## Risks:

Risk is happening of an unwanted event. In other words, what may go wrong in achieving the goal. For example, for a tobacco company, if the govt. bans tobacco in the country then the business may shut down. So the risk is banning of tobacco.

We can determine/calculate risk by two factors:

a) Likelihood of happening of the risk event. ( For example Highly possible, Not Possible)
b) Impact or consequence if the event occurs. (For example Loss of profit, Loss of reputation)

## Types of business risks:

- Strategic: These type of risk impact the goals of the organization.
- Financial: These types of risk impact the financials. For eg, Loss of asset.
- Regulatory (Compliance): These types of risks results in non-compliance to laws, rules and regulations.
- Reputational: This may result in impacting the image of the organization in the mind of the people.
- Operational: This may impact the operations of the organization and as a result of this the organization may not perform its activities in the most efficient manner.

- ***Memory Trick:***
  Salman filmed Romantic Rowdy Officer.
  Strategic ~ Salman
  Financial ~ filmed
  Regulatory (Compliance) ~ Romantic
  Reputational ~ Rowdy
  Operational ~ Officer

## Risk of Business Process Automation:

- Input & Access: The input data for processing may be incorrect or not provided in an authorized manner.
- File & Data transmission: There can be network issue for which files may not be processed accurately.
- Processing: The data processed may be inaccurate if there is any error or bug in the program.
- Output: The output may be erroneous due to program error or bug and may be distributed to unauthorized person (who is not supposed to receive the output)
- Data: There may not be strong control and as a result the data may be accessed by any person who is not supposed to access the data. After such unauthorised person accessing the data may change the data without anyone's knowledge.
- Infrastructure: Data & program may be lost if proper back up is not there.

***Memory Trick:***

India Fielded poorly on Dubai International.

Input & Access ~ India

File & Data transmission ~ Fielded

Processing ~ Poorly

Output ~ On

Data ~ Dubai

Infrastructure ~ International

## Controls

All business organization has some goals for which they are being formed. (Usually the goal is profit maximization). Now there can be some unwanted event due to which the goals may not be achieved. So in order to avoid such unwanted event or to ensure such unwanted event do not result in non-achievement of goal/goals, some steps must be

taken by the organization. These steps may are policies, Standard operating process, organization structure. Collectively, these steps are known as "**Controls**".
For example, the company may have a policy to procure only after POs are approved by General Manager.

An organization having a good effective internal control is said to have the following in the organization:

a) All transactions within the organization are approved by the management.
b) Transactions are properly accounted in the books of accounts keeping the accounting principles, accounting standards in mind.
c) All the assets of the organization are protected from being stolen or damaged.

## Types of controls

The controls are of following types:

a) Manual Control: For example, Invoice is manually verified with purchase order and challan.
b) Automated Control: For example, Invoice is verified with purchase order in the system.
c) Semi-automated Control: For example, includes both manual and automated control.

## Internal Control

We can understand the concept of internal control from the concept of "**Control**" has described above.
Internal Control refers to policies put in place and activities carried out by the organization so that the objectives and goals of the organization can be met.
The internal control system achieves the following objective:

1) Conducting the business efficiently
2) Proper and accurate accounting of transactions
3) Detection and prevention of fraud
4) Preparing the Financial Statements (P&L, Balance Sheet) on time
5) All the assets of the organization are protected from being stolen or damaged.

***Memory Trick:***

Egg And Anda Fried pakora Dosa Achari Poha Onion Tikka Sada Aloo

Egg ~ efficient conduct of business

And Aanda ~ Accurate Accounting

Fried pakora Dosa ~ Fraud Prevention & Detection

Achari Poha Onion Tikka ~ Accounts Preparation on time

Sada Aloo ~ Safeguarding Assets

## Components of internal control

Before we go into details-Lets understand in a summarised form.

The internal control shall be implemented by the top management. That means the top management will be the most interested party to have internal control in an organization. So implement controls, the top management will create an environment where everyone will be aware of controls. This is **Control Environment**.

The next two components will be finding out or anticipating what may go wrong and what impact will it create. This is **Risk Assessment**. And once, the risk is assessed, policies and activities will be in decided and implemented in the organization so that the risk so assessed can be avoided. This is **Control Activities**.

In order to ensure that there is regular communication happens with respect to activities, risk anticipated, there should be a clear communication among the employees, departments and top management. This is **Information & Communication**.

Finally, to ensure that the controls are in place and are working properly, regular monitoring/examination of the above components take place. This is **Monitoring controls.**

Consists of 5 components:

1) **Control Environment**: Board of Directors & top management creates awareness and drives initiatives for good internal controls across the organization. This is otherwise called **tone at the top**.
2) **Risk Assessment**: Management identifies events which can go wrong and results in non-achievement of organizational goals. These events can result in the following areas:

a) In operations resulting in losses.
b) In financial accounting resulting in accurate financial reporting.
c) In statutory compliance resulting in non-compliance to rules and regulations.

3) **Control Activities:** Policies and activities will be in decided and implemented in the organization so that the risk so assessed can be avoided. The control activities are as follows:

a) Segregation of Duties (SOD): This means all the activities will not be performed by one single person. If one person does all the activities end to end, then there is a possibility of fraud which is difficult to detect. Also, if that person does any mistake or error unintentionally (not with the motive of doing fraud), it will be difficult to detect. For eg, If same one person creates PO, books invoices and makes payment, then if that person fraudulently books an invoice and makes a payment then it will be difficult to catch such fraudulent activity.
So usually one person makes the transaction, one person records the transaction and one person will authorise the transaction.

b) Application Control: These refers that controls which ensures all the transactions have been recorded (nothing missed out), all the transactions have been correctly recorded, All the transactions have been approved by higher authority and nothing has been recorded without the knowledge of higher management. For example- Controls like Bank reconciliation, Third party (Debtor or vendor) balance confirmation etc.

c) General Control: These include control over information technology so that there is IT security (to avoid cyber-crime), proper IT infrastructure and correct software acquisition.

4) **Information & Communication**: As discussed earlier, this refers to that there is regular communication happens with respect to activities, risk anticipated, there should be a clear communication among the employees, departments and top management.

5) **Monitoring controls:** Finally to ensure that the controls are in place and are working properly, regular monitoring/examination of the above components take place. This ensures all the above mentioned components of internal controls are in place and working properly.

## Limitations of internal control:

1. Management will always want the **cost of putting the controls should not be more than the benefit.** For example, if the impact of fraud risk is only Rs 100000, management will not want to have controls in place which will cost the company Rs 500000/-.
2. **Unusual transaction** not usually covered by internal control. For example, if there is a mistake, carelessness etc. it may not be covered by controls implemented by the company.
3. If there is **a collusion** (that if employees make a pact among themselves to carry out a fraud) then internal control will not work or be effective. For example, if the accountant, purchase manager and stores in charge make plan to make payment for false purchase then it is very much difficult to catch such fraud.
4. **Top management personnel decide to deviate** from control then internal control will not work/be effective. For example, if the Managing director uses his/her power to make false payment, then internal control cannot prevent that.

## Diagrammatic representation of business process

(*Flowcharts, Steps for creating flowcharts, Business process modelling notation (BPMN), Advantages of flowcharts, Limitations of Flowcharts, Data flow diagrams, Overview of DFD*)
: Study material may be referred for this section.

*Risk & Controls for specific business process & Regulatory & Compliance Requirements*
*Will be covered in last part- Which I will try to upload at the earliest.*