|  |  |
| --- | --- |
|  |  |
| **RISK MANAGEMENT – A HELICPOTER VIEW** |  |

1. **What is risk?**

**Answer :**

**Our definition** – Risk is **uncertainty** that **matters.**

**ISO 31000** – Risk is the **affect of uncertainty** on **objectives**.

Foot note – Affect refers to **variability** from what is expected, **both positive and negative.**

One of the 11 principles of ISO 31000 clearly states that we are dealing with all types of uncertainty i.e.,**uncertain event or conditions.(**Elaborated in Q5 below)

Various other standards on **Operational Risk**, **Financial Risk**, **Environmental Risk**,**COBIT, Basel III, ICAI Internal Audit Standard 315, ICAI RBIA, Oxford dictionary,** etc. have their own definitions of risk and all these definitions comprise of the two elements –

**Uncertainty Element**

**Effect on Objectives Element**

Hence, many authorities define risk as –

Risk = **Probability/Frequency x Consequence/Impact.**

This results in a **2x2** matrix for **Risk Prioritization** as shown below :

**Frequency - Severity matrix for Risk Prioritization along with Response Strategy**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Frequency** |  |
|  |  | High | Low |
|  | High | HFHS - *Avoid* | LFHS - *Transfer/Share* |
| **Severity** |  |  |  |
|  |  |  |  |
|  | Low | HFLS - *Reduce/Mitigate* | LFLS - *Accept*/*Self Insure* |

We also know that there are 4 popular Risk Response Strategies captured by the mnemonic RATA or MATA standing for :

* Risk **Reduction/Mitigation**
* Risk **Avoidance**
* Risk **Transfer/Sharing**
* Risk **Acceptance**

**Following examples would provide a good idea -**

* **Low Loss Frequency, Low Loss Severity( LFLS)**

The first type of risk is low frequency and low loss severity events. One example is theft of office stationery. **The best way to deal with such risk is to retain them in full.Why? -**

The costs of managing them usually outweigh the cost of retaining them.

* **High Loss Frequency, Low Loss Severity (HFLS)**

The second type of risk is high loss frequency and low loss severity events. This type of risk is more serious. Examples of such risks include workers’ injuries and shoplifting.

**The most common way to manage this type of risk is through reduction i.e. Mitigation. For example, by installing security cameras and sensors, you can prevent shoplifting.**

If these losses occur frequently, you can also consider accepting these risks as part of your business.

Finally, do note that these small losses might accumulate to a big sum at the end of the year. So you may consider insuring these risks as well.

* **Low Loss Frequency, High Loss Severity (LFHS)**

**Insurance is the best technique to deal with risks that have low loss frequency, and high loss severity. These types of risk are usually catastrophic that might bankrupt your business.**

The low probability of these losses makes the insurance affordable despite the severity.

**Some examples of these type of risks are:**

* **Fires and explosions of your business premise**
* **Liability lawsuits**
* **Natural disasters**
* **High Loss Frequency, High Loss Severity (HFHS)**

The last type of risk is high loss frequency and severity events. **The first thing to consider is whether can you avoid it**. For example, if you develop a product that you know will have a high chance of a lawsuit, you should not launch that product.

Consider using a both mitigation and insurance techniques if avoidance is not possible.

Prevention techniques can reduce the frequency of losses to low loss frequency. You can also try reducing the loss through reduction techniques. Then you can use insurance to transfer the residual risks as the premiums are now more affordable.

1. **How is risk related to objectives?**

**Answer :**

**ISO 31000** – Risk is the **affect of uncertainty** on **objectives**.

Hence, **what is at risk?**

Obviously, the **objectives** are at risk. Thus, **Strategic/Operational/Financial Risk**  may be defined as the **effect of uncertainty on organization’s Strategic/Operational/Financial Objectives.**

There is a **hierarchy of objectives in an organization** –

All these got to be aligned- Paving the way for **Enterprise Risk Management (ERM) –** a **holistic** and **integrated** approach of managing risk for the **entire organization** as against the **silo** approach- chapter 8

**Strategic or Corporate Objectives**

**Departmental or Functional Objectives.**

**Program or Portfolio Objectives**

**Project or Operational Objectives**

**Process Objectives.**

**Activity Objectives.**

Risk and Risk management is defined **Top Down**, but managed **Bottom Up.**

1. **Are all risks bad?**

**Answer :**

**ISO 31000** – Risk is the **affect of uncertainty** on **objectives**. “Affect“ can be both Positive or Negative…….this means, we have both bad and good risks. These may accordingly increase/decrease costs, waste/save time, damage/enhance reputation, de-prove/improve performance, etc. Bad/Good risks are technically defined as Threats/Opportunities.

1. **Do we need to have separate RM framework for managing opportunities?**

**Answer :**

No! The same RM framework designed to identify, assess, manage, review and monitor threats can be used for opportunities as well - its just the mode of thinking that needs to be changed.

Remember, threats and opportunities are the same, they just differ in terms of sign.

1. **What is the common myth about risk?**

**Answer :**

Myth - Risk only relates to **negative** future **events**....This is incorrect because :

* Risk may be an **opportunity**
* Risk **may not** relate to a **future event**

**Based on the second bullet above, we may consider 4 types of risks –**

1. **Stochastic Risks –** Risk arising from uncertain future **events** that matters.

* What if one of my main suppliers goes out of business?
* What is one of my key employees leave?
* We do attach a ceratin probabilities to these uncertainties and we also asses their impact and then there are certain risk management responses that we can have to address them.

***Note –*** *There are 3 additional types of risk which do not involve an uncertain future event, instead, they involve an uncertain future condition –*

1. **Variability Risk -** Things that we know will **happen**.... but we **do not know the outcome**

Eg - Productivity , Commodity prices, Exchange rate fluctuations, digging a well, running a trial, etc.

**How to deal with these?**

First of all, create a range or in other words bind the outcome with minima ,most likely and maxima - A 3 Point of Estimate. Then use some kind of quantitative technique like **Monte Carlo Simulation (MCS)** – to be learnt in Chapter 5 to know what effect would it have on our objectives.

1. **Ambiguity Risk -** We don’t quite understand what all can happen –Regulatory risk, launching a product and competitive behaviour, etc.

So, it arises from lack of experience or lack of knowledge or lack of understanding - We can gain that knowledge, by sub-contracting( i.e., outsourcing)

1. **Emergent Risks** - The **Unknowable Unknowns** – **BLACK SWAN**

Risks whose origins we **don’t** know and we **can’t** know - these are risks we **never expected** but they come straight right out of the blue

The only way to deal with them is by making people, processes and systems in the organisation which are flexible and resilient. We got to have contingency planning in the form of **Business Continuity Planning (BCP)** and **Disaster Recovery Planning (DRP).**

1. **Explain the Risk Management Framework ( RMF)**

**The following 8 questions need to be asked and answered :**

1. **Governance** - **Objective setting** and **Risk Appetite** (Chapter 7 ) - What are we trying to achieve?

Note – *Risk Capacity* – Risk that the organization can take, say $200m

***Risk Appetite*** – Risk that the organization is willing to take, say $170m

***Actual Risk*** – Say $150m.

1. **Risk Identification** ( Chapter 2 ) - What uncertainties can affect my objectives (both +/-)
2. **Risk Assessment/Prioritization** - Out of the risks identified in q2, which risks are **more important**?

Prioritisation has to be in 2 dimensions...

What is the chance of that uncertainty materialising (probability)

And if the uncertainty does materialise, what impact ( +/-) will it have on our goals - Remember risk includes both threats and opportunities. Hence, this requires –

* **Risk Quantification –** Chapter 5 : Risk Models
* **Risk Evaluation –** Chapter 2 : Sources and Evaluation of Risks.

Now we get a prioritized list of uncertainties...

1. **Risk Response Planning and Strategizing** - What are we going to do about those key risks ?

**RATA**( Chapter 3 )

1. **Implement the Risk Response Strategy** – This is the most important step as many organizations just plan and don’t implement. This step has been missed by many authors including ICAI Study Mat.
2. **Evaluation of Risk Management Strategies**(Chapter 4) : Did our risk response action work as we had wanted or expected?

**Answer :**

In a way , this is post event performance appraisal or evaluation for improving the future - We might need tk modify our approach.

1. **What changed** - Monitor and review the dynamic environment as well as the firm.

*Note – RM is a proactive and continuous exercise. RM is a forward looking radar. It scans the future, of course using experience of the past.*

1. **Risk Reporting and Communication –** There has to be proper reporting to all stakeholders. The process owners will report project manager. Project Owner will report the program manager. Program owner will report to the department manager. Department manager will report to the senior management.

When all this is done holistically and in an integrated manner, it is called Enterprise Risk Management (ERM : Chapter 8)