

RISK MANAGEMENT – A HELICOPTER VIEW

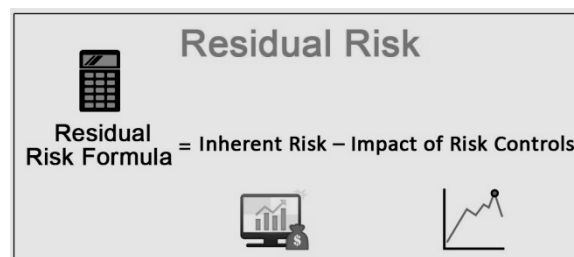
contd....

7. What is inherent risk and residual risk?

Answer :

Inherent risk is the level of risk assuming no internal controls, while residual risk is the level of risk after considering the impact of internal controls. For example, the risk of 'over/ understatement of revenue' without considering any internal controls indicates inherent risk. The above risk when considered with internal controls in place (say, monthly reconciliation of revenue and follow up, correction of discrepancies, etc.) indicate residual risk.

The objective of internal controls is to reduce the inherent risk and keep the residual risk within the organization's risk appetite. The gap between the inherent risk and residual risk shows the strength of the control and is known as the control score.



As a residual risk example, you can consider the car seat belts. Initially, without seatbelts, there were a lot of deaths and injuries due to accidents. After the seat belts were installed in the cars and made mandatory to wear by the law, there was a significant reduction in deaths and injuries. However, there are still injuries and deaths by the accidents even after the driver wears these seat belts; this could be said as a residual risk. The seat belts have been successful in mitigating the risk, but some risk is still left, which is not captured; that is why there are deaths by accident.

Let us look at further residual risk examples so that we can find out what the residual risk could be for an organization (in terms of potential loss).

Example

Consider the firm which has recently taken up a new project.

Without any risk controls, the firm could lose \$ 500 million. However, the firm prepares

and follows risk governance guidelines and takes necessary steps to calculate residual risk and mitigate some of the known risks. After taking the internal controls, the firm has calculated the impact of risk controls as \$ 400 million. This impact can be said as the amount of risk loss reduced by taking control measures.

- Now, inherent risk = \$ 500 million
- Impact of risk controls = \$ 400 million
- Thus, residual risk = inherent risk – impact of risk controls = 500 – 400 = \$ 100 million

Example : Risk of recording fictitious cash payments

Cash Disbursements : Three-way match in Accounts Payable (purchase order, receiving report, invoice)

Horizon Ltd. uses the disbursement module of its ERP system to print checks. Treasury prints checks based on the due date in the system and then matches the checks to the appropriate support (invoice, receiving report, purchase order). The checks are then given to the controller and CFO for approval and signature. After the checks are signed, they are given to the receptionist for mailing, and the support is returned to AP for filing.

8. Explain Audit Risk, and its relation to risk of Material Misstatement (RMM) and Detection Risk (DR)?

Answer :

AR is the risk that the auditor may unknowingly fail to modify appropriately the opinion on materially misstated financial statements. The auditor should plan the audit so that overall audit risk is limited to a low level. AR includes:

A. Risk of Material Misstatement (RMM) The risk that the financial statements are materially misstated.

B. Detection Risk (DR)

The risk that the auditor will not detect a material misstatement that exists in an assertion. DR relates to the auditor's procedures.

- The auditor can change this risk by varying the nature, extent, or timing of audit procedures.
- As the acceptable level of DR decreases, the assurance provided from substantive tests should increase.

$$\text{AR} = \text{RMM (assessed by auditor)} \times \text{DR (controlled by auditor)}$$

SA 315 of ICAI defines the term Significant risk in the context of auditing as – An identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration.

Question :

After making a preliminary assessment of the risk of material misstatement during planning and beginning to apply audit procedures, an auditor determines that this risk is actually higher than anticipated. Which would be the most likely effect of this finding on the auditor's desired level of detection risk and the overall level of audit risk, as compared to the levels originally planned?

	Auditor's Desired Level of Detection Risk	Overall Level of Audit Risk
1.	Decrease	Same
2.	Increase	Same
3.	Same	Higher
4.	Decrease	lower

Answer :

Choice "1" is correct.

The auditor would initially have planned the audit to achieve a low level of audit risk. If the risk of material misstatement increased, the auditor would need to reduce detection risk to achieve the same low level of audit risk as initially planned.

Choice "2" is incorrect. The increase in the risk of material misstatement results in an increase in overall audit risk. Increasing detection risk would only exacerbate this problem by increasing audit risk even further.

Choice "3" is incorrect. If the auditor does not modify the desired level of detection risk, it is true that the overall level of audit risk will increase, but this is not the most likely situation. An auditor who discovers a higher risk than initially anticipated would need to develop an appropriate response to offset this increase in risk, so that an overall low level of audit risk could still be attained.

Choice "4" is incorrect. Assuming that the auditor had already planned the audit to achieve an appropriately low level of audit risk, the auditor would most likely revise audit procedures in an attempt to achieve the same low level of audit risk as initially planned. Although it is possible that the auditor would reduce detection risk enough to actually lower overall audit risk, this is not the most likely response to the scenario described.

Question :

As the acceptable level of detection risk increases, an auditor may:

1. Change the nature of substantive tests from a less effective to a more effective procedure.
2. Postpone the planned timing of substantive tests from interim dates to year-end.
3. Lower the assessed level of inherent risk.
4. Select a smaller sample size.

Answer :

Choose "4" is correct.

As the acceptable level of detection risk increases, the assurance that must be provided by substantive tests can decrease. Therefore, the auditor may reduce the sample size.

Choice "1" is incorrect. As the acceptable level of detection risk increases, the level of assurance required from substantive tests decreases. Changing the nature of substantive tests from a less effective to a more effective procedure provides more assurance and is more likely to result from a decrease (not increase) in detection risk.

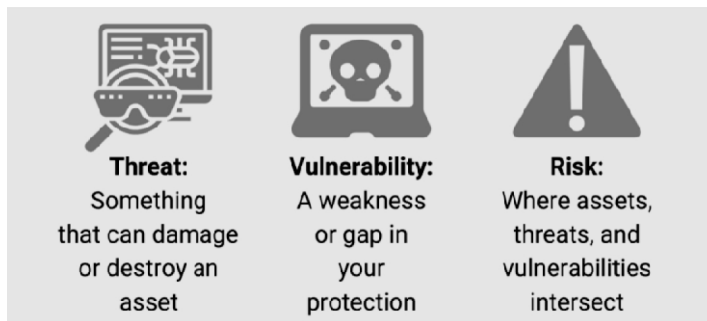
Choice "2" is incorrect. As the acceptable level of detection risk increases, the assurance that must be provided by substantive tests can decrease. Changing the timing of substantive tests from interim to year-end provides more assurance and is more likely to result from a decrease (not increase) in detection risk.

Choice "3" is incorrect. Although inherent risk affects the level of detection risk, detection risk does not affect the level of inherent risk. Inherent risk exists independently of the audit.

9. What is the difference between threat, vulnerability and risk?

Answer :

Risk itself is a function of threats taking advantage of vulnerabilities to steal or damage assets.



$$R = T \times V$$



10. What is the difference between peril, hazard and risk?

Answer :

- **Peril:** Cause of loss.
- **Risk:** Uncertainty arising from the possible occurrence of given events that would result in loss with no opportunity for gain.
- **Hazard:** Condition that increases the probability of loss. Thus, hazards increase the risk of a specific peril.

11. Pure (Hazard or Absolute) risk and Speculative (Opportunity) risk- Paul Hopkins

Pure Risks are associated with uncertainties which may cause loss. In a pure risk situation, a loss occurs or no loss occurs – there is no possibility for gain. These uncertainties may be due to perils such as fire, floods, etc. or may arise from human action such as theft, accident etc.

Types of Pure Risk

- **Personal risks** - It includes early death, sudden accident and disability, unemployment, etc.
- **Property risks** - reduction in value of assets due to physical damage, fire, theft, etc.
- **Liability Risks** - the risk of legal liability for damages accruing to customer, suppliers, vendors, etc. Such risks are also connected with compensation payable to employees for injuries and other harm afflicted in the workplace.

Above situations all come under the category of pure risks and are insurable.

Speculative (Opportunity) Risks have three possible outcomes: loss, no loss or gain. These risks arise from a conscious decision i.e., these are taken deliberately to make a gain knowing fully well that there can be loss. Examples of such risks include the decision to invest in some shares etc. The statistical techniques used in insurance cannot be applied to speculative risks. Further, these risks are deliberately taken with the hope of gain.

12. Difference between Fundamental Risk and Particular Risk ?

Answer :

Fundamental Risk. Exposure to loss from a situation affecting a large group of people or firms, and caused by (a) natural phenomenon such as earthquake, flood, hurricane, or (b) social phenomenon, such as inflation, unemployment, war. Fundamental risks may or may not be insurable.

A **particular risk** is a risk that affects only an individual and not everybody in the community. The incidence of a **particular risk** falls on the **particular** individual affected. **Particular risk** has its origin in individual events and its impact is localized (felt locally). These risks are insurable with conditions.

13. Difference between Static Risk and Dynamic Risk?

Answer :

Risks which occur even with no changes in the economy are classified as **Static Risks**. These include losses due to perils like fire, theft and dishonesty of individuals. These are insurable.

Dynamic Risks may arise due to changes in the economy like fluctuations in price levels, consumer references, distribution of income, product development, shifts in technology, etc. These are called Dynamic Risks. As they are less predictable, generally, they are not insurable.

14. What is the right way to classify risk?

Answer :

It may be noted that there is no 'right' or 'wrong' classification of risks. Risks can be grouped according to their nature, estimated cost or likely impact, likelihood of occurrence, countermeasures required, etc.

For example, Credit risk, is classified according to the likelihood of the collection of accounts receivable.

The most important issue is that an organization adopts the risk classification system that is most suitable for its own circumstances.

INTRODUCTION TO RISK

Part 1 :
Introduction

Part 2 :
Risk and
Uncertainty

Part 3 :
Classification of
Risk

Part 4 :
Dynamic Nature
of Risk

Part 5 :
Types of Risk

The discussion on part 2,3 and 4 is direct - that is first complete them.

Part 2 : Risk and uncertainty

A. Frank Knight

Uncertainty cannot be measure while risk can be measured

B. Douglas Hubbard

Uncertainty : The lack of complete certainty, that is, the existence of more than one possibility. The "true" outcome/state/result/value is not known.

Measurement of uncertainty: A set of probabilities assigned to a set of possibilities.

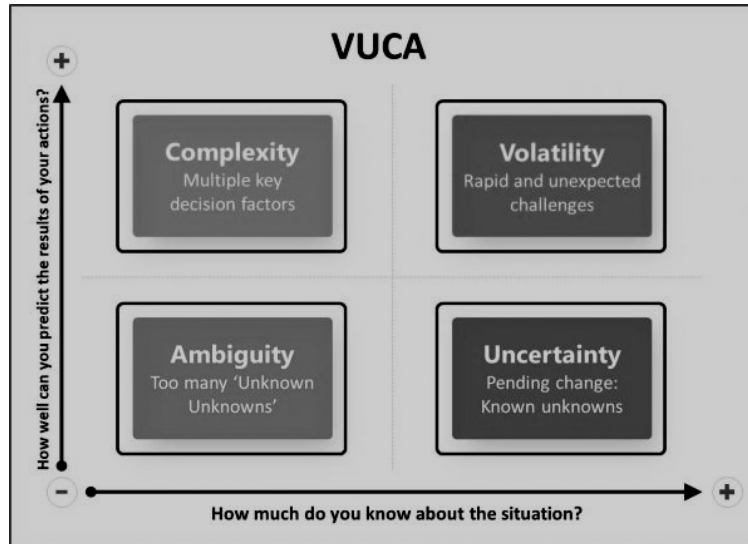
Uncertainty Table	
Probability	Outcome
0.2	-40
0.3	20
0.5	70

Risk: A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome. Thus in the table above the -40 scenario represents risk.

In this sense, one may have uncertainty without risk but not risk without uncertainty.

C. Our view : Risk refers to uncertainty that matters. Thus all risks are uncertainty but all uncertainties are not risk.

Note : The author has then shared the challenges of operating in the "VUCA" world



A detailed description is captured in the diagram below :

+ HOW WELL CAN YOU PREDICT THE RESULTS OF YOUR ACTIONS? -	<h2>complexity</h2> <p>Characteristics: The situation has many interconnected parts and variables. Some information is available or can be predicted, but the volume or nature of it can be overwhelming to process.</p> <p>Example: You are doing business in many countries, all with unique regulatory environments, tariffs, and cultural values.</p> <p>Approach: Restructure, bring on or develop specialists, and build up resources adequate to address the complexity.</p>	<h2>volatility</h2> <p>Characteristics: The challenge is unexpected or unstable and may be of unknown duration, but it's not necessarily hard to understand; knowledge about it is often available.</p> <p>Example: Prices fluctuate after a natural disaster takes a supplier off-line.</p> <p>Approach: Build in slack and devote resources to preparedness—for instance, stockpile inventory or overbuy talent. These steps are typically expensive; your investment should match the risk.</p>
	<h2>ambiguity</h2> <p>Characteristics: Causal relationships are completely unclear. No precedents exist; you face "unknown unknowns."</p> <p>Example: You decide to move into immature or emerging markets or to launch products outside your core competencies.</p> <p>Approach: Experiment. Understanding cause and effect requires generating hypotheses and testing them. Design your experiments so that lessons learned can be broadly applied.</p>	<h2>uncertainty</h2> <p>Characteristics: Despite a lack of other information, the event's basic cause and effect are known. Change is possible but not a given.</p> <p>Example: A competitor's pending product launch muddies the future of the business and the market.</p> <p>Approach: Invest in information—collect, interpret, and share it. This works best in conjunction with structural changes, such as adding information analysis networks, that can reduce ongoing uncertainty.</p>
	- HOW MUCH DO YOU KNOW ABOUT THE SITUATION? +	

Part 3 : Classification of risk

This involves risk classification according to Paul Hopkins. He classified risk into 3 categories :

- Hazard (or pure) risks : **Covered in Helicopter View**
- Control (or uncertainty) risks are associated with unknown and unexpected events. They are sometimes referred to as uncertainty risks and they can be extremely difficult to quantify. Control risks are often associated with project management. In these circumstances, it is known that the events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on minimizing the potential consequences of these events.
- Opportunity (or speculative) risks : **Covered in Helicopter View**

The section then talks about **Fundamental and Particular Risk - All Covered in Helicopter View.**

Part 4 : Dynamic nature of risk

Risk Management is a proactive, continuous and dynamic exercise. The firm and its environment keeps on changing. We have to keep on monitoring the same.

The author then describes **Static Risk (Environment stable)** and **Dynamic Risk (Unstable Environment) - Covered in Helicopter View.**

Part 1 : Introduction to Risk

There is extensive over here starting with definition of risk by various organisations and also involving classification and privatisation of risk.

A. Origin of the word "Risk" :

- Italia word "risco" which means danger
- "risicare" which means "to dare"
- French word "risque"

B. Risk : both upside as well as downside - both opportunity and threat - firm should take the right kinds of risk in the right proportion - reference to risk appetite.

Note : Page 1.2 of ICAI mat. gives an examples of a subcontract situations where a threat is converted into an opportunity.

C. Risk = Probability of occurrence × Financial impact of such occurrence

This is captured by both ICAI guide on RBIA and Open Group Standard.

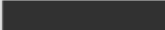
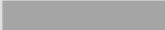

Open Group Standard.

Corporate Risk Impact Assessment					
Effect	Frequency				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

LEGEND	
E - Extremely high risk	The transformation effort will most likely fail with severe consequences.
H - High risk	Significant failure of parts of the transformation effort resulting in certain goals not being achieved.
M - Moderate risk	Noticeable failure of parts of the transformation effort threatening the success of certain goals
L - Low risk	Certain goals will not be wholly successful.

ICAI guide on RBIA

Measurement Yardstick for Risk Score					
Likelihood of Risk	Consequences of Risk				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	5 x 1 = 5	5 x 2 = 10	5 x 3 = 15	5 x 4 = 20	5 x 5 = 25
Almost Certain (4)	4 x 1 = 4	4 x 2 = 8	4 x 3 = 12	4 x 4 = 16	4 x 5 = 20
Almost Certain (3)	3 x 1 = 3	3 x 2 = 6	3 x 3 = 9	3 x 4 = 12	3 x 5 = 15
Almost Certain (2)	2 x 1 = 2	2 x 2 = 4	2 x 3 = 6	2 x 4 = 8	2 x 5 = 10
Almost Certain (1)	1 x 1 = 1	1 x 2 = 2	1 x 3 = 3	1 x 4 = 4	1 x 5 = 5

LEGEND	
	Risks which require immediate attention
	Risks which should be monitored and brought down to green
	Risks which do not require action

D. All definitions of risk carry the basic theme that risk has two elements:

- Uncertainty
- Effect on objectives

E. ISO 31000 Definition of risk : Done

F. ICAI SA 315

- **Defines ERM and states that as per ERM, there are four kinds of risks -**
 - Strategic
 - Operational
 - Financial
 - Knowledge
- **Defines business risk and classifies business risk as -**
 - Internal
 - External
 - Controllable
 - Uncontrollable
- **Significant Risk and Audit Risk - Done in Helicopter View**

G. ICAI RBIA

- Lays stress on importance of objectives while defining risk
- **Larger focus** - risk is **T** as well as **O**
- **Narrow focus** - risk is only **T**
- Stresses on stake holders value maximisations
- without proper risk management, firm displaying "**Frog in the well**" syndrome
- **Risk = Frequency × Impact - Risk scoring system - Done above**

H. Oxford English Dictionary : Definition of risk - same stuff i.e., uncertainty that matters.

I. Basel II norms : Definition of Operational risk

J. Risk classifications by COSO : ORC - this stands for Operational Risk, Financial Reporting Risk and Compliance Risk

K. Occupational Health and safety advisory services (OHSAS)

- Defines risk = probability × severity
- Risk in information security - Threat × Vulnerability
- Economic Risk
- Cyber Risk
- Environmental Risk like Chemical Risk
- Cognitive ability
- Emotional Intelligence

L. Risk in an organisational context

Illustrative Corporate Risks

Corporate Functions	Risk Areas
Human Resources	Poor morale & talent retention
Sales & Marketing	Poor Customer loyalty & retention
Operations	Inability to Digitize/ automate processes
Treasury	Low return on investments
Information Technology	Hacking and unauthorized access
New Product development	Product failure
Treasury	Mismatch in cash flows
Finance & Accounts	Unreliable financial statements

M. Financial Risk

- **NASDAQ Definition** : Cash flow inadequacy
- Risk due to financial leverage (use of debt)
- Volatility of investment returns
- **Real time risk** : Algo trading and the 2012 flash crash

N. Inherent and Residual Risk : **Done in Helicopter View.**