruntled employees.
- **Email Account Hacking :**
  If victim's email account is hacked and obscene emails are sent to people in victims address book.

Privacy:

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

- 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.

Cyber Crime:

In cybercrimes, computers are involved:

- Different from traditional crime where a person steals from others home by entering.
- In Cyber Crime, theft (Assume A) while sitting at home hacks the computer of another person B, and gathers some confidential and personal information. This has been done by not entering into victims (B's House).

Cyber Crime:

Below are some definitions used in IT Act:

Name	Description
"**Access**"	means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network
"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 impulse; ❒ 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.
"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
"Information"	Includes data, message, text, images, sound, voice, codes, computer program, software and databases or micro film or computer generated micro fiche.

"Data"	Means: 1. A representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner 2. 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

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.

Definition of Personal and Sensitive Personal data

Personal Information:-

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." Below are treated to be under the definition of personal information-

- Passwords
- Financial information
- Physical/physiological/mental health condition
- Sexual orientation
- Medical records and history; and
- Biometric information

Rule 5(1) 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.