

Categories of Business Processes

III. Management Processes – Budgeting Example

The **key guiding factor** for any business process shall be **top management vision and mission**.

This vision and mission shall be achieved through implementing Operational, Support and Management services.

These are referred to as categories of business process.

Table : Example representing all categories of Business Processes

S. No.	Nature of Business Decision	Description of decision
1	Vision and Mission	One of Asia's largest dairy product companies decided in 2005 to increase its turnover by 2X in next ten years . The present turnover was ` 10,000/- Crores.
2	Management Process	The top management sat down and listed activities to be done to achieve the said turnover . This included : ✓ Enter into new markets . It was <u>decided to have an all India presence</u> . At present the company products were being sold across 20 out of 25 states and all state capital excluding the four metros, namely Delhi, Mumbai, Chennai and Kolkata. ✓ Launch new products . Presently the company was mainly selling milk products . Few new products that were decided to be sold in future included; <u>Biscuits, Toast, Atta, Packaged Drinking Water</u> . ✓ Acquire existing dairies in markets <u>where company had no presence</u> .
3	Support Process	For <u>all activities to be done as envisioned by top management</u> , a huge effort was needed on human resources front. This included - ✓ <u>Defining and creating a new management structure</u> ✓ <u>Performing all human resource activities as listed above</u> .
4	Operational Process	Post the management processes, it is on the operational managers to implement the decisions in actual working form . It is <u>here where the whole hard job is done</u> .

Risks And Its Management

Introduction

- **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.

Sources of Risk

- 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 :**

1. **Potential loss** that exists as the result of threat/vulnerability process;
2. **Uncertainty of loss** expressed in terms of probability of such loss; and
3. The probability/likelihood that a **threat agent mounting a specific attack** against a particular system.

Types of Risks

The risks broadly can be categorized as follows :

A. Business Risks :

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

1. Strategic Risk :

- ✓ These are the risks that would **prevent an organization from accomplishing its objectives** (meeting its goals).
- ✓ **Examples** include risks related to strategy, political, economic, regulatory, and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs

2. Financial Risk :

- ✓ Risk that could **result in a negative financial impact to the organization** (waste or loss of assets).
- ✓ **Examples** include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.

3. Regulatory (Compliance) Risk :

- ✓ Risk that could **expose the organization to fines and penalties from a regulatory agency due to non-compliance** with laws and regulations.
- ✓ **Examples** include Violation of laws or regulations governing areas such as environmental, employee health and safety, protection of personal data in accordance with global data protection requirements and local tax or statutory laws.

4. Operational Risk :

- ✓ Risk that could **prevent the organization from operating in the most effective and efficient manner** or be disruptive to other operations.
- ✓ **Examples** include risks related to the organization's human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration.

5. Hazard Risk :

- ✓ Risks that are **insurable**, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.

6. Residual Risk :

- ✓ **Any risk remaining even after the counter measures are analyzed and implemented** is called Residual Risk.
- ✓ An organization's **management of risk should consider these two areas :**
Acceptance of residual risk and Selection of safeguards.
 - **Even when safeguards are applied**, there is probably going to be some residual risk. The risk can be minimized, but it can seldom be eliminated.
- ✓ Residual risk must be **kept at a minimal, acceptable level**.

As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the **risk can be managed**

B. Technology Risk : Done in Chapter 5 under heading - Challenges of IT

C. Data related risks :

These include Physical access of data and Electronic access of data. (these are well explained in Chapter 3)

Risk Management and Related Terms

Various terminologies relating to risk management are given as follows :

▪ Risk Management :

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

▪ Asset :

- ✓ Asset can be defined as **something of value to the organization**; e.g., information in electronic or physical form, software systems, employees.
- ✓ Irrespective of the nature of the assets themselves, they all have one or more of the following characteristics :
 - They are recognized to be of value to the organization.
 - They are not easily replaceable without cost, skill, time, resources or a combination.
 - They form a part of the organization's corporate identity, without which, the organization may be threatened.
 - Their data classification would normally be Proprietary, Highly confidential or even Top Secret.
- ✓ It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

▪ Vulnerability :

- ✓ Vulnerability is the **weakness in the system safeguards** that **exposes the system to threats.**
- ✓ It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat.
- ✓ Vulnerabilities **potentially "allow" a threat - to harm or exploit** the system.
For example, vulnerability could be a **poor access control method** allowing dishonest employees (the threat) to exploit the system to adjust their own records.
- ✓ Some **examples** of vulnerabilities are given as follows :
 - Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
 - Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.
- ✓ **Missing safeguards often determine the level of vulnerability.**
- ✓ Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing and penetration analysis.
- ✓ Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following :
 - **Allows an attacker** to execute commands as another user' or
 - Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
 - Allows an attacker to pose as another entity' or
 - Allows an attacker to conduct a denial of service'.



Threat :

- ✓ Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat.
- ✓ It is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm.
- ✓ It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems.
- ✓ **Every system has a data**, which is considered as a fuel to drive a system, **data is nothing but assets**. Assets and threats are closely correlated. A threat cannot exist without a target asset.
- ✓ Threats are typically prevented by applying some sort of protection to assets.

Likelihood :

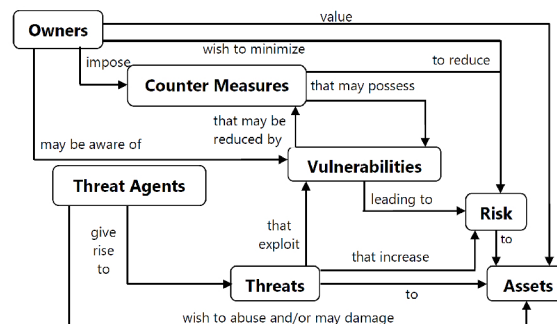
- ✓ Likelihood of the threat occurring is the estimation of the probability - that the threat will succeed in achieving an undesirable event.
- ✓ The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat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

Exposure :

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

Attack :

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



Risk and Related Terms

▪ **Counter Measure :**

- ✓ *An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.*

For example, well known threat 'spoofing the user identity', has **two countermeasures** :

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

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

Concludingly,

Risk can be defined as

the potential harm caused - if a threat exploits - a particular vulnerability to cause damage - to an asset, and

Risk Analysis is defined as

the process of identifying security risks and determining their magnitude and impact on an organization.

Risk Assessment includes the following :

- *Identification of threats and vulnerabilities* in the system;
- *Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should / if an identified vulnerability be / is 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.



Risk Management Strategies

Effective risk management begins with a clear understanding of an enterprise's risk appetite and identifying high-level risk exposures.

After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified.

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them.

Some risks may be minor and it may not be cost effective to implement expensive control processes for them.

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 :

Risk management strategy is explained and illustrated below :

1. Tolerate/Accept the risk.

- ✓ One of the primary functions of management is managing risk.
- ✓ Some risks may be considered minor because their impact and probability of occurrence is low.
- ✓ In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

2. Terminate/Eliminate the risk.

- ✓ It is possible for a risk to be associated with the use of a technology, supplier, or vendor.
- ✓ The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

3. 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.

4. 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.

5. Turn back.

- ✓ Where the probability or impact of the risk is very low, then management may **decide to ignore the risk**.

Framework of Internal Control as per Standards on Auditing

SA 315 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.

Control Activities

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.

Enterprise Risk Management Framework

ERM provides a **framework** for risk management which **typically involves**

- ✓ **identifying events** or circumstances relevant to the organization's objectives (risks and opportunities),
- ✓ **assessing** them in terms of likelihood and magnitude of impact,
- ✓ **determining** a response strategy and monitoring progress.

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.