FUNDAMENTALS OF RISK MANAGEMENT

DR. NEENA P.C
MANJULA JAIN

ALEXIS PRESS
JERSEY CITY, USA

FUNDAMENTALS OF RISK MANAGEMENT

FUNDAMENTALS OF RISK MANAGEMENT

Dr. Neena P.C

Manjula Jain

ALEXIS PRESS

ALEXIS PRESS

Published by: Alexis Press, LLC, Jersey City, USA
www.alexispress.us

First Published 2022

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Includes bibliographical references and index.

Fundamentals of Risk Management by *Dr. Neena P.C, Manjula Jain*

ISBN 978-1-64532-356-3

CONTENTS

CHAPTER 1

RISK MANAGEMENT OVERVIEW AND RISK DEFINITION METHODS

Dr Neena P.C, Associate Professor, Department of OB & HR,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email id-dr.neenapc@cms.ac.in

ABSTRACT:

Any company must identify, evaluate, and prioritize possible risks that might have an influence on its goals via the process of risk management. It is the process of assessing the potential harm from unpredictable occurrences and adopting proactive measures to lessen their possibility and effects. The basics of risk management are covered in the introduction, including its definition, significance, and advantages. Depending on the organization's viewpoint and situation, several risk definition strategies are used. The subjective method focuses on stakeholders' opinions and attitudes toward the possibility and repercussions of the occurrence, while the objective approach defines risk as the probability and severity of an event happening. While the quantitative method makes use of statistical analysis and modeling to evaluate the possibility and effect of risks, the qualitative approach relies on expert opinion and experience to identify and prioritize risks. In the end, the strategy chosen will rely on the objectives, available funds, and risk appetite of the company. It is crucial to comprehend the various methods of defining risk in order to create effective risk management plans and boost organizational resilience.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management.

INTRODUCTION

Risk in this sense relates to bad results and is described by the Oxford English Dictionary as "a chance or possibility of danger, loss, injury, or other adverse consequences," while at risk is defined as "exposed to danger." However, taking a gamble might also be beneficial. The third concept is the link between risk and outcome uncertainty. Consider owning a car as an example. The majority of people see owning a car as an opportunity to benefit from increased mobility. Owning a car does come with certain unknowns, especially in terms of maintenance and repair costs. Last but not least, accidents involving cars undoubtedly have a negative effect. It's important to be aware of the legal obligations that come with owning a car, as well as the rules that must be adhered to while the car is being driven on a public road.

There are many sites to get definitions of risk; some significant definitions are offered below. A alternative definition is also provided to emphasize the vast variety of risks that might affect businesses. The Institute of Risk Management (IRM) defines risk as the outcome of an event's probability and effects. Consequences might be either positive or negative. This definition is practical and easy to use, with a wide variety of applications. In the ISO Guide, a comprehensive reference for risk-related topics, risk is described as "the effect of uncertainty on objectives." This phrase is challenging to put into practice, and it seems to call for some level of risk

management skill. The importance and use of this phrase will become clearer as the reader proceeds through this book.

The Guide has previously mentioned the likelihood of a positive, unfavorable, or unexpected result. Owning a car served as an example in the previous section to show how these three types of events may be linked to risks as an opportunity, hazard, or uncertainty. The book makes the argument that risk is often defined in terms of occurrences, changes in circumstances, consequences, or a combination of these, and how they could affect achieving objectives. The Institute of Internal Auditors (IIA) defines risk as the unpredictability around the occurrence of an event that might have an impact on the achievement of objectives. The IIA further notes that risk is calculated using probability and consequences. Across fields, the definition of "risk" varies greatly. Health and safety specialists define risk as a combination of chance and scale, albeit this definition may not be sufficient for more ambitious risk management objectives. Given that the word "risk" has several interpretations, it is imperative that the corporation choose the one that best advances its own goals. The group may use a definition that is either narrow or wide. The following is the author's succinct definition of the word risk:

Risk in an organizational setting is often defined as anything that might prevent the attainment of business objectives. It is an event that has the potential to hinder, improve, or raise questions about the effectiveness and efficiency of an organization's core functions. However, the majority of businesses often fail to express their company objectives clearly. When objectives are defined, they are often presented as annual objectives for internal reform. This is particularly true of the personal objectives that the firm sets for its personnel, since these objectives often refer to advances or change rather than continuous or routine corporate operations. Effect of uncertainty on objectives. Be mindful that an influence can be different from what was expected or it might be either positive or bad. In addition, a situation, a change in the environment, or an outcome are often used to describe risk.

It is generally agreed that emphasizing hazards as occurrences, as in the definitions of risk provided by ISO and the Institute of Internal Auditors, is the best method to define risk. A threat cannot materialize without a triggering event. The risk management method is likely to become clearer if the focus is placed on occurrences, which is perhaps the simplest definition of a risk: "an unplanned event with unexpected consequences." Consider the potential obstacles to, say, a theatrical performance. Among the situations that might cause disruption include power failures, the absence of a prominent performer, significant transportation issues or road closures that delay audience arrival, as well as a significant staff illness. After identifying the possible performance-disturbing occurrences, the theater's management must decide what to do to reduce the risk that one of them will force the cancellation of a performance. Risk management is being used in this theater's administration's investigation. Risk may produce either positive or negative outcomes, or it might just provide uncertainty. Consequently, risks may be seen to be associated with a chance, a loss, or the presence of uncertainty for a firm. Every threat has distinctive characteristics that need specialist management or inquiry. In this book, risks are divided into four groups:

1. Risks related to required compliance.

2. Pure risks, or risky risks.
3. Risks that can be managed or uncertainty.
4. Speculative risks or chance hazards.

Organizations will often work to minimize opportunity risks, control risk management issues, and compliance risks. It's critical to keep in mind that there is no "correct" or "wrong" approach to allocate risks. Other subcategories that readers could encounter in other works of literature might be as pertinent. Risks are often split into two groups: pure risks and speculative risks. The terminology employed in risk management is, in fact, the subject of many debates. Despite theoretical disagreements, it is imperative that a company choose the risk categorization system that is most suitable for its unique set of circumstances [1].

There are some dangerous circumstances that can only go wrong. These risks, also known as hazard risks or pure risks, may be classified as operational or insurable risks. Hazard risk tolerance varies by company, therefore these risks must be managed within organizationally acceptable bounds. Theft is a prime example of a risk concern that many businesses deal with. Different threats make it difficult to predict how a situation will play out. These are referred to as control risks and are often involved in project management. Organizations often detest taking calculated risks. There may be doubts about the benefits the project offers as well as whether it will be completed on time, on budget, and in accordance with the project's requirements. The management of control risks is often employed to ensure that the outcomes of business activities fall within the desired range. Lessening the gap between anticipated and actual outcomes is the goal.

DISCUSSION

Companies also actively take risks to make a profit, especially those associated with the market or the economy. A corporation will have a certain propensity for taking such risks, and these risks might be classed as speculative or opportunity risks. Opportunity risks have to deal with the relationship between risk and return. The idea is to take a risk in order to get something. Chance risks will be focused on investment. The application of risk management techniques and methods to the management of hazard risks is the best and most well-known area of risk management, and this paper will place a strong emphasis on hazard risks. A hierarchy of controls that apply to hazard hazards is discussed in Paper. Hazard risks are linked to a potential source of harm or a situation that might have a negative impact on objectives, and hazard risk management aims to reduce the potential impact. Hazard risks are the most common dangers associated with operational risk management, including workplace health and safety initiatives.

Control risks are related to unanticipated and unknown events. They may be difficult to measure and are sometimes referred to as uncertainty risks. Project management and the deployment of methods are often associated with risk management. It is evident in certain circumstances that certain things will occur, but it is hard to predict or control precisely where those events will lead. The approach is thus based on limiting the potential consequences and repercussions of these events. Opportunity risks may be separated into two groups. While there are dangers and risks associated with seizing an opportunity, there are also dangers associated with passing it up.

Opportunity risks may sometimes be of a financial nature and may not be immediately apparent. Even when opportunity risks are taken in the hopes of achieving positive outcomes, there is no guarantee of success. However, the essential plan of action is to take advantage of the opportunity and any associated risks. Relocating to a new location, purchasing new property, expanding, and diversifying into new products all provide potential risks for small businesses.

Information about Risks

A risk must be fully understood in order for ownership and duties to be acknowledged and for a common understanding of the risk to be developed. The range of information that must be recorded in order to fully understand a threat. Since the information list presently only refers to hazard issues, it will need to be revised to properly address control or opportunity risks. It is critical to comprehend the distinctions between compliance, hazard, control, and opportunity risks in order to collect the right quantity of information about each risk. The example below aims to demonstrate the distinctions between these four risk categories so that the precise information required to define each category may be determined.

Inherent Level of Risk

Understanding the entire scope of each and every threat mentioned is essential. This is the level of risk before any actions are taken to change the likelihood or severity of the hazard. Knowing the level of risk that is there has advantages, but some threats make it hard to do so in real life. Identifying the underlying level of risk might help assess how important the control mechanisms that have been put in place are. The IIA has always upheld the view that assessing the inherent degree of risk should come first in the analysis of all risks. The goal of any risk assessment remains the same, regardless of the controversy surrounding whether to conduct them at an inherent or current level, in accordance with previous guidance from the IIA: "in the risk assessment, we look at the inherent risks before considering any controls." Its objective is to ascertain what is believed to be the current level of risk and to list the major safeguards in place to ensure that it is actually maintained.

To show the underlying risk level in terms of likelihood and magnitude, a risk matrix is often utilized. The risk's residual or current level may then be established once the control or controls have been put into place. The effort required to reduce the risk from its inherent level to its current level may be clearly shown in the risk matrix. Depending on the situation, the inherent risk may also be referred to as the absolute risk or gross risk. Other names for the current level of risk include the residual level, net level, and managed level of risk. The example in the box below demonstrates how the adoption of acceptable and practical risk response options may reduce the risk involved in activities that are high-risk by definition [2].

Techniques for Categorizing Hazards

Risks may be grouped according to their attributes, such as their projected duration of effect, the kind of impact they will have, and/or their estimated magnitude. They might also be categorized according to how long after an event they have an impact. The risk's origin may also be taken into consideration while categorizing. In this case, a risk may be classified according to its

source, such as counterparty risk or credit risk. Consider the kind of the impact when further classifying dangers. While certain hazards may negatively impact the organization's financial situation, others may negatively impact its day-to-day operations or physical infrastructure. In addition, risks may have an impact on the company's reputation, position, and market status and image.

The part or feature of the organization that might be affected can also be used to classify risks. Examples include categorizing dangers according to how they will affect people, places, objects, processes, or things. When picking their risk categorization system, organizations must decide whether the risks will be classified according to the source of the risk, the component impacted, or the consequences of the risk materializing. Each firm will choose the risk categorization system that is most suited to their operations and kind of business. Furthermore, several risk management frameworks and standards advocate the use of a particular method for categorizing hazards. The organization will probably follow the advised classification structure if it adopts one of these standards. The method of risk classification used must be utterly suitable for the firm in issue. Every business has different demands, thus no one classification system can satisfy them all. It is likely that categorizing each risk in a variety of ways will be essential in order to properly understand the potential effects. Many classification systems do, however, provide uniform or equivalent structures [3].

The Likelihood and Magnitude of the Danger

A risk matrix is the simplest approach to show the likelihood and size of a danger. Different methods may be used to create risk matrices. Regardless of its layout, a risk matrix is a very helpful tool for risk management professionals. The basic risk matrix contrasts the likelihood of an event occurring with its potential magnitude or impact. a simple risk matrix illustration, sometimes called a risk map or heat map. This method is often used to illustrate risk likelihood and the magnitude or severity of the occurrence, should the risk materialize. Using the risk matrix to display risk probability and magnitude is a significant risk management tool. The company may use the risk matrix to show the nature of each individual risk in order to decide whether or not it is acceptable and falls within the scope of the business's risk appetite and/or risk capacity. Throughout the whole book, a standardized method for presenting a risk matrix has been adopted. Indicated on the horizontal axis is probability. The risk matrix measures how often certain events occur, although the word frequency implies that they will surely happen. For this reason, probability is used instead of frequency. The notion of "likelihood" is more expansive and includes frequency and the possibility that an unexpected event will really happen. However, risk management literature often uses the word "probability" to convey the likelihood that a risk will manifest [4],[5].

The vertical axis displays the magnitude. The phrase size rather than severity is used to represent compliance, hazard, control, and opportunity risks utilizing the same kind of risk matrix. The intensity of the occurrence implies that it was negative, and that it was related to compliance and hazard problems. The risk's gross or inherent level may be interpreted as a measure of its magnitude prior to the implementation of controls. However, rather than the scale of the event, risk managers should focus more on the impact of the incident and the outcomes that follow. For

instance, a large fire may start and completely demolish the facilities of a distribution and logistics company. If the organization has appropriate insurance, the financial cost to the business may be modest, and if the company has made strategies to cope with such an event, the consequences on the entire operation may be considerably less than would otherwise be expected, despite the possibility that the event may be of a sizeable scale. The scale of an event may be thought of as its inherent level, and its influence as its risk-managed level. Since an event's impact (and the consequences it creates) are often more important than its size (or severity), every risk matrix used in the next papers of this book will display effect vs probability rather than magnitude against likelihood[6]–[8].

CONCLUSION

In conclusion, the overview and risk definition methods are important tools for understanding and managing risks in various fields, including biotechnology, environmental sustainability, and public health. These methods provide a structured approach to identify, assess, and mitigate risks associated with complex systems and processes. The use of overview and risk definition methods can help to identify potential hazards and risks associated with new technologies, products, or processes, allowing for timely risk mitigation measures to be put in place. It also enables stakeholders to make informed decisions based on a comprehensive understanding of the risks and benefits associated with a particular course of action.

However, it is important to recognize that the use of overview and risk definition methods is not without limitations. These methods rely on assumptions and data that may be incomplete or uncertain, and may not account for complex interrelationships between different factors and variables. Therefore, it is important to ensure that overview and risk definition methods are used in conjunction with other tools and approaches, such as stakeholder engagement, scientific research, and expert opinion. This will ensure that the results obtained from these methods are robust, reliable, and relevant for decision-making. Overall, the use of overview and risk definition methods is an important step towards ensuring the safe and responsible use of new technologies, products, and processes. By identifying and managing risks, we can promote sustainable development and protect public health and the environment, while also promoting the advancement of science and technology.

REFERENCES:

[1] G. Pascarella *et al.*, “Risk analysis in healthcare organizations: Methodological framework and critical variables,” *Risk Manag. Healthc. Policy*, 2021, doi: 10.2147/RMHP.S309098.

[2] C. Eckert, “Corporate reputation and reputation risk,” *J. Risk Financ.*, 2017, doi: 10.1108/jrf-06-2016-0075.

[3] M. Nemeth, C. Miller, and A. Bräuer, “Perioperative hypothermia in children,” *International Journal of Environmental Research and Public Health*. 2021. doi: 10.3390/ijerph18147541.

[4] M. Wiedenmann and A. Größler, “Supply risk identification in manufacturing supply networks,” *Int. J. Logist. Manag.*, 2020, doi: 10.1108/IJLM-02-2020-0081.

[5] R. Aicale, D. Tarantino, and N. Maffulli, "Overuse injuries in sport: A comprehensive overview," *Journal of Orthopaedic Surgery and Research*. 2018. doi: 10.1186/s13018-018-1017-5.

[6] M. Leo, S. Sharma, and K. Maddulety, "Machine learning in banking risk management: A literature review," *Risks*, 2019, doi: 10.3390/risks7010029.

[7] M. Suprin *et al.*, "Quality Risk Management Framework: Guidance for Successful Implementation of Risk Management in Clinical Development," *Ther. Innov. Regul. Sci.*, 2019, doi: 10.1177/2168479018817752.

[8] H. Jankensgård, "A theory of enterprise risk management," *Corp. Gov.*, 2019, doi: 10.1108/CG-02-2018-0092.

CHAPTER 2

IMPACT OF RISK ON ORGANIZATIONS

Dr.Anantha Subramanya Iyer, Associate Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- asi@cms.ac.in

ABSTRACT:

Organizations are significantly impacted by risk because it may impair their capacity to meet goals and maintain competitiveness. Organizations may experience short-term or long-term effects from risk, which may have direct or indirect effects. Financial loss is one of the most severe effects of risk and may be brought on by a variety of circumstances, including market swings, fraud, cyberattacks, natural catastrophes, and legal liability. Financial loss may result in decreased profitability, a decline in investor confidence, and reputational harm. Operational disruption, which may result from system failures, supply chain interruptions, or staff misbehavior, is another effect of risk on firms. Missed deadlines, lower productivity, and reputational harm may all result from operational instability.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

Strategy, since better strategic judgments will be made after a thorough analysis of the risks involved with various strategic possibilities. Tactics, as the choice of the tactics and the hazards associated with any potential alternatives will have been taken into account. Operations will be less likely to be disrupted by occurrences since they will be detected in advance, and measures will be taken to minimize the damage they may do and keep their cost under control. The risks of failing to comply with statutory and customer responsibilities will be acknowledged, which will improve compliance. Following the events in the global financial system during, risk and risk management are now more important to all enterprises. It is becoming clearer that managing risks explicitly and systematically has advantages[1]. The following four areas of improvement may be attained by firms by adopting a proactive approach to risk and risk management:

It is no longer acceptable for enterprises to be in a situation where unforeseen occurrences result in financial loss, interruption of routine business operations, reputational harm, and loss of market presence. Stakeholders increasingly anticipate that businesses will fully account for the risks that might result in business interruption, project delays, or strategy failure. An individual risk's exposure may be described in terms of the possibility of the risk occurring and the effect of the risk if it does. The likelihood of an effect will rise along with the level of risk exposure. This assessment of probability and effect is referred to by Guide as the present or 'level of risk'. This amount of risk should be compared to the organization's risk tolerance and attitude toward that kind of risk. A collection of risk criteria may be used to characterize the risk appetite.

The word "magnitude" is used often in this text to describe the enormity of an event that has happened or might happen. 'Influence' refers to how an incident has an influence on an

organization's resources, operations, standing, and/or marketplace (FIRM). This phrase is congruent with how impact is used in assessments of business continuity plans. This is a measurement of risk at the present time. In this book, the word "consequences" refers to the degree to which an incident hinders the achievement of effective and efficient strategy, tactics, operations, and compliance (STOC).

Effects of Risky Situations

Hazardous risks defeat goals, and the severity of such risks is a gauge of their importance. The management of hazard hazards has the oldest history and the most fundamental roots in risk management. The management of insurable risks and hazard risk management are closely connected. Keep in mind that a risk (or pure risk) may only result in harm. Hazard risk management addresses problems including workplace health and safety, preventing fires, avoiding property damage, and dealing with the effects of faulty goods. Hazard risks may interfere with daily operations and result in higher expenses and negative PR from disruptive incidents [2]. Risks associated with hazards are connected to company dependencies, such as IT and other auxiliary services. Most firms are becoming more and more reliant on their IT infrastructure, and IT systems are susceptible to disruption from computer failure, server room fires, virus infections, and malicious hacking or computer assaults. For many firms, theft and fraud may also pose serious risk factors. This is particularly true for businesses that deal with cash or oversee a large volume of financial transactions. Adequate security protocols, the separation of financial responsibilities, authorization and delegation processes, as well as the pre-employment screening of workers, are all significant prevention methods for theft and fraud.

It is important to consider language since, should an occurrence occur, this is crucial in connection to hazards and dangers. If a danger of hazard materializes, it might have a very significant impact, such destroying an organization's primary distribution center. The company will be affected by this major event in terms of possible financial losses, infrastructure damage, reputational harm, and the incapacity to operate in the market. The risk's gross or inherent level is represented by its magnitude. The restrictions that are in place, however, will lessen the effect of the occurrence. Impact is a measure of the risk's net, remaining, or current level. These measures lessen the financial effect, the degree of infrastructure devastation, as well as safeguards intended to safeguard brand image and business operations. However, the organization must also consider the effects of the significant warehouse fire. These effects pertain to how the fire may affect the organization's strategy, tactics, operations, and compliance initiatives [3].

DISCUSSION

A large-scale catastrophe of this nature may not have much of an effect on the organization's finances if it results in a huge financial loss that is insured. The effects of this huge fire from the perspective of the customers will be so well controlled that consumers need not be aware that a significant fire has occurred thanks to effective crisis management and business continuity. Finally, it is important to recognize the significance of compliance concerns. For many firms, particularly those operating in tightly regulated business areas, compliance risks may be

significant. The achievement of the level of compliance activities required by the relevant regulator can have a significant impact on the reputation of the organization and substantial consequences for routine business activities. In some cases, compliance with mandatory requirements represents a "licence to operate."

The Inclusion of Hazards

Despite the fact that the majority of common definitions of risk state that hazards are related to company goals. The graphic depicts risks as having the potential to affect the crucial dependencies that support the organization's central operations. The fundamental organizational processes are defined in part by corporate goals and stakeholder expectations. These essential processes, which might relate to operations, tactics, corporate strategy, as well as compliance activities, are important elements of the current nature and future development of the business model and are further discussed in Paper [4].

The purpose of is to show that aspects of an organization other than corporate goals may carry considerable dangers. The organization's primary dependencies, corporate goals, stakeholder expectations, and a review of its basic business processes may all be used to identify significant risks. For instance, Northern Rock failed as a result of the collapse of the bank's dependent wholesale money markets. Consider the characteristics as alternative beginning points for doing a risk assessment as another approach to look at the idea of attached hazards. For instance, a risk assessment may be done by determining what stakeholders anticipate from us.", as well as "what dangers can jeopardize meeting those stakeholder expectations?" Banks and other financial institutions created operational and strategic goals in the run-up to the current financial crisis. Risk management had a role in the accomplishment of the high-risk goals that eventually contributed to the downfall of the businesses by examining these objectives and identifying the risks that may hinder their success. This example shows that it is not only conceivable but also maybe desirable in certain situations to associate risks with characteristics other than aims. It is undeniably true that danger is higher when conditions are changing. Therefore, it is not irrational to associate risks to change goals, but analyzing each target separately may not result in reliable risk awareness or identification. In any event, company goals are often expressed too broadly for effective risk attachment.

The corporate objectives should include a thorough description of the company's short-, medium-, and long-term goals in order to be helpful to the organization. Internal, yearly goals for change are often insufficient since they may not accurately reflect the organization's needs in terms of operations, efficiency, change, and leadership. The danger of ignoring the context in which hazards originated is the primary drawback of the "objectives-driven" approach to risk and risk management. Risks cannot be evaluated rigorously and intelligently if they are examined in a manner that is disconnected from the circumstances that gave rise to them. There is a case to be made for the 'dependencies-driven' approach to risk management in producing a more reliable analysis.As long as any advantages can be derived from this strategy, many firms will likely continue to employ an examination of corporate goals to spot hazards. Utilizing this "objectives-driven" approach, for instance, makes it easier to analyze risks in regard to the unpredictable and good parts of events that may occur, as well as the bad and compliance-related aspects. If the

business decides to link risks to its goals, it is crucial that these goals have undergone thorough and thorough development. The assumptions that support the goals should also be given great consideration and critical analysis in order to guarantee that they are comprehensive and complete [5].

The paper that discusses core processes may be thought of as the high-level procedures that power the organization. 'Delivering successful outcomes on the field' is one of the operational procedures in the example of a sports club. Along with being tied to goals and/or important dependencies, risks may also be associated to this fundamental process. The four categories of core processes are strategic, tactical, operational, and compliance (STOC). The fundamental procedures must always be successful and efficient. The efficacy and efficiency of key processes may then be improved via the creation of mature or sophisticated risk management activities. Although risks may be connected to other organizational components, the typical strategy is to link risks to company goals. One of the common definitions of risk is anything that has the potential to influence undermine, enhance, or raise doubts about the accomplishment of company goals. Although this definition is helpful, it does not provide the only place to look for major hazards.

Risks are increasingly being linked to important dependencies, particularly stakeholder expectations. In Paper, the significance of stakeholders and their expectations are covered in greater depth. The process of using key dependencies to find hazards may be simple. The organization has to determine what aspects or elements of the organization and its external environment are essential to success. As a consequence, the organization's strengths, weaknesses, opportunities, and dangers will be identified. This is often known as a SWOT analysis. Having determined the important dependencies, as shown in Table. the company may then think about the threats that might affect these dependencies. This strategy is covered in further depth with actual risk instances. Another characteristic of risk and risk management is that firms often incur risks in order to reap rewards. the connection between the degree of risk and the potential magnitude of profit. A company will introduce a new product because it thinks that good marketing will result in more profits. The company will risk resources when introducing a new product since it has determined that taking some risk is acceptable. The value at risk is a representation of the organization's risk tolerance in relation to the activity it is engaging.

When an organization takes this kind of risk, it should do so fully aware of the risk exposure and confident that the level of risk exposure is acceptable to the business. It should make sure it has the resources to cover the risk exposure, which is much more crucial. In other words, the organization's ability to tolerate any anticipated negative outcomes should be clearly stated, the degree of risk exposure should be assessed, and the desire to accept that level of risk should be affirmed. Not all commercial endeavors will provide the same return for the same degree of risk. Startup businesses often carry a high level of risk and may have poor initial projected returns. demonstrates the potential development of risk vs reward for a new business or product. As a start-up operation with a high risk and poor reward, the activity will start at the bottom right corner.

The firm will probably migrate to a better return for the same amount of risk as it grows. For the company or product, this is the period of growth. The payoff might stay high as the investment ages, but the hazards ought to go down. A company will eventually reach full maturity and migrate into the low-risk, low-return quadrant. In very developed marketplaces, it is typical to anticipate that an organization or product would see a decrease. Management or the organization itself will need to identify the specific dangers the company confronts. The risks that have been identified will then need to be managed properly using the appropriate procedures. Part Four of this book considers the nature of these risk reactions and the nature of their effect. Opportunity hazards are covered by the topic of risk and reward mentioned above. The work put into risk management must, however, always pay off. Less disruptive incidents are probably the result of greater risk management effort when it comes to hazard risks.

When it comes to project risks, putting more effort into risk management will pay off by increasing the likelihood that the project will be completed on schedule, on budget, and in accordance with specifications. The risk vs return analysis should lead to fewer failed new products and, at worst, a reduced degree of loss for all new activities or new products when it comes to opportunity hazards. Profit or a higher quality of service is always the payoff for taking a risk. More consideration is given to the idea of the risk versus return analysis in regard to strategic hazards. Different companies will approach risk in different ways. Some businesses can be categorized as risk averse, while others might be risk aggressive. The industry, the makeup and maturity of the market where the organization works, as well as the attitudes of the individual board members, will all have some bearing on how the business views risk [6].

Risks must be assessed in the context in which they first surfaced. When a board has determined that an opportunity should not be passed up, it may look that a company is taking excessive risks. The opportunity's significant risk component, however, may not have been completely taken into account. Making ensuring that strategic choices that seem high risk are really made with all of the information available is one of the primary contributions of effective risk management. One of the main advantages of risk management is an increase in the robustness of decision-making processes. The organization's risk appetite and attitude toward risk are closely linked but not the same concepts. Risk appetite and risk attitude both reflect how a company views risk over the long term and the near term, respectively. This is comparable to the distinction between a person's current hunger for food and their long-term or established attitude toward the food they consume.

The maturity cycle stage is one of the other important variables that will affect how the company views risk. A more proactive approach toward risk is needed for a start-up company than it is for one that is growing or one that is an established company in a well-established industry. In mature markets when a business is in decline, there will be a considerably more risk-averse attitude toward risk. It is commonly argued that some high-profile businesspeople are extremely effective at entrepreneurial start-up but are not as successful in managing established organizations since the attitude toward risk must alter whether a company is a start-up operation rather than a mature organization. At various stages of the company maturity cycle, different risk-taking mindsets are needed. A vote in favor of Britain's withdrawal from the European

Union (Brexit) was obtained in the June referendum in the UK on the future of EU membership. The process for the UK to exit the EU must be started by the UK government. The most often debated choices accessible to the UK government are outlined in the text box below. Overall, the UK government's task is to maintain the UK economy's prosperity based on a Brexit plan and other measures that will maintain the UK's resilience.

Norwegian Design

Norway does not belong to the EU but is a member of the European Economic Area. Although it must adhere to EU rules and regulations and is unable to impose immigration restrictions, it enjoys full access to the single market. Norway must also pay its share of the EU budget.

European Model

With considerable success, Switzerland has established a two-way relationship with the EU that effectively grants it access to some niche markets inside the continent in exchange for adhering to appropriate EU regulations and making financial commitments to the EU budget.

Canada's Design

The UK can try to imitate the kind of arrangement that Canada recently (in November) approved in their most comprehensive trade agreement ever with Europe. Financial services pass porting may not be permitted going forward under such an arrangement. All of these approaches have difficulty with the crucial problem of regulatory control. The UK now needs to assess how Brexit will affect business risks and opportunities using these three models as a foundation.

Risk is also referred to as result uncertainty. This term, although a little technical, is still helpful and is especially relevant to the management of control risks. The most challenging risks to recognize and quantify are control risks, which are often connected to projects. A project's overarching goal is to provide the required results on schedule, within budget, and in accordance with the project's specifications for quality or performance. For instance, it may not always be possible to accurately predict the nature of the ground conditions while a structure is being erected. More details on the nature of the circumstances will become accessible as the building work progresses. The fact that the earth is firmer than anticipated and less foundation work is needed may be good news. Alternately, it could be found that the earth is polluted, weaker than anticipated, or that there are other potentially harmful situations, such the discovery of ancient relics. Given this uncertainty, these risks need to be seen as control risks, and the project's overall management ought to take the uncertainty of these various risk categories into consideration. The project manager shouldn't expect that only negative features of the ground conditions would be found. In a similar vein, the project manager shouldn't assume that things will go better than anticipated simply because they should.

Because control risks introduce uncertainty, it's possible to assume that an organization will dislike them. The actual aversion could be to the eventual variability in results that would then need to be addressed. It is OK to deviate from the project schedule to some extent, but not too much. When it comes to managing risks, tolerance may be thought of as having the same meaning as when engineering components are manufactured; these components must have a

certain dimension while being within acceptable tolerance limits. The risk management process is continually being represented in new ways to make it more understandable for managers and other stakeholders involved in risk management operations. The bow-tie is one of the newly created tools for displaying risk management operations. This book makes frequent references to the bow-tie as a symbol for the risk management approach. a simple illustration of the bow tie that may be used to describe situations that could interfere with ongoing, effective operations [7].

Unexpected occurrences with the Bow Tie

The source of a certain danger is shown on the left side of the bow tie, which also shows the organization's categorization scheme for risk sources. These sources of risk are at a high level and include compliance, tactical, strategic, and operational hazards. The effect, should the risk occurrences materialize, is described on the bow tie's right side. uses the high-level elements of the effect of a risk materializing on the financial, infrastructure, reputation, and market (FIRM). The risk event is located in the center of the bow tie. The same categories of people, premises, processes, and products are employed here as well as the kinds of disruption that may impact enterprises. The bow-tie picture serves to illustrate the organization's risk categorization methods as well as the possible scope of repercussions in the event that a risk materializes. Vertical lines on the left side of the bow tie may be used to symbolize controls that can be put in place to stop the event from happening. On the right side of the bow-tie, recovery controls may be shown in a similar way [8].

CONCLUSION

Operational disruption, which may result from system failures, supply chain interruptions, or staff misbehavior, is another effect of risk on firms. Missed deadlines, lower productivity, and reputational harm may all result from operational instability. Additionally, risk may affect how well a company complies with legal duties and regulatory standards, which may subject it to financial penalties and other legal consequences. Regulation non-compliance may also harm an organization's brand and result in lost clients and investment. Overall, the influence of risk on companies emphasizes the need of putting into place efficient risk management systems to reduce possible adverse effects. Organizations may improve their capacity to accomplish their objectives and maintain market competitiveness by proactively recognizing, analyzing, and managing risks. The risk management process may be represented by a bow-tie in a variety of ways, including the depiction of opportunity hazards. The bow-tie may also be used to represent the many kinds of controls that are accessible to organizations; this is covered in further depth in the paper on loss control. Bow ties are now often used, particularly in the public sector. The example of using the bow-tie to identify preventative and response measures for a fire in a residential home's kitchen is shown in the box below.

REFERENCES:

[1] R. L. Kumar And S. Park, “A Portfolio Approach To Supply Chain Risk Management,” *Decis. Sci.*, 2019, Doi: 10.1111/Deci.12332.

[2] A. Wagner, R. Schaffert, And J. Dratva, "Adjusting Client-Level Risks Impacts On Home Care Organization Ranking," *Int. J. Environ. Res. Public Health*, 2021, Doi: 10.3390/Ijerph18115502.

[3] E. M. Zelie, "The Effect Of Internal Control Components On Mitigating The Impact Of Covid-19 Risks In Healthcare Organizations In Ethiopia," *J. Econ. Business, Account. Ventur.*, 2021, Doi: 10.14414/Jebav.V23i3.2517.

[4] R. Sharma, A. Shishodia, S. Kamble, A. Gunasekaran, And A. Belhadi, "Agriculture Supply Chain Risks And Covid-19: Mitigation Strategies And Implications For The Practitioners," *Int. J. Logist. Res. Appl.*, 2020, Doi: 10.1080/13675567.2020.1830049.

[5] F. De Andreis And M. Florio, "Risk Management Instruments, Strategies And Impacts In The Complex Organizations," *Am. J. Ind. Bus. Manag.*, 2019, Doi: 10.4236/Ajibm.2019.95078.

[6] A. Shahzad, M. Khan, T. Salahuddin, And S. Qaim, "Impact Of Perceived Business Risk On Organization Performance: An Integrated Risk Management Framework Based On Internal Controls," *Int. J. Manag.*, 2021, Doi: 10.34218/Ijm.11.12.2020.293.

[7] A. Gurtu And J. Johny, "Supply Chain Risk Management: Literature Review," *Risks*. 2021. Doi: 10.3390/Risks9010016.

[8] L. Hu, R. Liu, W. Zhang, And T. Zhang, "The Effects Of Epistemic Trust And Social Trust On Public Acceptance Of Genetically Modified Food: An Empirical Study From China," *Int. J. Environ. Res. Public Health*, 2020, Doi: 10.3390/Ijerph17207700.

CHAPTER 3

A FUNDAMENTAL CONCEPT OF TYPES OF RISKS

Dr.Raja Sankaran, Associate Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.raja_sankaran@cms.ac.in

ABSTRACT:

Any company must deal with risk, and companies must comprehend the many hazards in order to put good risk management practices into place. Risks may be categorized in a variety of ways. There are several other categories into which hazard risks might be subdivided, including risks to people, dangers to property, and risks to business continuity. Numerous official risk categorization systems exist, and they are discussed in Paper. A core idea of risks is to classify them according to their nature, source, and effect. For companies to successfully identify, analyze, and manage risks and improve their capacity to accomplish their goals and objectives, they must have a thorough understanding of the many kinds of risks.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

This section analyzes the benefit of categorizing risks according to the timeline for the effect of the risk, while it shouldn't be taken as a formal risk classification system. Analysis of an organization's risk exposure may be done extremely effectively by categorizing risks according to their long-, medium-, and short-term impacts. These risks will be connected to the organization's strategy, tactics, and operations, in that order. Risks might be seen in this sense as being connected to things like occurrences, changes in the environment, actions, or choices.

In general, long-term hazards will manifest themselves many years possibly up to five years after the incident or choice. Strategic choices consequently have an impact on long-term risks. When the decision is made to introduce a new product, it may take some time before the outcome of that choice (and the product's success) becomes clear. The effect of medium-term risks often manifests a year or so after the event or decision, depending on the circumstances. Medium-term hazards are often connected to specific projects or work programs. For instance, choosing a computer system is a long-term or strategic option if new computer software has to be installed. The endeavor to adopt the new software, however, will include medium-term choices with medium-term risks. Short-term dangers start to affect you as soon as the incident happens. Short-term hazards include theft, fire, road accidents, workplace accidents, and other occurrences that have an immediate impact and lasting effects. These short-term risks disturb regular, effective operations right away and are arguably the simplest sorts of risks to recognize, manage, or minimize.

Despite the uncertainty surrounding the precise timing, amount, and effect of insured occurrences, insurable risks are often transient hazards. In other words, insurance is designed to provide defense against risks with immediate repercussions. In the case of insurable risks, the

event's nature and effects may be understood, but its timing is unpredictable. In reality, when the insurance coverage is purchased, it is unknown if the incident will happen at all. Take a closer look at the functioning of a new computer software system as an example. In an effort to increase functionality and efficiency, the company will install the new software. There are potential hazards associated with the decision to install new software and the program selection. A project will be needed for the installation, and that project will contain certain hazards. The project-related hazards are within our control. The new program will be exposed to risk factors after installation. It may not provide all of the necessary capabilities, and the program could be vulnerable to different dangers and virus infection. These are the potential hazards that this new software system may provide.

DISCUSSION

What will be the mechanism that will cause a risk to manifest is a factor that businesses must take into account more and more. It's possible that the company confronts a number of significant risks, many of which might be disastrous if they came to pass. The difficulty for management then lies in understanding the conditions in which one or more substantial risk occurrences may occur. As important to take into account as the source of risk and the characteristics of the event, if it were to occur, is the issue of what would set off such an event. The occasion for Northern Rock's downfall is examined in the box below.

Four categories of risk

Risks are said to fall into four categories throughout the paper, and descriptions of each of these categories are provided in Appendix B. The four categories of risk are as follows:

1. Compliance hazards.
2. Dangerous hazards.
3. Manage hazards.
4. Possibility dangers.

Strategic risk is the first kind of risk and it has to do with the goals, objectives, and business model of a firm. Strategic risks may affect the long-term survival of an organization and are caused by things like shifting market circumstances, technical development, and competition. Operational risk, sometimes referred to as internal process, system, and human error risk, is the second category of risk. Operational risks may affect an organization's effectiveness, production, and reputation. They might include supply chain interruptions, system malfunctions, and staff misbehavior. The third category of risk is financial risk, which has to do with a company's capacity to pay its debts. Financial risks may affect an organization's profitability, cash flow, and solvency and can be caused by variables including market volatility, credit risks, and liquidity hazards. Compliance risk, which has to do with how well a company complies with legal and regulatory obligations, is the fourth category of risk. Non-compliance with environmental standards, data privacy laws, and anti-bribery and corruption legislation are just a few examples of compliance hazards that may harm an organization's image and result in financial fines [1], [2].The last form of risk is reputational risk, which is defined as hazards brought on by unfavorable impressions of a company among its stakeholders, such as clients, shareholders, and

staff. Reputational risks may occur as a result of events like product recalls, data breaches, and ethical transgressions, and they can have an adverse effect on a company's brand value, client loyalty, and investor confidence. If risk management is to contribute as much as possible inside a company, there has to be a shared language of risk. The company will be able to establish a shared understanding of risk and attitude toward risk by using a single language. The agreement on a risk categorization system, or succession of such systems, is a necessary step in creating this shared vocabulary and sense of risk. Consider someone who is assessing their financial situation and the hazards they now face. It's possible that generating enough money and controlling spending are the main financial dependence. An evaluation of the risks to pension plans, real estate ownership, and other assets should be part of the examination. The income risks and their makeup (opportunity risks) will be discussed in this section of the examination.

Consider the risks connected with owning a vehicle as a concrete illustration of the nature of compliance, hazard, control, and opportunity risks. The dangers of noncompliance here concern the responsibilities of owning and operating a vehicle under the law. The owner does not want the occurrences that pose a danger to occur. The expenses that are known to be associated with uncertainty may change. The advantages of owning a vehicle are, finally, the opportunities. In terms of money, the evaluation will take spending trends into account to evaluate if cost-cutting is required (hazard risks). There may be some uncertainty surrounding spending and the price of these activities (control risks), and it will also take into account leisure activities like travel plans and hobbies.

Hazard risks are those that will only prevent the company's purpose from being accomplished. These hazards or dangers are often those that can be insured, such as fire, storm, flood, injury, and so on. The control and reduction of hazard hazards are the roots of the discipline of risk management. Loss, damage, failure, theft, and other dangers connected with a broad variety of dependencies may interfere with regular, effective operations. cites instances of disruption brought on by people, places, things, and processes (Ps). The Ps may be seen as an illustration of a risk categorization system, and these dependencies can also be causes of risk. Risks that cast doubt on the organization's capacity to carry out its objective are known as control risks. An effective approach to a control risk is to implement internal financial control measures. There is no way to predict what will happen if the control mechanisms are eliminated. The most difficult sort of risk to convey is control risk, however the paper on project risk management will help with comprehension [3].

Uncertainty-related control risks include, for instance, the possibility for failing to attain legal compliance and losses brought on by fraud. They often rely on competent people management and the use of control measures. Despite the fact that the majority of businesses make sure that control risks are well controlled, they may still be potentially important. Opportunity risks are those that the corporation (typically) consciously seeks out or accepts. These risks are there because the company wants to improve mission fulfillment, but they might also hinder the organization if the result is unfavorable. The most significant kind of risk for the long-term success of any firm is this one. In anticipation of a large profit or return, many firms are eager to invest in high-risk business initiatives. These groups might be seen as having a voracious hunger

for opportunity investing. The same organization will often have a different stance on hazard concerns and have a low hazard tolerance. This may be suitable since the firm may have the mentality that it does not want risk-related hazards eating its resources when it is spending so much value in opportunities [4].

The additional category of compliance risks, in addition to hazard, control, and opportunity risks, may need independent analysis. Compliance concerns are crucial for highly regulated businesses including energy, banking, gaming, and transportation. Due to the unique nature of compliance risks, they are sometimes seen as a discrete type of risk and are frequently handled or reduced in a different way. Many businesses will want to guarantee complete adherence to all laws and regulations and assume no risk in this area. For compliance risks, this could be conceivable, but for risks related to hazards, controls, and opportunities, it's nearly likely not the case. Strategic, tactical, operational, and compliance (STOC) risks are further discussed in Paper as part of the STOC hazards debate.

Risk Categories

Accept opportunity risks

Organizations take certain risks voluntarily in order to accomplish their goals. These risks are often business or market risks that have been taken with the hope of making a profit. Alternative terms for these opportunity risks include commercial, speculative, or business risks. Opportunity risks are the kind of risk that have the potential to improve (but they may also hinder) the accomplishment of the organization's purpose. These are the dangers connected to seizing business opportunities [5].

Every firm has a desire to take advantage of possibilities and a willingness to invest in them. The organization will continually strive for effective and efficient operations, tactics, and strategy. Opportunities may also be created through increasing the effectiveness of operations and putting change efforts into place, although opportunity risks are often linked to the creation of new or modified strategies. Each firm will need to determine its hunger for capturing new possibilities and the necessary amount of commitment. For instance, a company can be aware that the market needs a new product that it can create and deliver thanks to its experience. However, if the company lacks the means to create the new product, it may not be able to put this plan into practice, and it would be foolish for it to pursue such a potentially dangerous course of action.

The decision to take advantage of the apparent opportunity will be made by the company's management. The organization may have that hunger, but it does not always imply it is the right thing to do. The company's board should be cognizant of the possibility that, despite their desire to seize the opportunity, the organization may not have the risk tolerance to sustain that course of action. The goal of opportunity management is to maximize the advantages of taking entrepreneurial risks. Businesses will be willing to take investment risks in opportunity. Strategic planning and opportunity management are clearly related. The goal is to increase the possibility that investments in business prospects will produce a major positive consequence. The example that follows examines risk variables by categorizing them as controllable and uncontrolled and relates them to individual lifestyle choices. Although the example deals with personal health risk

factors, determining whether or not business hazards are within the organization's control is a crucial part of effective business risk management.

Control Risk and Uncertainty

A measure of uncertainty must be accepted by an organization while launching initiatives and executing change. Risks related to control or uncertainty are an inherent component of doing a project. A project budget will need to include a contingency reserve to cover unforeseen expenses, and project timelines will need to account for this time as well. The company must provide the resources required to identify controls, put controls in place, and deal with the fallout if any control risk materializes in order to establish acceptable solutions to control risks. The degree of uncertainty and the kind of risk determine the nature of control risks and the relevant solutions. A departure from the desired or anticipated result is represented by uncertainty. A project that an organization is working on, like improving a process, must be completed on schedule, within budget, and according to specifications. Additionally, the improvement must provide the desired results. Project advantages that differ from expectations indicate uncertainties that can only be tolerated up to a certain point [6].

Internal auditors and accountants base their risk management strategy on control management. As of September, the UK corporate governance code's obligations for risk management mostly ignored risk assessment in favor of internal control. Control management aims to lessen the uncertainty around key risks and the unpredictability of results. If a business focuses too much on control management, there are risks. Because an excessive emphasis on internal control and control management is often said to stifle entrepreneurial endeavor, the company shouldn't get fixated on control risks.

Minimize Danger Threats

Organizations are subject to a variety of dangers, as covered in Papers and These risks will include opportunity, control, and hazard risks. Organizations must be willing to invest in opportunity risks, accept exposure to control risks, and endure hazard risk exposure. It is widely agreed upon that organizations should have zero tolerance for health and safety concerns and should take all necessary steps to remove them. In reality, this is not feasible, and businesses will reduce safety hazards to the barest minimum that still complies with the law and is cost-effective. For instance, it is theoretically possible to install trains with an autonomous braking system to prevent them from running red signals. However, the railway operating corporation could consider this to be an excessive investment. The organization's risk exposure or hazard tolerance may be seen as being affected by the effects of trains running past red signals, yet the expense of installing an automated braking system may be viewed as being unreasonably costly. Theft is a less emotional illustration. Most businesses will experience a small amount of petty theft, which may be manageable. Businesses operating in an office setting, for instance, may experience some stationery theft, such as the loss of paper, envelopes, and pencils. It becomes more cost-effective for the company to assume that these losses will happen since the expense of eradicating this small-scale theft might be quite high. The following example shows how various retail sectors may tackle shoplifting quite differently [7].

It is necessary to identify the variety of hazard hazards that might impact a company. Hazard risks may cause the company to experience an unforeseen interruption. Disruptive occurrences reduce productivity and should be avoided unless they are necessary, such as during scheduled maintenance or emergency procedure testing. Regarding hazard risk management, the ideal situation is one in which there are no unforeseen disruptions or inefficiencies caused by any of the factors. a rundown of the things that might lead to unanticipated interruption or inefficiency. These occurrences are broken down into a number of categories, including people, places, things, processes, and things. The company must assess the potential kinds of occurrences, their causes, and their expected effects on regular, effective operations for each category of hazard risk. Analysis and management of three hazard risk components go hand in hand with hazard risk management. In Papers and, this is covered in further depth. In conclusion, the organization should consider the required steps to stop the loss from happening, restrict the harm that the event may do, and keep the expense of recovery from the event under control. The insurance industry has historically used a hazard management strategy. Organizations will have a threshold for risky hazards. The strategy need to be built on lowering the probability, size, and effect of hazard losses.

Poor Quality of Goods or Services

The method for reducing the financial cost of losses is represented by the disruption brought on by supplier failure, the delivery of faulty products or components, or the failure of outsourced facilities and services. Additionally, certain hazard concerns may be categorized as compliance risks since they are connected to regulatory requirements. The majority of businesses want to reduce compliance risks. The organization's risk tolerance has to be thoroughly examined before deciding on the amount of insurance to obtain. Organizations may be ready to tolerate a specific number of motor vehicle accidents as a cost that will be covered by the organization's daily profit and loss. The company will need to decide what amount is acceptable since this will only be bearable up to a certain point. Following that, insurance should be bought to cover losses that are expected to surpass that sum.

Cut Down on Compliance Risks

The extensive variety of compliance criteria that enterprises must meet will be known to all of them. These regulatory standards differ greatly amongst company sectors, and many are heavily regulated with a specific regulator for the sector or industry. For instance, most nations throughout the globe set strict regulatory restrictions on businesses engaged in the gambling or gaming industries. 'License to operate' may be revoked by the regulator if regulatory standards are not met. This drastic response by a regulator might lead to the organization's eventual demise [8].

All businesses that deal with money are obligated to have policies to lessen the likelihood of money-laundering operations being carried out. Banks and other businesses that deal with large sums of cash must have anti-money-laundering procedures, and often, a top executive who is solely focused on this issue. Compliance concerns are important and may be difficult in the insurance sector. Compliance concerns offer special challenges when an insurance policy is

issued in one nation to safeguard assets or pay obligations in another one. If an unapproved form of insurance or illegal insurance policies have been issued, failure to comply with all requirements may result in insurance claims not being paid or, in the worst case scenario, being illegal in a certain nation. There are still many regulatory standards that must be met by organizations even if there aren't specific regulators for that area of the economy or industry. Most nations across the globe, in particular, have health and safety regulations that impose duties on companies to protect the welfare and health of workers and other people who may be impacted by their job activities. These safety criteria often include not just locations within the organization's direct control, but also the health and safety of personnel working abroad. Organizations with cars will also be subject to certain road safety requirements, particularly if they carry persons or hazardous materials [9].

CONCLUSION

Generally speaking, firms will strive to fully comply with all relevant laws and regulations in order to reduce the risks associated with noncompliance. In many situations, specialized risk management teams will be recruited. This is especially true when it comes to security measures, health and safety regulations, and money laundering. Organizations must be aware of their compliance risks and take them into account while conducting risk management procedures. Additionally, it is crucial to make sure that the company's different risk management sectors cooperate with one another in order to establish a coordinated and/or structured approach to compliance.

REFERENCES:

[1] T. Aven, “How Some Types Of Risk Assessments Can Support Resilience Analysis And Management,” *Reliab. Eng. Syst. Saf.*, 2017, Doi: 10.1016/J.Ress.2017.07.005.

[2] H. M. Li, X. C. Wang, X. F. Zhao, And Y. Qi, “Understanding Systemic Risk Induced By Climate Change,” *Adv. Clim. Chang. Res.*, 2021, Doi: 10.1016/J.Accre.2021.05.006.

[3] D. Dequech, “Fundamental Uncertainty And Ambiguity,” *East. Econ. J.*, 2000.

[4] T. Aven, “An Emerging New Risk Analysis Science: Foundations And Implications,” *Risk Anal.*, 2018, Doi: 10.1111/Risa.12899.

[5] J. Pospíšil, N. Matulayová, P. Macháčková, P. Jurníčková, I. Olecká, And H. Pospíšilová, “Value-Based Financial Risk Prediction Model,” *Risks*, 2021, Doi: 10.3390/Risks9110205.

[6] N. Schneiderman, R. C. Mcintosh, And M. H. Antoni, “Psychosocial Risk And Management Of Physical Diseases,” *Journal Of Behavioral Medicine*. 2019. Doi: 10.1007/S10865-018-00007-Y.

[7] S. O. Hansson, “Risk: Objective Or Subjective, Facts Or Values,” *J. Risk Res.*, 2010, Doi: 10.1080/13669870903126226.

[8] S. Abe And M. Ozawa, “Science Of Societal Safety: Living At Times Of Risks And Disasters,” *Crimrxiv*, 2020, Doi: 10.21428/Cb6ab371.2d564ad6.

[9] S. A. P. Clouston And B. G. Link, "A Retrospective On Fundamental Cause Theory: State Of The Literature And Goals For The Future," *Annual Review Of Sociology*. 2021. Doi: 10.1146/Annurev-Soc-090320-094912.

CHAPTER 4

SCOPE OF RISK MANAGEMENT

Dr.Vishal Soodan, Assistant Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.vishalsoodan@cms.ac.in

ABSTRACT:

Organizations may discover, evaluate, and prioritize any risks that might have an influence on their goals by using the crucial process of risk management. Risk identification, risk analysis, risk appraisal, and risk treatment are all included in the scope of risk management. Identification of all possible hazards that might have an influence on an organization's goals is the first stage in risk management. Identifying risks that result from both internal and external elements like competition, technological development, and regulatory changes is part of this. Risk analysis, which entails determining the probability and effect of each identified risk, is the following stage once hazards have been identified. Analyzing both the likelihood of the risk happening and its possible effects is part of this process.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

Risk management has several different historical roots and is used by many different types of professions. One of the first innovations in risk management came from the handling of insurance in the United States. Because insurance in the s was so expensive and had such a narrow scope of coverage, risk management practices expanded more widely and were better coordinated. Companies understood that buying insurance alone was not enough to ensure the safety of both persons and property. As a result, insurance purchasers started to worry about the level of property protection, health and safety regulations, product liability problems, and other risk management difficulties. During the s, a combined approach to risk financing and risk management emerged in Europe, and the notion of total cost of risk gained significance. As this strategy gained traction, it also became clear that corporations faced several risks that could not be insured. Then, as will be covered in more detail later in this paper, risk management tools and practices were applied to other disciplines.

Institute of Risk Management

Selection of the risks a business should take and the risks that should be avoided or mitigated, followed by action to avoid or reduce risk, is a process that aims to help organizations understand, evaluate, and take action on all of their risks in order to increase the probability of success and decrease the likelihood of failure. The discipline of risk management has reached a point of maturity where the connections to insurance are now significantly less. Although insurance is today regarded as one of the methods for reducing risk, it only applies to certain types of hazard hazards. Financial, commercial, market, and reputational risks are acknowledged to be of extreme importance yet fall beyond the traditional purview of insurance. The definitions

of risk management serve as examples of the variety of approaches to risk management. Just as challenging as coming up with a suitable and widely recognized concept of risk is coming up with a suitable definition of risk management. A description and definition that accurately captures the wide range of risk management activities is needed since it is widely acknowledged that risk management should be concerned with the risks, uncertainties, and opportunities. The author provides the following definition:

The series of actions done by an organization to provide the best possible result and lower the volatility or variability of that outcome is known as risk management. The list of problems listed in may be used to show why risk management is becoming more and more important. Numerous of these problems show how far risk management has come from its beginnings in the insurance industry. However, the insurance-based roots of risk management continue to be crucial and are still included into the strategy for hazard management. The nature of risk management and the predetermined steps that make up the risk management process are also topics covered in this paper. In the past, the word "risk management" was used to refer to a strategy that was exclusively utilized to address hazard risks. The field is now evolving in a manner that will allow risk management to contribute to better control risk and opportunity risk management [1].

Directing an Organization

Variable costs or availability of raw materials Cost of retirement, pension, and social benefits Demand for greater organizational transparency Impact of e-commerce on all facets of business life Increasing reliance on information technology (IT) systems Growing importance of intellectual property (IP). Greater supply chain complexity/dependence Reputational harm, particularly to global businesses High-profile failures and losses tarnish reputations Continued regulatory constraints are a factor. Joint ventures are becoming increasingly frequent as national legislation requirements change or vary.

Alterations in the Market

Globalization of consumers, suppliers, and goods Changes in the business and market environment Increased competition in the market. increased client expectations, often driven by rivals. Need to make bold strategic choices on a regular basis because of the need to react more quickly to stakeholder expectations and more turbulent markets with less consumer loyalty. It is necessary to achieve short-term success without sacrificing ongoing product innovation. Rapid advancements in technology pose risks to the global and national economies. Influenza or other pandemic threat Possibility of global organized crime. Increasing political dangers and societal unrest Extreme weather catastrophes that cause population shifts

Increasing Risk Management

There have been years since risk management became an established subject. Its early roots may be found in the specialized field of insurance, which has a long and illustrious history. The demand for risk management criteria grew as insurance got more regulated and structured, particularly in regard to the insuring of goods being moved by ships throughout the globe. The creation of the "Plimsoll Line" to denote the amount of cargo that a ship may safely carry

without being dangerously overloaded was perhaps one of the early advancements in this sector. Education programs to support the growth of risk management as a profession evolved as risk management grew more established. At this time, risk management laws related to corporate governance started to emerge, and different regulators received more power in regards to certain risks like health and safety) as well as in regards to certain business sectors like financial institutions. The process of creating risk management credentials got more institutionalized.

Risk management standards came into existence as a result of the advancement of risk management education and certification, as well as the more organized approach used by regulators. One of the first instances of a thorough approach to risk management is the AS/NZS risk management standard. Particular risk management strategies have also developed in some areas, such the banking industry, in addition to the general risk management guidelines applicable to all businesses. A higher degree of risk management maturity is expected of financial organizations, as shown by the establishment of regulated capital requirements for banks and insurance firms. In the United States, throughout the s, the function of corporate risk management expanded to include choices about the purchase of insurance. Contingency planning became increasingly significant to enterprises throughout the s. Beyond risk financing, loss prevention and safety management also received attention. Self-insurance and risk retention procedures emerged inside corporations in the s. Additionally, captive insurance firms began to emerge. Business continuity plans and catastrophe recovery plans later evolved from contingency plans.

The risk management strategy used by occupational health and safety practitioners saw significant development throughout the s and s at the same time. The use of risk management strategies in project management advanced significantly throughout the s. During the s, financial institutions kept improving the way they applied risk management tools and approaches to market risk and credit risk. The financial institutions expanded their risk management activities in the s to include methodical evaluation of operational hazards. Treasury departments also started to adopt the financial approach to risk management in the s. The need for greater coordination between insurance risk management and financial risk management strategies was acknowledged by finance directors. Products for risk finance that integrated insurance and derivatives started to appear.

The first chief risk officer (CRO) was appointed at that time, and at the same time, corporate governance and listing requirements urged boards to put a greater focus on enterprise risk management (ERM). Financial services companies have been urged to create internal capital models and risk management systems. CRO roles in banks, insurance businesses, and energy corporations have increased quickly. Due to the Sarbanes-Oxley Act in the United States, boards are increasingly devoting more time on ERM. Additional corporate governance standards as well as more thorough risk reporting have been adopted. But the financial crisis raised concerns about how risk management, particularly in financial institutions, might contribute to business success. Without a doubt, the global financial crisis could not have been avoided by using risk management tools and practices. Instead of intrinsic flaws in the risk management strategy, this failure was a failure to properly implement risk management processes and procedures [2], [3].

DISCUSSION

Areas Of Risk Management Expertise

A discipline that is continuously growing and changing is risk management. Risk management has significant ties to the credit and treasury operations in addition to its roots in the insurance sector and other areas of hazard management. Several departments inside major firms, including tax, finance, human resources, procurement, and logistics, will have a significant risk management component to their operations. However, experts in such fields are unlikely to see their work as just a subset of the risk management discipline.

Health and safety at work may be one of the most well-known and specialized fields of risk management. Planning for catastrophe recovery and business continuity is another area of expertise. Given the significant importance given to quality management systems, such as ISO, it is also undeniable that quality management is a highly well-developed part of risk management. Over the last several decades, more specialized fields of risk management have also emerged, including:

1. Risk management for projects;
2. Clinical and/or medical risk management;
3. Management of energy risk;
4. Managed financial risk;
5. Risk management for IT.

The development and use of risk management tools and approaches has greatly benefited from the contributions made by all of the aforementioned risk management specialty areas. The use of risk management tools and approaches is especially advanced in the field of project risk management. The management of uncertainty or hazards under control is a key component of project risk management, as was previously addressed [4].

The field of clinical risk management has been growing for a while. Patient care is the main focus of this field of risk management, particularly during surgical procedures. Risk management systems have been created as a consequence of the high cost of medical malpractice lawsuits and the inexcusable wait in insurance reimbursements. Making patients aware of the hazards linked with the operation they are about to undergo is one of the most important parts of clinical risk management. It's crucial for surgeons to document any mishaps that have place during operations. Clinical risk management has put a lot of emphasis on the need of reporting any accidents that take place in the operating room in a precise and timely way. A lot of effort has gone into developing the requisite systems and methods to address this specialized area of risk management, and there are several books on the subject.

Along with project and clinical risk management, a variety of specialized sectors have also adopted risk management methods and procedures. The financial and energy industries have used risk management strategies in particular. Operational risks, along with market, credit, and other financial risks, are the main focus of risk management in the finance industry. Chief Risk Officer is a position that originated in the financial industry. The use of risk management

methods and strategies has also received more attention in the energy industry. The future price of energy and exploration risk are the two key concerns for certain firms in the energy industry when it comes to risk management. Because hedging and other complex financial procedures serve as the foundation of the risk management endeavor, the risk management strategy is comparable to the tasks performed by the treasury department [5].

The relevance of operational risk management within the financial industry is discussed in Paper. Financial risk management has recently acquired a prominent visibility. Operational risk is simply one aspect of risk management in the financial industry. Operational risk, market risk, and credit risk will all be of concern to banks and other financial organizations. IT risk management is another highly developed and specialized discipline of risk management. Finance and insurance are highly regulated economic sectors that are controlled by international standards like Basel III and Solvency II. There are now distinct standards that apply to IT risk management due to the growing significance of information to enterprises in terms of data management and security. One of the most well-known of these risk management standards is COBIT, which resembles the COSO standard outlined in Paper in many ways.

Simple Risk Management Illustration

The steps that make up the risk management process are well-established. Each of these phases contributes significantly to the development of these worthwhile risk management operations. The risk management process may be portrayed in a variety of ways, and each of the standards discussed in this paper offers a somewhat different explanation. Risks should be recognized or identified, together with their nature and the conditions under which they could manifest. A risk register's "risk profile" is created by rating or evaluating hazards according to their probability and size. Comparing the existing or remaining level of risk to the specified risk appetite or risk criteria. Taking action in response to major hazards, includes choosing the best course of action in relation to the alternatives listed below:

1. Tolerate
2. Treat
3. Transfer
4. Terminate

Controls over resources are implemented to make sure that the essential preparations are done to launch and maintain the required control activities. Event management and/or response planning. This will involve disaster recovery or business continuity planning for hazard threats. using the organization's risk architecture for communication, reporting, and monitoring of risk performance, actions, and incidents. Reviewing the risk management system, which includes internal audit protocols and setups for changing the risk architecture, strategy, and protocols. a simple diagrammatic illustration of the risk management process is provided. The Rs and Ts of hazard risk management are the fundamental justification for the risk management procedure. The following are some of the risk management-related activities:

1. Understanding hazards;
2. Assessing hazards;

3. Ranking based on risk factors;
4. Taking action in the face of major hazards;
5. Resource management;
6. Event and reaction planning;
7. Risk performance reporting;
8. Examining the mechanism for managing risk.

By making certain that important dependencies are analyzed, tracked, and evaluated, risk management may enhance the management of an organization's essential activities. Tools and approaches for risk management will help in managing the hazards, controls, and opportunities risks that might have an influence on these critical dependencies.

Hazard Risk Management's Rules and Guidelines

To get over the challenge of a static picture of the state of the risks confronting the firm, organizations should make sure the risk management process is performed as frequently as required. This will guarantee that risk management continues to be an active process.

Organizational Risk Management

The enterprise or enterprise-wide risk management (ERM) strategy is another area where the risk management discipline has advanced recently. There is discussion on this risk management strategy. The primary characteristic that sets ERM apart from what would be called more conventional risk management is the more holistic or integrated approach used in ERM. It may be seen as a concept that unifies the management of all risks in various ways rather than as a novel or innovative strategy. An organization is beginning an enterprise risk management approach when it takes into account all of the risks it confronts and how these risks might affect its strategy, initiatives, and operations. Enterprise risk management ('ERM') is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio, according to the US risk management association, the Risk and Insurance Managers Society (RIMS). An enterprise-wide strategy has several benefits since it considers the possibility of upsetting stakeholder expectations as a whole. For instance, health and safety is thus seen as a part of ensuring that personnel is constantly accessible so that the entire operational core process won't be disturbed, rather than or maybe as well as a distinct hazard management problem [6].

Levels Of Complexity in Risk Management

The many forms of risk management that are now used are described in this paper. Risk management currently involves more disciplines and professions than in past years. This broadens the scope of how the discipline of risk management is developed. A company must not only have a sophisticated approach to and expectations for risk management, but also be mature in how it goes about managing risk. In Paper, the value of risk maturity is discussed. An corporation may not initially be aware of the contractual and legal commitments it must fulfill. It will be required to notify the organization of its responsibilities with regard to the risk in such

situation. The company will become more conscious of the need for greater risk management in general as well as the requirement to comply with responsibilities as the degree of complexity increases. The organization will need to change in response to the danger of hazard once it is aware of its commitments. The company will work to adhere to the proper risk control criteria as it reacts to the risk. After this point, the company could see that the risk has advantages. After that, the company will be able to function and see the risk as

For instance, a publisher may recognize that the lack of ethnic minority representation in the staff prevented it from completely complying with equal opportunity laws. The business will decide what needs to be done to change its practices so they comply with legal obligations. Once compliance is achieved, the publisher should be aware that a significant section of the staff has a broad ethnic background. The business should regard the diversity of its employees as an asset that will help it compete more successfully in the market by looking at chances to create and publish new magazines that would appeal to an audience that is more ethnically varied [7].

Levels of risk management sophistication are represented by the phases of reform, conformity, and performance. However, moving from danger to control to opportunity is not required for a risk or the practice of risk management. In reality, under some conditions, dangers may decrease. In an organization, a certain risk will always be of a certain sort. The effective management of such risk at whatever degree of complexity is acceptable at the moment may result in benefits. In conclusion, risk management only needs to be as complex as the company needs it to be in order to be beneficial. Despite the complexity of risk management's four tiers. There is a risk that businesses may become so preoccupied with risk management that crucial choices won't be made, despite the fact that they represent an enhanced approach to risk management. At this stage, it may be argued that giving risk and risk management too much attention would lead to the organization's operations deforming [8].

CONCLUSION

There are several charities and volunteer groups in the majority of the world's nations. The directors or trustees of these organizations should be very concerned and aware of risk management, which is reasonable and quite acceptable. But it's often said that trustees are more focused on risk management and good governance than they are on generating money for the charity they support. The causes that the charities are supporting would suffer if the organization's operations were paralyzed by this risk management worry. Risk management professionals should respect the contribution that alternative methods to risk management may make as their level of expertise rises and they become aware of them.

Even when good compliance requirements are met, management of compliance cannot be done in pieces. Hazard management experts may discover that, as a consequence of a more comprehensive approach to risk management, there has been a tendency toward a desire to retain more insurable risks (and purchase less insurance). Control management experts must refrain from stifling the organization's entrepreneurial spirit and endeavor. The effective exploitation of business prospects and the improvement of strategic choices may both be attributed to risk management tools and procedures, which strategic planners must acknowledge. The usage of the

Ns in Paper also takes into account the method for enhancing risk management sophistication that is explained in this section. The fragmented, organized, influential, leading (FOIL) method, which is also covered in greater depth in Paper, is an alternate strategy for achieving higher degrees of risk management sophistication or risk management maturity. The overall goal of risk management is to successfully discover, analyze, evaluate, and manage risks. This is accomplished via a variety of actions. Organizations may increase their capacity for achieving their goals and maintaining their competitiveness in the market by putting into place efficient risk management techniques.

REFERENCES:

[1] A. Y. Alam, "Steps in the Process of Risk Management in Healthcare," *J. Epidemiol. Prev. Med.*, 2016, doi: 10.19104/jepm.2016.118.

[2] A. Ghadge, S. Dani, and R. Kalawsky, "Supply chain risk management: Present and future scope," *The International Journal of Logistics Management*. 2012. doi: 10.1108/09574091211289200.

[3] A. A. Fashina, M. A. Omar, A. A. Sheikh, and F. F. Fakunle, "Exploring the significant factors that influence delays in construction projects in Hargeisa," *Heliyon*, 2021, doi: 10.1016/j.heliyon.2021.e06826.

[4] M. Altuntas, T. R. Berry-Stölzle, and J. D. Cummins, "Enterprise risk management and economies of scale and scope: evidence from the German insurance industry," *Ann. Oper. Res.*, 2021, doi: 10.1007/s10479-019-03393-x.

[5] R. P. Silva, G. S. C. Valente, and A. C. L. F. Camacho, "Risk management in the scope of nursing professionals in the hospital setting," *Rev. Bras. Enferm.*, 2020, doi: 10.1590/0034-7167-2019-0303.

[6] C. J. Costa, "Project management challenges," *OAE – Organ. Archit. Eng. J.*, 2019, doi: 10.21428/544e68e8.e4468a76.

[7] S. A. A. Shah, R. Sukmana, and B. A. Fianto, "Integration of Islamic bank specific risks and their impact on the portfolios of Islamic Banks," *Int. J. Islam. Middle East. Financ. Manag.*, 2020, doi: 10.1108/IMEFM-01-2020-0021.

[8] T. Creasy, Y. Fan, and N. Johnson, "Practitioners' preference: Which project planning components offer the most promise?," *Int. J. Proj. Organ. Manag.*, 2017, doi: 10.1504/IJPOM.2017.085290.

CHAPTER 5

PRINCIPLES AND AIMS OF RISK MANAGEMENT

Dr.Trupti Dandekar Humnekar, Associate Professor,
Department of Marketing, CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.truptidandekar@cms.ac.in

ABSTRACT:

The goals and guiding principles of risk management are intended to assist businesses in identifying, evaluating, and prioritizing any risks that might have an influence on their goals. The ISO 31000 standard serves as the foundation for the risk management goals and concepts, which are relevant to all sizes and kinds of businesses. The objectives of risk management include boosting an organization's capacity to accomplish its goals, enhancing stakeholder trust and confidence, safeguarding an organization's reputation and assets, and streamlining decision-making procedures. Overall, companies may successfully identify, evaluate, priorities, and manage risks using a complete framework that is based on the principles and objectives of risk management. Organizations may increase their resilience and maintain their competitiveness in the market by using efficient risk management techniques.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

The primary idea behind risk management is that it benefits the company. In other words, risk management actions are created to decrease outcome volatility or uncertainty while achieving the greatest potential result. There have been several efforts to identify the larger set of ideas that risk management is based on. A comprehensive list of recommended risk management concepts is provided in ISO 31000. The descriptions of what risk management activity should be and what it should accomplish are included in many of the lists of guiding principles. It is crucial to make a distinction between the goals of the risk management effort and the features of the risk management framework that will be implemented. A successful risk management project (and framework) is predicted to be:

1. Proportionate to the organization's degree of risk;
2. Coordinated with other corporate operations;
3. Complete, methodical, and organized;
4. Incorporated into company practices and standards;
5. Dynamic, iterative, and change-responsive.

This offers the acronym PACED and a highly sound set of guidelines that serve as the cornerstones of every organization's effective approach to risk management. a more thorough explanation of the risk management PACED concepts. The concept behind risk management is that it is something that can be recognized and managed. The concepts listed above pertain to the key components of risk management. These guidelines outline how risk management should really be done. Some sets of guiding principles additionally specify what risk management ought

to accomplish or achieve. It is helpful to divide the guidelines for risk management into two lists: the qualities that risk management should have, as described above, and the outcomes that it should produce, as given below.

1. Requirements imposed on the organization;
2. Confirmation of the handling of material hazards;
3. Choices that fully take into account danger factors;
4. Core procedures that are successful and productive.

The aforementioned guidelines should be followed when the risk management initiative is designed and the risk management framework is created if businesses are to get the most out of their risk management efforts. In many respects, choosing the organization's goals serves as the foundation for all risk management initiatives. The mandate, assurance, decision-making, and effective and efficient core processes (MADE) are some potential goals or drivers for a risk management project. Core processes, which might be strategic, tactical, operational, or compliance (STOC) in nature, serve as a representation of the organization's actions [1].

The acronym MADE, which stands for the objectives of risk management, confirms that the outcomes of risk management will result in less disruption of routine, effective operations, less tacit uncertainty, and better decisions regarding the assessment and selection of alternative strategies. In other words, effective organizational decision-making is a crucial component of risk management. The goal is to establish an optimal response to risk, prioritized in line with an assessment of the limited resources available for risk management.

Aims of Risk Management

Every firm must take steps to manage risk in a manner that it can justify to an acceptable level since risk cannot be completely avoided. The kind, scope, and complexity of the organization, as well as the threats it encounters, will determine the necessary spectrum of solutions.

The Significance of Risk Management

Several instances that highlight the significance of risk management. Due to the current global financial crisis and several high-profile business failures throughout the globe that preceded it, risk management has recently gained more attention. Additionally, risk management has grown more crucial due to rising stakeholder expectations and the improvement in communication tools.

Risk management may help with better decision-making, increased efficiency, and stakeholder assurance in addition to these other benefits. This guarantee consists of two key parts. Any organization's directors must have faith that risks have been recognized and that the necessary measures have been taken to manage them to an acceptable level. Additionally, firms are being urged to disclose information accurately, including risk data. Stakeholders need comprehensive data on business performance, including knowledge of risk. The major requirement of the Sarbanes-Oxley Act (SOX) in the United States is the accuracy of financial reporting. It demands complete and correct disclosure of all facts about the company and raises the importance of accurate outcomes reporting [2].

Despite the fact that SOX is a particular piece of law that only applies in certain situations, the ideas it includes are crucial for all risk management professionals. As a result, Papers and believe that accurate reporting and risk assurance are crucial elements of the whole risk management process. The architecture of the risk management initiative and the risk management framework must represent the reasons why risk management is being conducted in the company, in terms of MADE, when determining the significance of risk management in the organization. The risk management objectives of the specific company must be taken into consideration while making these judgments. The drivers could have anything to do with a specific MADE aspect, such the efficacy and efficiency of operational core procedures. Some businesses have designated a loss control manager whose only duty is to lower the incidence and expense of accidents involving people as well as those involving damage to property and machinery. The project may sometimes be motivated by the aim to boost the organization's image by improved adherence to relevant laws and regulations or the capacity to exhibit more ethical behavior, especially in the supply chain.

Managing Risk Activities

A process like risk management may be broken down into many phases. One illustration of the steps in the risk management process is provided by the IRM Risk Management Standard. The International Standard ISO and other publications provide other examples of the risk management approach. In Paper, these criteria are discussed in further depth. To illustrate the process as the Rs and Ts of hazard risk management, the vocabulary used to describe the steps in the risk management process has been purposefully chosen. explains in further detail each of the phases. The risk management process is defined as the systematic application of management policies, procedures, and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring, and reviewing risk.

This is how it is described in the ISO Guide and British Standard BS. The development of rules, procedures, and practices, together with the duties of communicating, advising, and creating that environment, might be said to be more a part of the risk management framework than the risk management process itself. The risk management process is seen as a limited set of actions in this book, including the aforementioned identifying, analyzing, assessing, treating, monitoring, and reviewing of risk. This makes it obvious how the risk management process differs from the framework that guides and supports it. In order to create a thorough risk management standard, descriptions of the risk management process and the risk management framework are necessary.

If a single risk management approach, diagram, or both can be utilized to represent the management of compliance risks, hazard risks, control risks, and opportunity risks has been the subject of considerable debate. The four categories of risks are simply used to show the steps of the hazard risk management process since this book utilizes other language to explain them. When addressing hazard hazards, there are many alternatives. These are sometimes referred to as the Ts of hazard risk management, and in Paper, these risk response alternatives are more thoroughly discussed. In conclusion, the following are the options for addressing hazard risks:

1. Tolerate.

2. Treat.
3. Transfer.
4. Terminate.

DISCUSSION

Operational risks that are insurable or hazard risks might have an immediate effect. Therefore, the primary goal of the first implementation of risk management concepts was to assure that regular, effective operations would continue. Project management and the execution of programs to improve key business processes have become more important as risk management has grown. Processes must be both efficient and effective in that they provide the desired outcomes. For instance, having an effective software program is of little use if it cannot do the necessary variety of tasks. The most crucial choices a company must make are strategic ones. Better information is delivered via risk management, allowing for the more confident execution of strategic choices. A company must be able to achieve the desired goals with the plan it chooses. There are several instances of corporations that chose the wrong strategy or failed to execute the chosen strategy effectively. Numerous of these businesses experienced corporate collapse.

When technological advancements or shifts in consumer expectations occur, as is often the case with grocery shops, strategic choices are sometimes the most challenging. The example of a mature supermarket firm that attempted to implement a new strategy but failed is shown in the box below. Shortly after, the business was acquired. The goal of strategy should be to seize chances. For instance, a sports club could see the opportunity to increase product sales to its current clientele. Some organizations may set up a travel agency and provide related travel insurance to its supporters who go abroad. Additionally, a club credit card might be established and run by a fresh financial division. After identifying these opportunities, the club will need to consider the risks involved with prospective opportunity investments and develop an appropriate project schedule to carry out the chosen strategy. The likelihood that the right strategy will be chosen, the right tactics will be designed, and operations will ultimately be effective and profitable will rise if proper consideration of risk is given to each of these processes. It's important to remember that projects and work plans are the strategies used to carry out strategy.

Businesses that have effective and efficient operations, compliance, and strategies but have the wrong overall strategy fail. No matter how effective the risk management initiatives are at the operational and project levels, this will still be the case. More company failures have been caused by poor strategy than by ineffective or inefficient operations or tactics. However, as the text box below from The Rank Group Plc's Annual Report and Financial Statements demonstrates, the significance of compliance operations cannot be overstated [3].

Putting Risk Management in Place

Risk management is a subject that is quickly expanding, therefore there is potential for various practitioners to become intolerant of the strategy used by others. Internal control experts who think that managing risk is all about achieving organizational goals and managing uncertainty shouldn't grow intolerant of the more conventional insurance risk management strategy. There is

no benefit to one group of professionals dismissing the strategy used by another and refusing to use the knowledge that is there in the other group.

In any event, there isn't a single risk management methodology or strategy that has all the answers. It is obvious that the many styles that might be used inside an organization should function as complementing methods. The integrated approach to risk management acknowledges that the firm must be willing to tolerate certain hazard risks and invest in opportunity risks. To accomplish the following, risk management tools and strategies should be used:

1. Risk governance is provided through compliance management;
2. Hazard management lessens undesirable effects;
3. Control management narrows the potential outcomes;
4. Management of opportunities improves results.

Any hazard event's consequence will be less detrimental with the help of hazard management. Insurance serves as a technique for limiting the financial cost of losses when a risk materializes in the context of hazard management. Techniques for risk management and loss management will lower the anticipated losses and should guarantee that the total cost is controlled. The organization's risk tolerance will inevitably and appropriately decrease as a result of the combination of insurance and risk control/loss management lowering the real cost of hazard losses. The organization's risk capacity will thus be more readily accessible for opportunity investment. The variety of potential outcomes from every event is reduced via control management. Internal auditors' well-established methods of internal financial control serve as the foundation for control management. The major goal is to lessen losses brought on by ineffective control management while also narrowing the range of potential outcomes. This is the contribution internal control should make to an organization's overall risk management strategy. The goal of opportunity management is to increase the likelihood and importance of favorable outcomes. The company should consider opportunities to boost sales of the product or service as part of its opportunity management strategy. Opportunity management should make it easier to give greater value for money in not-for-profit organizations[4].

Getting Results

The creation of bonus and incentive programs for employees and management is one option that may be explored during strategy meetings in order to improve rewards. In light of the lessons from the global financial crisis, it is obvious that these incentive programs need to be balanced and shouldn't encourage excessive risk-taking. The concepts of risk management that outline what risk management should be and what it should accomplish have been taken into consideration in this paper. Although firms may be aware of the advantages of risk management adoption, effective implementation must be done as a project or initiative. A thorough analysis of the steps necessary for effective enterprise-wide risk management is provided in Appendix C.

The obstacles to and facilitators for risk management implementation are discussed in further depth. The most crucial thing to stress is how critical it is to have top management's backing and, preferably, a board member's sponsorship. A strategy for execution is also required to address the worries of the workforce and other stakeholders. Although risk management is essential to an

organization's performance, many managers may need to be convinced that the advised implementation strategy is the best one. It's vital to remember that not all actions and responsibilities conducted by managers should be attributed to risk management by the risk manager. Even while risks are inherent in all choices, processes, procedures, and activities, not all actions inside the business will be guided by risk management [5].

Risk managers often ask themselves, "Why do automobiles have brakes? The response given is that they allow the automobile to go forward more quickly. This suggests that risk management should be seen as the organization's activity brakes. This is an entirely negative perspective that paints risk management in a bad light. Operations, tactics, and strategy are all made possible by effective risk management. It is important to consider the aforementioned query once again. In keeping with the analogy, risk management should be compared to the three automobile pedals. Risk management acts as a brake, reducing operational risks and assisting the company in avoiding disruptions, improving operational effectiveness.

Similar to how projects carry out the strategies in an organization, the clutch pedal in a vehicle is concerned with shifting gears. Risk management is thus also the clutch pedal in that it aids in the effective management of tactical change and the elimination of related uncertainty, enabling the company to successfully implement change. Last but not least, just as the accelerator makes a vehicle go more quickly, risk management satisfies this need by assisting the business in seizing strategic chances and pursuing rewards. This ensures that the organization develops and effectively executes a plan that provides precisely what is needed. This book spends a lot of time discussing how risk management is used in operations. Hazard risks are likely to have an influence on operations, hence hazard management is the main emphasis of risk management in relation to operations. Organizations must, however, concentrate on loss control if they want to get the most out of risk management input in operations. Loss control combines cost containment, damage management, and loss avoidance [6].

Projects must be finished on schedule, within budget, and to the desired performance or quality standards. All endeavors will inevitably be accompanied by a significant element of uncertainty. Risk management makes a contribution by reducing these uncertainties. Control management refers to the process of managing hazards inside projects. The risk assessment of the many strategic choices that a company has at its disposal is the main focus of risk management input into strategy. Therefore, the emphasis of risk management's contribution to an effective strategy is on the decision-making processes. The Es of opportunity management compares prospective return to risk exposure. Before making strategic choices, organizations that practice strategic risk management thoroughly examine all promising new business opportunities and do thorough risk assessments.

Several bullet points may be used to encapsulate the overall advantages of risk management. Less operation disturbance, project delivery success, and better strategic choices are anticipated by launching a risk management strategy. Initiatives for risk management will also be supported by a desire for proper risk assurance. The acronym MADE is made up of several elements: required, assurance, decision-making, and effective and efficient core processes [7].An company will be able to illustrate the advantages of a risk management project by using the format of the

FIRM risk scorecard. A theater that has been pursuing a systematic proactive enterprise risk management strategy for roughly three years will probably have received the following advantages: Financial gains via improved budget allocation, spending oversight, and less fraud vulnerability. Benefits to the infrastructure have included fewer IT system failures and lower worker absence rates. Benefits in terms of reputation from organic food consumption and ethical sourcing practices in the restaurant, as well as from successful niche shows in the theater. Benefits from the market led to occupancy rates of %, up from % three years before, and more patron spending at the theater. The theater will keep growing its risk management program and gaining advantages. Activities related to risk management are now part of the organization's management culture [8].

CONCLUSION

In conclusion, firms must adhere to the goals and principles of risk management in order to accomplish their goals, safeguard their assets and reputation, and increase stakeholder trust. Organizations may manage risks and improve their resilience by setting the context, identifying and analyzing risks, evaluating risks, treating risks, and monitoring and reviewing risks. The goals and guiding principles of risk management apply to both small and medium-sized businesses in addition to big companies. Organizations may use risk management procedures to find development possibilities and create a preventative strategy for possible dangers.Organizations confront a variety of risks in the quickly evolving business world of today, including economic, technical, and regulatory risks. In order to guarantee that a business is successful in attaining its goals, good risk management is crucial. The ideas and objectives of risk management may help organizations make better decisions, spot new possibilities, and handle risks in a proactive and efficient way. Overall, risk management is a vital procedure that may assist businesses in reducing possible hazards, maintaining their competitive edge, and achieving their long-term goals.

REFERENCES:

[1] O. Y. Tamimi, “The role of internal audit in risk management from the perspective of risk managers in the banking sector,” *Australas. Accounting, Bus. Financ. J.*, 2021, doi: 10.14453/aabfj.v15i2.8.

[2] M. Vaismoradi, S. Tella, P. A. Logan, J. Khakurel, and F. Vizcaya-Moreno, “Nurses’ adherence to patient safety principles: A systematic review,” *International Journal of Environmental Research and Public Health*. 2020. doi: 10.3390/ijerph17062028.

[3] H. Langdalen, E. B. Abrahamsen, and J. T. Selvik, “On the importance of systems thinking when using the ALARP principle for risk management,” *Reliab. Eng. Syst. Saf.*, 2020, doi: 10.1016/j.ress.2020.107222.

[4] A. Nawaz, A. Waqar, S. A. R. Shah, M. Sajid, and M. I. Khalid, “An innovative framework for risk management in construction projects in developing countries: Evidence from Pakistan,” *Risks*, 2019, doi: 10.3390/risks7010024.

[5] Iskandar, A. Nuruddin, and S. Siregar, “Manajemen Resiko Pembiayaan pada Bank Syariah : Suatu Tinjauan Filsafati,” *Al-Ulum*, 2017.

[6] L. Myeza, N. Nkhi, and W. Maroun, "Risk management factors contributing to transgressions in the procurement practices in South African SOEs," *J. Account. Emerg. Econ.*, 2021, doi: 10.1108/JAEE-03-2021-0073.

[7] N. Kuduz, "Green Business," *J. Corp. governance, Insur. risk Manag.*, 2021, doi: 10.51410/jcgirm.8.1.12.

[8] R. Luburić, "Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks," *J. Cent. Bank. Theory Pract.*, 2017, doi: 10.1515/jcbtp-2017-0003.

CHAPTER 6

APPROACHES TO RISK MANAGEMENT

Dr Kalavathy, Associate Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.kalavathy@cms.ac.in

ABSTRACT:

The identification, evaluation, and treatment of possible risks that might affect an organization's goals depend heavily on risk management strategies. Depending on their size, complexity, and the risks they must manage, organizations use a variety of risk management strategies. The conventional method of risk management focuses on identifying and evaluating risks before putting mitigation plans into place. This method is reactive and predicated on the notion that threats are external and beyond of one's control. This strategy often entails utilizing insurance to shift the risk to a different party. Risk management in the current era is proactive and focuses on spotting opportunities and possible dangers. This strategy identifies possible hazards and opportunities by employing scenario planning and data analytics. Additionally, it entails working with stakeholders to create plans for reducing risks and seizing opportunities.

KEYWORDS:

Business, Environment, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

The Code of Audit Practice to examine conformity with the laws, rules, and regulations that are within their purview. Our continuing success and expansion depend on the management of business risk, which can only be accomplished if all three risk components threat, uncertainty, and opportunity are acknowledged and handled holistically. The board has given the audit and risk committee the authority to create, coordinate, and oversee the group's risk management procedures. To identify and manage key risks in the operating divisions, business units, and subsidiaries, it oversaw the creation of an extensive risk management system.

The internal control systems are intended to reduce rather than completely eliminate risk, and they offer a reasonable level of assurance regarding the accuracy and dependability of the financial statements, compliance with applicable laws and regulations, and the safety and accountability of the group's assets. In addition to the group's internal risk management procedures, the group executive committee conducts a guided risk assessment workshop twice a year to identify, quantify, and analyze the group's risks. The board's risk appetite and tolerance metrics serve as a reference for measuring the qualitative and quantitative aspects of risk severity. The audit and risk committee reviews the risk profiles and risk responses at least once every six months. For each operational division, risk matrices are created and reported to the audit and risk committee in addition to the group risk assessment. With the help of this process, risks and opportunities are prioritized, and cost-effective solutions are created and put into action to mitigate their consequences and seize their potential.

Risk-Management Guidelines

Standards For Risk Management's Range

There are many well-known risk management frameworks and standards. Following those being produced in Canada, Japan, the UK, and the United States, the first was created by the standards body in Australia in. Other national standards groups, as well as government agencies all throughout the globe, have also created standards. Every one of these standards follows a similar general strategy. In many companies, the COSO standard's ERM variant is also frequently used. Risk Management: Code of Practice and Guidance for the Implementation of BS ISO, British Standard.

Towards the end of, the ISO standard 'Risk Management: Principles and Guidelines' was released. Although certain standards are more widely accepted than others, businesses should choose the strategy that is most appropriate for their specific situation. A risk management framework should not be confused with a risk management standard. A risk management standard outlines the overall strategy for the efficient management of risk, together with a description of the risk management process and a proposed structure to support it. A risk management standard is, to put it simply, the union of a description of the risk management process and the suggested framework.

Later on, we'll go through the main components of a risk management framework. Summarizes the most popular risk management frameworks and standards. The IRM, in collaboration with Airmic and Alarm, created one of the most well-known and extensively used risk management standards. The IRM Standard is a high-level strategy intended for non-risk management experts. The Australian Standard and the COSO standard/framework are mainly intended for use by professionals with specialized knowledge in risk management. The risk management method, as represented in Figure 1, and the IRM Standard are both free to download from the IRM website.

In addition to the British, ISO, and COSO standards, there are a few more that are respected and widely used. The Securities and Exchange Commission (SEC) in the United States views the risk guidelines from the Financial Reporting Council (FRC), which was revised in, as a viable substitute for the COSO Internal Control framework for Sarbanes-Oxley compliance. A substantial amount of information on risk management has been issued by several government departments, in addition to the existing standards and frameworks. The current risk guidance is available as a free download from the website of the UK-based FRC. The highly regarded Orange Book, which includes a substantial quantity of relevant data on risk management methods and approaches, was issued by HM Treasury in the UK. This book makes several references to the ideas and theories provided in the Orange Book [1].

While some of the standards that are now in use were created by risk management experts, others were created by accountants or auditors. The different standards all adhere to one of three main approaches: "risk management" strategy, which is adopted by ISO, British Standard BS, and the IRM Standard; the "internal control" methodology created by the FRC risk advice and the COSO Internal Control framework; the CoCo framework, a "risk-aware culture" strategy created by the Canadian Institute of Chartered Accountants.

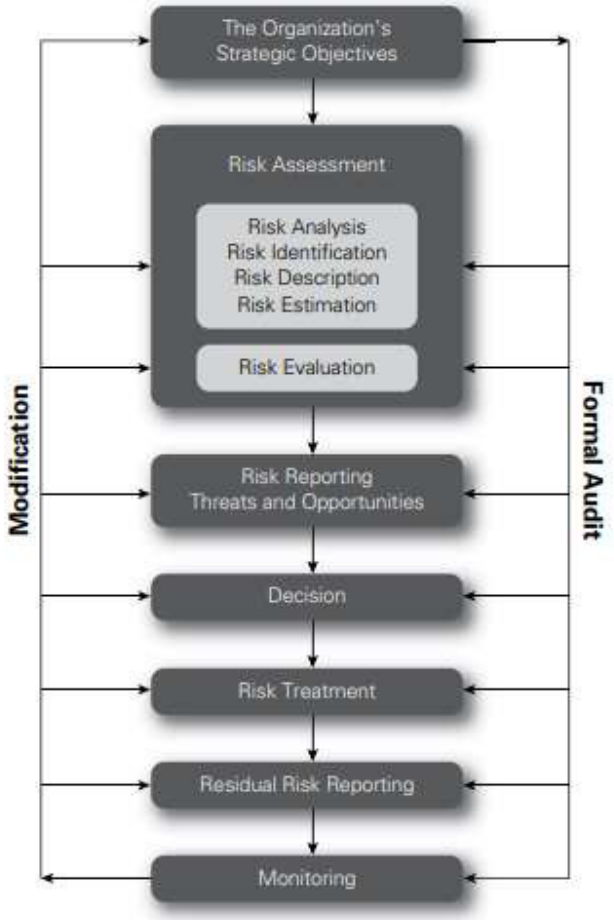

Figure 1: The Risk Management Process.

Process for Managing Risks

The risk management process is shown simply, and all recognized risk management standards include a method that is quite comparable. The framework that implements and supports the risk management process is distinguished from the process itself in many of the standards. However, many of the well-established risk management standards/frameworks do not always make this difference evident. The IRM Standard, ISO, BS, and COSO ERM framework are the most well-known risk management strategies. While a risk management framework is described in all four, the IRM Standard, ISO, and BS put a stronger focus on the risk management process. The COSO method focuses primarily on framework issues and does not make a difference between the framework and the risk management process itself. As part of their criteria to be listed on a stock market, some nations have created their own internal control and risk management standards. These are often COSO Internal Control-inspired frameworks, which is unquestionably the case with the UK's present FRC risk guideline standards [2].

The fundamental phases of the risk management process remain the same regardless of how it is represented. The vocabulary used to explain the various phases might be confusing, thus Appendix B contains explanations of fundamental concepts as well as cross references for the

many terminologies that can be used. The plan-implement-measure-learn (PIML) framework is used in Appendix C to define the steps required in effective risk management. This closely resembles the structure of "plan-do-check-act," or "PDCA," which is used in many international standards. PIML is meant to denote a more methodical and systematic approach.

There are several risk management frameworks and standards that have been developed by numerous businesses. It is widely accepted that a standard is a written document that provides information on both the risk management framework and procedure. It is mentioned in many risk management standards that risk management activities should be carried out in the context of the company, the business environment, and the risks that the organization faces. A framework is needed to implement and assist the risk management process in order to define and characterize the context. When conducting risk management activities, the internal context, external context, and risk management context should all be taken into account, according to ISO, which lays special emphasis on context. The risk management framework is mentioned in all of the published risk management standards, despite the fact that it is shown in various ways. The acronym risk, architecture, strategy, and protocols (RASP) has been created in order to provide a clear description of the extent of the risk management framework.

The key components of a risk management framework that is built around and supports the risk management process are outlined in the organization's risk guidelines as risk protocols, which also include the rules and procedures, risk management methodologies, tools, and techniques that should be used. The idea of the risk management context or risk management framework as specified in ISO is completely congruent with the RASP methodology. The risk architecture, strategy, and protocols (RASP) are covered in further depth in Part 5 of this book. These components make up the framework that the risk management process operates inside. For risk management efforts to be effective, these three-risk architecture, strategy, and procedures elements must be present. Prior to defining the framework that supports the risk management process, there must be a clear knowledge of the process itself. Considering that the framework is a collection of elements designed to help the risk management process [3].

The risk management framework must make communication and the flow of risk data easier to execute and assist the risk management process. Two distinct factors are taken into account in the risk management framework. It must, first and foremost, support the risk management process and, second, make sure that the process' outputs are shared across the business and result in the advantages that the organization expects. An organization would need to build up a framework that included the structure, responsibilities, administration, reporting, and communication components of risk management if it decided to adhere to the IRM Risk Management Standard. A risk management handbook will therefore have a record of all of these processes.

Characteristics of RM standards

The IRM Standard, ISO, British Standard BS, and COSO ERM framework are the four primary risk management standards that have been produced. Risk Management: Code of Practice and Guidance for the Implementation of BS ISO, a British Standard, was released in. It highlights

how a risk management framework is necessary to support the separately outlined risk management methodology. The risk management process should provide a systematic, effective, and efficient means of managing risks at various levels within the company, according to British Standard BS. Everywhere in the globe, there is a demand for regular standard reviews, usually every four years. As a result, both the already-existing standards and the new ones that are being created will be periodically reviewed. This will make sure that the recommendations and instructions provided in the different standards are current and consistent with best practices [4].

There are several internal control standards in place in addition to risk management guidelines. With the exception of the Criteria of Control (CoCo) framework created by the Canadian Institute of Chartered Accountants, these internal control frameworks have a different focus and are beyond the scope of this book.

ISO's Risk Management Methodology

The CoCo standard's methodology is briefly discussed here and assessed in greater depth in the book's concluding section. The strategy used by CoCo is based on an assessment of the organization's culture or internal control environment [5].

Updates To Current Standards

It is ongoingly desired to maintain corporate governance guidelines and risk management standards current and relevant. Regulators from all around the globe are constantly learning from one another and from company disasters. The development of management standards that are pertinent to a variety of risk management issues, such as business continuity, information security, corporate governance, and compliance management, is another emerging trend for standards organizations. An ISO management standard specification has a predetermined format, which is discussed in Paper. The most established of the ISO management standard specifications is ISO on quality management, and it is used for standards against which a company may be certified. The established risk management standards, such as ISO, the IRM standard, and the COSO ERM cube, often do not use the ISO format. The technical committee for ISO that is in charge of ISO has said that risk management activities are not suitable for external certification, which is one of the reasons for this.

Making ensuring that the risk management standards they publish are relevant to the organization's future performance is a problem for standards bodies. As can be seen from the text box below, COSO has adopted the stance that, while upgrading the COSO ERM framework, stakeholder expectations and the connection between risk and strategy should be given more weight. Organizations may gain a variety of advantages, including the following, by integrating enterprise risk management into strategic planning, according to the COSO consultation paper in particular:

By taking into account both the good and negative sides of risk, the variety of options is increased. Enhancing performance via comprehensive entity-wide risk identification and management. Minimizing unpleasant shocks, maximizing benefit, and profiting from favorable occurrences. Lowering performance variability via disruption-reducing measures. Enhancing

resource allocation and improving resource deployment. Although there are many advantages to adopting a recognized risk management standard, it is unquestionably true that organizations will need to modify and adapt any existing standard's specific requirements to their unique circumstances and/or the external, internal, and risk management contexts. When a risk management strategy has been precisely tailored for the business by the organization itself, there will be more acceptance of the strategy inside the organization. The fact that the plan implement measure learn (PIML) method is becoming more popular is one of the main aspects of developing approaches to risk management. This is the foundation of the US standard ASIS SPC and is often referred to as plan do check act (PDCA).

Area of the Situation

According to ISO, establishing the context is the first step in the risk management process. In addition to the risk management method, the context was described in the previous Australian Standard AS as having three components. The risk management context, internal context, and external context are these elements. A relationship between the three settings is seen in the following. The following three elements of context may be taken into consideration: The risk architecture, strategy, and procedures, or the risk management framework inside the company, have previously been defined as the risk management context. Two requirements must be met by this framework:

Assure that the outcomes of the risk management process are communicated to internal and external stakeholders and support the risk management process inside the company. The term "internal context" describes an organization's internal environment, including its operations, range of capabilities, and organizational structure. The expectations of internal stakeholders are included in the internal context. This might be seen as the organization's strengths and shortcomings. The environment in which the organization operates is known as the external context. The business sector in which the firm works, external stakeholders and their expectations, and the external financial climate will all be taken into account in this environment. This might be seen as the organization's opportunities and dangers. Setting the context for risk management requires careful assessment of the nature and scope of the risk management process. What the risk management process is supposed to accomplish or the reason why the firm has risk management activities in place is the crucial question. The risk management context also takes into account who will be in charge and determines the resources needed to carry out risk management tasks.

The determination of risk appetite or risk criteria is a crucial factor to take into account in the context of risk management. This will assist the company in determining the controls that need to be implemented and if the existing or residual level of risk is acceptable. The context of risk management should also provide a way to determine the whole total risk exposure so that it may be compared with the organization's risk tolerance and risk tolerance capacity. The internal context includes the organization's culture, its resources, how risk management process outputs are used and how they impact behavior, as well as how risk is supported and managed. The internal context includes the organization's capacity and competencies, goals, and established business core procedures. How the company takes choices is a crucial factor to take into account

when looking at the internal environment. The organization's external context includes stakeholder expectations, industry laws and regulators, competitive activity, and the broader economic climate. The external environment also takes into account the forces and developments that may have an impact on an organization's performance and capacity to meet its goals.

Added Context

'Establish the context' is the first step in the risk management process, according to ISO's risk management standard. Setting the context is a crucial component of effective risk management, and other international standards recognize it as a crucial first step in putting a management system standard into practice. also mentions that an organization's strategic planning must take context into account. The external context, internal context, and risk management context are the three parts that make up providing the context for risk management activities. The expectations of external stakeholders must be taken into consideration while establishing the external environment.

Customers will often be the most significant group of external stakeholders for many firms. The kind of consumers a business has and the goods or services it provides will have a big impact on the external environment. A significant component of the business model for the organization and its applicability to risk management is the company's consideration of customers and the customer offering. A company may examine the variables that affect the external environment for the organization in greater depth after it has determined what is expected of external stakeholders, including taking into account consumers and the services and goods they are supplied. The FIRM risk scorecard offers a framework for doing a thorough analysis of the organization's situation. The FIRM risk scorecard's reputational and market components are largely tied to the external environment, whilst the infrastructural and financial components are mostly related to the internal situation [6].

a thorough collection of inquiries about the creation of a riskiness index based on the FIRM risk scorecard's framework. In conclusion, the reputational aspect of a company's external environment determines how consumers see the firm, whether they want to do business with it, and the degree of customer retention. The following problems should be looked at in particular while analyzing the reputational aspect of the external context:

1. Attitudes of the general public about the organization's industrial sector.
2. Standards for corporate social responsibility that the firm has attained.
3. Governance requirements and how heavily regulated the industry is.
4. Standards for after-sales service and/or product quality.

The market and the organization's degree of market presence make up the other FIRM risk scorecard component pertinent to the external environment. The volume of client trade or spending will be impacted by this. The following concerns should be taken into consideration while assessing the external environment's market component, in particular:

1. The market's level of revenue creation and return on investment.
2. The existence of hostile rivals and/or high client expectations.

3. The stability of the economy, especially its sensitivity to interest rates and currency exchange rates.
4. The supply chain's complexity and the unpredictability of raw material prices.
5. Exposure to political risk, conflict, and terrorism-related global disruption.

A strengths, weaknesses, opportunities and threats (SWOT) analysis or the usage of one of the risk categorization systems covered in Paper may be used in addition to the FIRM risk scorecard to assess the organization's external environment. Determining the degree of riskiness connected with the external environment in which the business works is the ultimate goal of analyzing the external context. The firm will be able to use this to verify its current business model and create a future plan as well as the methods needed to carry it out.

Internal Setting

The expectations of internal stakeholders must be taken into consideration while establishing an organization's internal environment. There will be a variety of internal stakeholders, but the individuals directly dependent on the company will be the most significant group. This will include employees and those working as suppliers, contractors, or outsourced service providers. Once the expectations of internal stakeholders have been determined, along with their significance to the organization's operations and compliance efforts, it will be feasible to examine the elements influencing the internal context in greater depth. The FIRM risk scorecard offers a framework for doing a thorough analysis of the organization's situation. The reputational and market factors are largely tied to the internal environment, while the financial and infrastructural factors are mostly related to the external context in the FIRM risk scorecard [7].

a thorough collection of inquiries about the creation of a riskiness index based on the FIRM risk scorecard's framework. In conclusion, the financial aspect of an organization's internal environment specifies the financial practices and methods for managing finances and achieving profitability. The following considerations should be taken into consideration while considering the financial aspect of the internal context:

1. The availability of sufficient funding to carry out strategic initiatives;
2. The existence of reliable processes for the appropriate distribution of investment capital;
3. The environment for internal financial controls to stop fraud;
4. The availability of cash to cover current and foreseeable responsibilities.

Infrastructure is the second element of the FIRM risk scorecard that is relevant to the internal context since it affects the kind of procedures carried out inside the firm. The degree of inefficiency and dysfunction that may develop during internal processes is defined by infrastructure risks. The following problems should be taken into consideration while assessing the internal context's infrastructure:

1. The organization of senior management and the characteristics of the risk culture;
2. The availability of sufficient intellectual property as well as human resources and expertise.
3. The presence of sufficient physical resources to support operational activity.

4. An adequate information technology infrastructure for data protection and resilience.
5. There are strategies in place to maintain business continuity in the event of a significant interruption.
6. Plans for the provision of services, transportation, and a solid communications infrastructure.

The FIRM risk scorecard is one tool for assessing an organization's internal environment, although other strategies, such as a SWOT analysis, may be used. The political, economic, social, technical, legal, and environmental/ethical (PESTLE) risk categorization method is used by many organizations. In Paper, the PESTLE risk categorization system is discussed in further depth. The PESTLE risk categorization system has certain components that are important to the external context, some that are relevant to the internal context, and others that are applicable to both the internal and external contexts. It is possible for an organization to determine the kind of the external and internal environment in which it functions by using one of the various checklists that are available. The adoption of a categorization system or question list is less crucial than the need to identify the complete spectrum of risk challenges the firm faces. The company will be able to verify the current business model, the resources needed to deliver the business model, and the degree of resilience within the current business model as a result [8].

Context for Risk Management

The paper carefully examines the risk management environment in light of the risk architecture, strategy, and protocols (RASP) created by the company. An organization's RASP outlines the framework for the risk management context and the procedures for putting its elements into practice in order to get the intended results from the enterprise risk management project. It is crucial that an organization's risk management context be able to offer the essential risk management plan and foster the requisite risk-aware culture. Leadership, engagement, learning, accountability, and communication (LILAC), as more specifically explored, are the elements of a suitable risk-aware culture. The senior management mandate, which specifies the scope and degree of authority for carrying out risk management activities in the business, is a crucial part of the risk management framework. The organization's risk management policy has to specify the mandate given to the risk manager, head of internal audit, and other participants in the risk management program.

The organization's risk management context is defined by its risk attitude and appetite, which are determined by the risk criteria for various categories of hazards. These criteria also serve as the foundation for conducting risk assessments and documenting the findings in the risk register. The kind and degree of transmission of the data in the risk register across the organization's risk architecture also contributes to the definition of the risk management context. The implementation of the enterprise risk management effort is perhaps the most crucial aspect of the risk management environment that will impact its success. The planning, implementing, measuring, and learning (PIML) process for an enterprise risk management effort is outlined in Appendix C.

The risk management environment must support the organization's performance and the fulfillment of both internal and external stakeholder expectations. Identification of emerging risks and support for organizational responses to changes in the external and internal environment are requirements of the risk management context. Emerging hazards may have a complicated character and, by definition, are quite unpredictable. The risk management context should provide the early warning system to aid the firm in identifying the nature of developing hazards. This has been referred to as the organization's "risk radar" and it must entail the timely study and assessment of data pertaining to developing hazards. The system for detecting emerging risks should also contain a provision for recognizing opportunities that may be taken advantage of in the future in order to fully establish the precise effect and implications for the company.

In conclusion, the organization must recognize every specific internal, external, and risk management context issue that could have an impact on the organization, gather and assess timely knowledge and information about them, assess the opportunities and risks these context factors present, and take the necessary steps to seize those opportunities and mitigate the risks. Within the parameters of the risk architecture, strategy, and protocols (RASP), all of this must be recorded.

The Creation Of A Risk Registry

For many risk managers, using risk registers has become standard procedure. The chance that the data entered in the risk register will not be utilized in a dynamic fashion is only one of the drawbacks of using risk registers. The organization's risk action plan might be replaced with a static record of the status of risks in the risk register. According to the ISO Guide, a risk register is a "document used to record risk management process for identified risks." According to the book, the risk register's main objective is to make it easier for each risk to be owned and managed. The important risks that the company or project are experiencing are often covered by the risk register. The findings of the risk assessment for the project, business unit, location, process, or operation under consideration will be recorded [9].

It is more typical for the risk assessment to be utilized as part of the decision-making process when a risk assessment of strategic choices is conducted. This information is often offered to the decision maker as part of the entire range of information available for making that strategic choice rather than being documented in the form of a risk register. Creating a shared record of the important risks that have been recognized is the goal of the risk register. The risk register will also be used to keep track of the current control efforts. It will also serve as a record of any extra steps that are suggested to strengthen the management of the specific risk.

The risk registry will also include additional information concerning dangers. Despite the fact that this document has no set format, it may be thought of as having a fundamental structure. It may not be required to include all of the risk description details listed in the risk register since doing so would likely make the document cumbersome and confusing. Depending on the kind of risk assessment that is being documented, risk registers may be created in a variety of forms. gives a sample of a risk register for a sports club that is just half completed. The risk register may

be kept on a computer as a document in its most basic form. Serious traffic accident involving the transfer of fuel/explosives is one of the many more complex types of risk registers, however. Depending on the compounds involved, prepare for deaths and a km-radius evacuation. Potential for up to tonnes of liquid fuel to be released into the nearby environment. Up to six hours of disruption due to storm-force winds on transportation routes. Expect that the majority of the nearby roads will be blocked or limited. Longer travel durations and possible late delivery.

There is a good chance that one to seven days of operation time will be missed when there is a high frequency of rain. The previous two years' worth of issues indicate that the failure will happen twice a year. Due to the inability to put the action plan for better facilities into effect, the progress towards achieving standards in child care will continue to be unsatisfactory, resulting in care that falls short of the national requirements for children. Patients have a positive opinion of the existing setting and the caliber of treatment given. To guarantee that standards do not deteriorate, strong action must be done. databases have records of serious dangers. When quantifying exposure is necessary, a straightforward risk register kept as a paper is unlikely to be enough. This is accurate for systems that track operational hazards since these systems need to quantify risk exposure.

The Use of a Risk Register

An effective risk management strategy is built on a well-designed, dynamic risk register. The risk register, however, runs the risk of turning into a static record of the current state of risk management operations. This has the practical consequence that senior management may believe their risk management responsibilities have been satisfied by attending a risk assessment session and creating a risk register, and no further measures are necessary. It is preferable to think of the risk register as a risk action plan that offers a record of the key controls that are already in place as well as the specifics of any new controls that need to be implemented, as well as the state of the organization with regard to risk management. It shall be made clear who is responsible for carrying out the suggested steps when creating such a risk action plan [10].

the alternatives for recording the data from the risk register in a risk management information system (RMIS). Additionally, the organization's intranet may host the data included in the risk register, which will aid in communicating and comprehending risks. In certain businesses, the risk register is designated as a restricted record that internal audit may utilize as one of the primary sources of reference while conducting an audit of risk management practices. Even in the event that this is not the case, the data included in the risk register should be extremely thoroughly thought out and assembled. To accurately identify the origin, source, occurrence, size, and effect of every risk event, for instance, the risks included in the register must be carefully described. Additionally, any suggested new controls must be defined in detail and their proposed additions must be correctly noted.

For the controls to be understood by the audience, risk control actions should be sufficiently stated. This is crucial when the risk register has to do with the organization's regular business activities. Additionally, risk registers for projects and to support strategic choices should be created. An extremely dynamic document is required for a project risk register. At each project

review meeting, specifics of the project's risks, as listed in the risk register, should be reviewed. Risk registers must assist business decisions in addition to being relevant to projects. In this situation, a risk register's exact format could be less formal. The risk analysis of the proposed strategy should be included when a board-level strategic decision has to be made. The hazards of implementing the plan and an examination of the risks presented by not implementing the suggested strategy might both be included in this risk assessment. A risk register, which serves as a record of the risks that might affect the success of the business strategy, should also be included. establishing a business plan-compatible format for the context simple risk register. In this instance, a few straightforward examples of the risks that might prevent the business strategy from being realized are shown. For instance, a sports club could want to include reputational hazards in the risk register. There may be specific worries about the club's image, thus the board may demand a thorough assessment of the reputational risks associated with:

1. A win on the field.
2. Legal conformity.
3. The provision of moral products at reasonable cost.

The necessary degree of control and accountability for brand management will be assessed when taking reputational problems into account. The club will also ensure that any new controls and current measures are defined in a form that allows for a thorough audit of their implementation. The risk register should be presented to the board at least once every quarter, and more often if major changes take place. By doing this, you can be confident that the risk register will always be current and dynamic. Additionally, it will guarantee that the required measures are performed and the board is informed.

CONCLUSION

Enterprise-wide risk management (ERM), which incorporates risk management into an organization's broader strategy and decision-making processes, is another method of risk management. The ERM strategy entails identifying and evaluating risks across all business units and functions, ranking risks, and creating risk mitigation plans that complement the organization's goals. The ISO 31000 standard offers businesses a framework for implementing an organized and methodical approach to risk management. Establishing the context, identifying and analyzing risks, evaluating risks, addressing risks, and monitoring and reviewing risks are all important, according to the standard.

In conclusion, depending on their size, complexity, and the risks they confront, companies may employ a variety of methods to risk management. While the contemporary strategy is proactive and concentrates on finding opportunities and possible dangers, the conventional strategy focuses on detecting and evaluating risks. The ISO 31000 standard offers a framework for a methodical and organized approach to risk management, whereas the ERM approach incorporates risk management into an organization's broader strategy and decision-making processes.

REFERENCES:

[1] F. Bazzanella, N. Muratore, P. A. Schlemmer, And E. Happ, "How The Covid-19 Pandemic Influenced The Approach To Risk Management In Cycling Events," *J. Risk Financ. Manag.*, 2021, Doi: 10.3390/Jrfm14070296.

[2] A. Mills, "A Systematic Approach To Risk Management For Construction," *Structural Survey*. 2001. Doi: 10.1108/02630800110412615.

[3] S. F. Pileggi, M. Indorf, A. Nagi, And W. Kersten, "Corimas-An Ontological Approach To Cooperative Risk Management In Seaports," *Sustain.*, 2020, Doi: 10.3390/Su12114767.

[4] S. Jomthanachai, W. P. Wong, And C. P. Lim, "An Application Of Data Envelopment Analysis And Machine Learning Approach To Risk Management," *Ieee Access*, 2021, Doi: 10.1109/Access.2021.3087623.

[5] A. Bochkovskyi, "Actualization And Ways Of System Approach To Risk Management In Occupational Health And Safety," *J. Sci. Pap. "Social Dev. Secur.*, 2020, Doi: 10.33445/Sds.2020.10.3.8.

[6] R. E. Melchers, "On The Alarp Approach To Risk Management," *Reliab. Eng. Syst. Saf.*, 2001, Doi: 10.1016/S0951-8320(00)00096-X.

[7] M. Alauddin, M. A. Islam Khan, F. Khan, S. Imtiaz, S. Ahmed, And P. Amyotte, "How Can Process Safety And A Risk Management Approach Guide Pandemic Risk Management?," *J. Loss Prev. Process Ind.*, 2020, Doi: 10.1016/J.Jlp.2020.104310.

[8] I. Of R. M. (Irm), "A Structured Approach To Enterprise Risk Management (Erm) And The Requirements Of Iso 31000 Contents," *Risk Manag.*, 2010, Doi: 10.1016/J.Solmat.2010.12.013.

[9] J. M. Farber *Et Al.*, "Alternative Approaches To The Risk Management Of Listeria Monocytogenes In Low Risk Foods," *Food Control*. 2021. Doi: 10.1016/J.Foodcont.2020.107601.

[10] D. R. Zoidze And O. O. Gubarev, "Evolution Of Approaches To Risk Management In Organizations," *Bus. Inf.*, 2021, Doi: 10.32983/2222-4459-2021-4-276-285.

CHAPTER 7

A STUDY ON ENTERPRISE RISK MANAGEMENT

Dr.Sharat Kumar, Associate Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- sharat.kumar@cms.ac.in

ABSTRACT:

A complete approach to risk management known as enterprise risk management (ERM) include detecting, evaluating, prioritizing, and managing risks throughout a company. ERM is a comprehensive and organized plan that fits risk management with the overall goals and strategies of a business. Risks are seen by ERM to include both internal and external elements that may have an influence on an organization's capacity to meet its goals. Using the ERM technique, risks are identified across all business units and functions, and their potential effects on the goals of the company are assessed. ERM also entails creating risk mitigation plans that complement the organization's goals and risk tolerance. These tactics could include avoiding, minimizing, shifting, or embracing risks.

KEYWORDS:

Business, Enterprise, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

There have been significant advancements in risk management technique during the last several years. First, specialized disciplines of risk management, such as project, energy, financial, operational, and clinical risk management, have emerged. Second, firms have accepted the ambition to approach risk management from a wider perspective. This larger strategy has been referred to by a number of names, including holistic, integrated, strategic, and enterprise-wide risk management. The most popular and widely recognized nomenclature for this larger approach is enterprise or enterprise-wide risk management (ERM). Moving away from risk management as the discrete management of specific hazards is the primary tenet of the ERM methodology. ERM adopts a unified, more comprehensive, and integrated methodology. An organization that uses the ERM method examines all of the risks that it confronts in all of its activities. The control of risks that might have an influence on an organization's goals, critical dependencies, or fundamental activities is the focus of enterprise risk management (ERM). Along with managing control and hazard risks, ERM is also concerned with managing opportunities. The fact that many hazards are interconnected and that conventional risk management ignores the link between risks has also been taken into account. The ERM technique uses the possibility of two or more risks having an influence on the same activity or aim to determine the link between risks. The ERM strategy is centered on analyzing all of the risks that might have an influence on the target, critical reliance, or core process[1]–[3].

Risk management is a discipline that organizations use in many different ways. But most of these techniques have a lot of characteristics. a description of the components of enterprise risk management in contrast to the silo-based strategy, in which various risk categories are managed

using separate tools and methodologies on their own. In most firms, enterprise risk management is now the standard method for carrying out risk management tasks. This enables the company to have a comprehensive picture of all the dangers it confronts. includes all potential risk exposure areas for a firm, including financial, operational, reporting, compliance, governance, strategic, and reputational risks. rather than treating them as separate risk "silos," prioritizes and manages those exposures as a linked risk portfolio. Considers all important internal and external settings, systems, conditions, and stakeholders while evaluating the risk portfolio. acknowledges that organizational-wide individual hazards are interconnected and may result in a combined exposure that is different from the sum of the individual risks. gives all risks, whether they are mainly quantitative or qualitative in nature, an organized approach for management. aims to make risk management a part of all important decisions made within the firm. gives the business a way to determine the risks that it is prepared to accept in order to accomplish its strategic goals. builds a channel of communication for discussing risk problems so that everyone is aware of the risks the company faces and their significance. supports internal audit's efforts by giving the board and audit committee a mechanism for receiving assurance. believes that good risk management is a competitive advantage that helps companies accomplish their goals both strategically and commercially. that it is capable of managing these risks via coordinated action. However, specialized risk management activities like business continuity and health and safety continue to be important.

Consider a sports club as an illustration of the ERM strategy, where the main objective is to increase game attendance. This process consists of a number of steps, including marketing, promotion, the distribution and sale of tickets, as well as logistical planning to make sure that fans have the best possible experience during the game. Making ensuring there are sufficient parking and transportation options, together with acceptable food and other welfare preparations in the stadium, can help maximize attendance at sporting events. The club is able to identify the risks that might affect both these important activities and the core process by determining the key activities that provide the chosen core process. The club's commercial director has been given responsibility for the success of this fundamental procedure, and goals may then be established for increasing attendance at upcoming games. The prospects for raising game attendance may also be taken into account in this larger strategy.

ERM Definitions

a collection of definitions for enterprise risk management that have been proposed. A thorough description of the ERM process must include these three elements. These include the effect (or benefit) that results from those outputs, the description of the process that supports enterprise risk management, and identification of the process's outputs. The actions that make up the ERM method are described in several definitions, which focus on the process. Although this is a wonderful beginning point, the outcomes of the process itself are more significant. Some of the definitions do include reference to the outcomes of the process, such as the ability to manage risks within the organization's risk appetite and to provide an acceptable level of confidence over the accomplishment of goals [4].

The definition must, however, take into account the anticipated effect of those outputs in order to be complete. In conclusion, better choices will be made, improved core processes will be found and implemented, maybe via the use of strategies like projects or work programs, and operations will be effective, efficient, and free from unanticipated interruption. The accomplishment of statutory requirements, assurance attained, improved decision-making, and the introduction of effective and efficient core processes (MADE) are all examples of enterprise risk management outputs.

The author provides the following as a thorough explanation of ERM:

ERM entails the identification and assessment of important risks, ownership assignment, execution, and monitoring of activities to manage these risks within the organization's risk appetite. The output is information that is given to management to help with business choices, lessen ambiguity, and provide reassuring confidence that the organization's goals will be achieved. The benefits of ERM include increased service delivery effectiveness and efficiency, better capital (resource) allocation for company development, increased shareholder value, and improved risk communication with stakeholders.

DISCUSSION

ERM in Actual Use

It is explained how the risk manager's position is evolving. The seniority of the risk manager should be commensurate with the risks that the business encounters, it was noted. A risk director at the board level is often suitable for many firms, particularly those in the energy and financial sectors. The chief risk officer (CRO) is a term that is often used to refer to the risk management at the board level when it is suitable and reasonable. This may change as ERM becomes more solidly entrenched in a broader variety of firms, but up to this point, these appointments have been made nearly exclusively in the energy and banking industries.

One example of how ERM should be implemented in reality is the CRO's seniority. Enterprise risk management is completely compatible with the risk management tenets outlined in PACED. The PACED (proportionate, aligned, comprehensive, embedded, and dynamic) principles govern risk management. A variety of advantages may be provided by using a thorough approach to business risk management, and they are established. The enterprise risk management initiative's form and how these advantages will be realized are up to each business. The evaluation of all material hazards to the company is the main component of ERM. It is important to understand how hazards interact with one another so that the organization's overall risk exposure can be calculated. Once the organization's overall risk exposure has been determined, it may be compared to the board's appetite for risk and the organization's own risk capacity.

Business continuity and ERM

Business continuity management (BCM) and enterprise risk management (ERM) have a significant interaction. Business impact analysis (BIA), which forms the cornerstone of business continuity planning (BCP), and risk assessment, which is necessary as part of the risk management process, are closely connected. It outlines the characteristics of an enterprise-wide

strategy. The typical strategy for risk management is to assess the goals and identify the specific risks that may have an influence on them. Identification of the important activities that must be maintained for the company to continue operating is the result of a business impact study. One can see that the ERM approach and the business impact analysis approach are very similar based on the definition of the key dependencies and functions that must be in place for the continuity and success of the business. This is because both approaches are based on the identification of the key dependencies and functions that must be in place for the evaluation of core processes [5].

The next activity is where ERM and BCP diverge since business continuity focuses on the steps that need to be performed to ensure the continuation of specific operations, while risk management focuses on managing risks that might affect key business processes. The very particular purpose of the business continuity strategy is to identify the steps that need to be done to reduce the effect of a risk once it has materialized. The cost-containment and damage-limitation parts of loss control are referred to as BCP.

Energy and financial ERM

The fields of energy and finance have matured into well-established specialized subfields of risk management. An ERM initiative's goal in the financial industry is to increase shareholder value by: providing an impartial foundation for resource allocation and taking use of natural hedges and portfolio effects to increase capital and efficiency. supporting financial decision-making by taking into account places with a high potential for harm and by taking advantage of areas where there are advantages due to risk. Increasing investor trust by securing outcomes, shielding them from disruptions, and exhibiting proactive risk management. The treasury function and the specialized knowledge of hedging against the price of a barrel of oil are often used in energy sector ERM. Several energy firms have built quite sizable divisions in this field of financial risk management. However, the management of treasury risks continues to be intimately linked to the practice of ERM in energy businesses.

The regulatory environment is one of the factors influencing risk management in the financial industry. Banks are getting ready to apply Basel III standards after being subject to Basel II for a while. The Solvency II Directive will soon impose comparable restrictions on the European insurance industry. Financial institutions are obligated as a result to assess their operational risk exposure. The capacity to estimate the capital that needs be maintained in reserve to meet the effects of the identified risks materializing is the result of operational risk management (ORM) efforts in financial institutions. These ORM operations have the effect of improving risk identification and management, which lowers the capital needed to cover the repercussions of the risks materializing. The ERM technique may be considered as having a specific use in ORM inside financial firms. The collapse of the global financial system raised concerns about the efficiency of bank risk management programs, particularly operational risk management. One effect of the global financial crisis is that risk management is now often mentioned in news stories as having failed. In actuality, taking risks is necessary for firms to succeed. It is more challenging to refute the claim that banks' risk management efforts have failed. However, the truth is that the financial crisis was not brought on by a lack of risk management standards. It was the incorrect application of such concepts[6], [7]. Many banks committed two errors at once:

Banks made choices based on the benefits offered rather than taking a more balanced perspective of the risks involved in pursuing those greater profits because an appropriate risk and reward analysis was not conducted. The banks were adopting such a risk-aggressive stance that certain occurrences were seen to be so rare that they could be disregarded, making it difficult to quantify the degree of risk involved. It is beyond the purview of this paper to analyze the financial crisis in detail. However, it seems that the collapse of two separate sets of risk analysis models was what brought about the disaster. First off, the banks believed that repackaged loans, such as subprime mortgages, would remain marketable commodities, but this turned out to be untrue. Second, the banks believed that there would still be opportunities for short-term borrowing in the wholesale money markets. Banks utilize this short-term capital to continue lending money on a long-term basis at a higher profit rate. The majority of banks' credit models did not account for the collapse of the wholesale money markets.

Future developments in the field of enterprise risk management are likely to be concentrated on two main areas: first, ensuring that risk management activities are fully integrated into the organization's core business processes; and second, presenting quantifiable financial benefits related to the implementation of an enterprise risk management initiative. Leadership, participation, learning, accountability, and communication (LILAC) enable the organization to incorporate ERM. The assessment of an organization's overall risk exposure is likely being driven by advancements in the field of operational risk management.

It is important to discuss the strong growth of resilience as an organizational necessity for the s. while also taking into account the continuous development of enterprise risk management. Business continuity, crisis management, and more general needs pertaining to society's and enterprises' resilience will be covered by the ISO set of standards. In conclusion, enterprise risk management is a field that is well-established and here to stay, but it must be able to provide tangible, quantifiable financial advantages. These financial advantages must be shown via higher profits for businesses in the private sector and better service delivery efficiency and/or value for money in the public sector.

Risk managers must convince the firm and its stakeholders of the value offered by risk management, but this is not a simple process. How can risk managers convey the value they are creating when it may only be recognized in the case of unanticipated circumstances or, in the event that the new control mechanisms are effective, in the event that the risk never materializes? Risk managers must keep in mind that the ERM program's actual execution creates value on its own. Risk managers often lack the time to explain this benefit to the company because they are so busy effectively managing the program. The most important benefit of integrating a corporate risk management program into an ERM system is the growth of the whole firm's physical, financial, and cultural resilience while maintaining a focus on accomplishing its overall business goals. Risk managers may be their own worst enemies since a strong desire to effectively design, execute, and sustain an ERM program is one of the essential characteristics of a successful practitioner. Consequently, this devotion is a weakness since the practitioner must keep in mind that not everyone shares their passion.

The emergence of a "ivory tower" attitude is one of the main issues ERM programs deal with. In this case, a single department is responsible for all risk knowledge and actions. Risk managers must provide a framework that promotes the use of risk management tools and processes across the enterprise. Additionally, balance is necessary. Risk management procedures should not be imposed by practitioners in operational areas with minimal benefit. A system that is adaptable enough to work with the business to properly capture and manage the major risks without adding extra labor to address lower level risks is essential to the success of an ERM program [8].

CONCLUSION

Making choices based on a thorough knowledge of possible risks is one of the main advantages of ERM for businesses. ERM aids companies in identifying possible risks that might harm those chances for growth and development. The ERM framework offers a structured and organized method for risk management. Internal environment, goal setting, event detection, risk assessment, risk response, control actions, information and communication, and monitoring are the eight main parts of the framework. For big, complex businesses that deal with a variety of risks across several business units and activities, ERM is especially crucial. ERM, however, is adaptable to all sizes and kinds of businesses. ERM offers businesses a thorough approach to risk management that helps them to integrate risk management into their overarching goals and strategies. Organizations may make wise choices, spot possibilities for expansion, and successfully manage possible risks by implementing an ERM strategy.

REFERENCES:

[1] M. A. Arab, H. R. Khankeh, A. M. Mosadeghrad, and M. Farrokhi, “Developing a hospital disaster risk management evaluation model,” *Risk Manag. Healthc. Policy*, 2019, doi: 10.2147/RMHP.S215444.

[2] T. T. Duong, T. Brewer, J. Luck, and K. Zander, “A global review of farmers’ perceptions of agricultural risks and risk management strategies,” *Agriculture (Switzerland)*. 2019. doi: 10.3390/agriculture9010010.

[3] G. Žigiene, E. Rybakovas, and R. Alzbutas, “Artificial intelligence based commercial risk management framework for SMEs,” *Sustain.*, 2019, doi: 10.3390/su11164501.

[4] L. Otero González, P. Durán Santomil, and A. Tamayo Herrera, “The effect of Enterprise Risk Management on the risk and the performance of Spanish listed companies,” *Eur. Res. Manag. Bus. Econ.*, 2020, doi: 10.1016/j.iedeen.2020.08.002.

[5] J. Klučka and R. Grünbichler, “Enterprise risk management – approaches determining its application and relation to business performance,” *Qual. Innov. Prosper.*, 2020, doi: 10.12776/QIP.V24I2.1467.

[6] G. Glowka, A. Kallmünzer, and A. Zehrer, “Enterprise risk management in small and medium family enterprises: the role of family involvement and CEO tenure,” *Int. Entrep. Manag. J.*, 2021, doi: 10.1007/s11365-020-00682-x.

[7] M. F. Malik, M. Zaman, and S. Buckby, "Enterprise risk management and firm performance: Role of the risk committee," *J. Contemp. Account. Econ.*, 2020, doi: 10.1016/j.jcae.2019.100178.

[8] L. Bakos and D. D. Dumitrașcu, "Decentralized enterprise risk management issues under rapidly changing environments," *Risks*, 2021, doi: 10.3390/risks9090165.

CHAPTER 8

ALTERNATIVE METHODS AND THE EVOLVING NATURE OF RISK MANAGEMENT

Dr.Krishna Koppa, Associate Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- krishnakoppa@cms.ac.in

ABSTRACT:

In response to the evolving nature of risk management, other methods are developing. Organizations are confronting new and complicated risks as a result of rising globalization, technological development, and a changing economic environment. This calls for a more creative and flexible approach to risk management. Agile risk management is an alternate method to risk management that takes a more dynamic and adaptable stance. Agile risk management include regular risk reassessments, risk prioritization, and risk mitigation strategy adaptations in response to changing conditions.

KEYWORDS:

Economic, Enterprise, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

A good risk effort is destined to evolve and become more complex, just like any management program that is ingrained into how the business functions. Dramatic changes have occurred in the field of risk management, particularly in recent years. Additionally, there has been significant integration of risk management needs into corporate governance. During that period, several new risk management innovations have emerged. Risk management practitioners used to refer to integrated or holistic risk management in the 1990s, but enterprise risk management (ERM) is now the commonly used term for the wide application of risk management throughout the whole business. In a shorter amount of timeperhaps five yearsoperational risk management (ORM) has also been formed and grown quite extensively. The fact that the field of risk management is continually evolving and adapting to new situations may be considered as advantageous in many ways. However, there is a chance that risk management professionals may be seen as conveying a message that is inconsistent since it is always changing.

This is not to say that risk management should become a static discipline, but it is important to keep in mind that senior board members will become confused and lose interest if the basis on which risk management analysis and advice is provided is changed. The global financial crisis and the part risk management played in its emergence must be acknowledged in any analysis of how risk management has evolved. Two themes were often emphasized in newspaper and television stories as the global financial crisis grew: "risk is bad" and "risk management has failed." Both of these claims are untrue. Organizations must take calculated risks, and the failures that contributed to the global financial crisis were due to poor risk management implementation rather than poor risk management in general.

Without a doubt, taking on too much risk may be improper and lead to the downfall of the whole firm. However, many organizations have found that they nearly always manage to get away with it or (at the very least) survive. It is not meant to prevent all audacious strategic choices from being made in light of a thorough grasp of the amount of risk contained in the company. Although risk awareness shouldn't stop a company from pursuing a high-risk plan, the choices will be made with full knowledge of the hazards involved. Businesses should keep looking for chances and sometimes admit when one appears particularly risky but is really very excellent. The company may still be interested in pursuing that risky course of action, but the next phase of the conversation should center on how to manage the risks so that they stay within the organization's risk tolerance and how to measure the risks so that the board is always aware of the actual risk exposure.

It is incorrect to say that risk management fell short during the global financial crisis. It denotes a failure to fully and appropriately implement risk management processes and procedures that reflect a risk-aggressive organization's risk appetite. When a company is risk-averse, there is less room to classify hazards as high likelihood/high impact, which reduces the spectrum of risks that the board will examine. In other words, the organization's risk universe is extremely constrained and will not include hazards that need the board's attention. The organization will identify relatively few high priority substantial risks if it is risk aggressive and follows a methodology that is consistent with. As a consequence, the company will create a "closed universe of risk" for the board, which might limit further in-depth debate and analysis. Being risk aggressive for a company, however, is not intrinsically wrong. The need to repeat risk assessments, question the scope and outcomes of risk analysis activities, and make sure that a highly dynamic approach to risk management is maintained at all times and at all levels in the company increases if a firm is risk aggressive.Other difficult problems for risk management exist in addition to the worries about risk management sparked by the global financial crisis. Though the theories of risk appetite and the upside of risk are worthwhile, additional research is needed before their definitions and their implementation can ensure advantages.

DISCUSSION

Managing New Dangers

Changes in the internal and external environment that result in new possibilities, problems, and uncertainties worry all companies. These modifications might be seen as the new dangers that the company must deal with. However, unless the company has a comprehensive understanding of the types of developing risks it confronts, taking them into account might be challenging. The following three categories may be used to categorize emerging risks: new risks that have evolved in the external environment but are linked to the organization's current strategy; new risks in well-known context. Existing dangers that were previously recognized to the organization but were brought into play by newly formed or altered conditions. dangers that the company has never before encountered since they are related to altered fundamental processes and new dangers in novel situations[1].

Moving into new markets, adopting new technology, and creating more complicated supply chains are just a few recent business innovations that have raised the degree of risk faced by firms. In most cases, the organization itself will have control over these rising dangers. There are also a lot of new or growing dangers that are beyond the control of any one firm. An organization should determine if the risks should be handled as hazard, control, or opportunity risks while trying to manage these rising risks. Many of these new hazards might either be dangers to the business or chances for growth in the future, depending on the actions of the organization. In certain circumstances, the new risks will just add to the existing uncertainties that need to be addressed.

The pace at which new threats might materialize is a crucial factor to take into account. Risk development and change velocity is a term used by certain risk management professionals. Nanotechnology is a prime illustration of an emerging danger. To increase the efficacy of aesthetic treatment of skin disorders, nanotechnology is widely employed in the medical and, to some degree, cosmetics industries. It has not yet been conclusively determined if using nanotechnology would provide any long-term dangers. The adoption of mobile phones is another excellent illustration. Mobile phones are already widely used, but technology has advanced quickly in recent years. Years ago, mobile phone signals were substantially stronger. Therefore, if any health complaints start to surface about the usage of mobile phones, these health impacts are probably related to the outdated technology. Determining whether any health risks no longer exist due of changes in technology or if they are still extant and will turn out to be equally related to current technology will create substantial hurdles[2].

Nanotechnology Risks

As a new subject, there is much discussion on how nanotechnology may affect human health, both positively and negatively. The potential for medical uses of nanotechnology to treat illness and the possible health risks provided by exposure to nanomaterials may be considered separately as two elements of nanotechnology's influence on health. Nanomaterials are considerably easier to absorb by the human body than larger-sized ppapers because of their incredibly tiny size. One of the major problems that has to be overcome is how these nanoppapers react within the body. The size, shape, and surface interaction of nanoppapers with the surrounding tissue determine how they behave. In addition to what might happen if non-degradable or slowly degradable nanoppapers build up in organs, another worry is their potential interaction with biological processes inside the body. Due to their large surface, nanoppapers will immediately absorb some of the macromolecules they come into contact with when exposed to tissue and fluids. It is difficult to make generalizations regarding the health concerns connected with exposure to nanomaterials since there are many factors determining toxicity; each new nanomaterial must be evaluated separately and all material features must be taken into consideration. In the workplaces of businesses that produce or use nanomaterials as well as in the research labs for nanoscience and nanotechnology, environmental and health concerns are intertwined. It is reasonable to assume that nanoppaper dusts cannot be directly regulated by the present occupational exposure regulations for dusts[3].

The Significance of Resilience is Rising

Resilience is a subject that has drawn more attention in recent years. The tendency may have originated with the federal, state, or local governments. In the s and s, it was acknowledged that society in general and communities in particular needed to become more resilient. This growing awareness first surfaced in response to civic situations as well as natural disasters like earthquakes and severe weather. Although thinking about how to react to large-scale catastrophes may have given rise to the first resilience issue, more recent developments have given rise to wider worries.

This description is helpful, however resilience is often related to crisis management, and this definition does not specifically address how an organization behaves in a crisis. The ability of an organization to consistently reach a desired condition after a change in circumstances could be a better description. This term more broadly encompasses both the capacity to effectively handle less spectacular or disruptive occurrences as well as the management of a crisis. Specialists in risk management and business continuity have a chance to collaborate as resilience takes off to provide a more coordinated approach to corporate risk management, business continuity, and crisis management. An organization should adopt the following three habits if it wants to boost its resilience:being aware of changes in the internal, external, and risk management settings to guarantee ongoing focus on resilience. Regarding all forms of resources, including assets, networks, relationships, and intellectual property, one should "prevent, protect, and prepare." In response to disruptive occurrences, one should be able to quickly react, reflect on lessons learned, and adjust.

Finally, it is important to note that it seems as if another trend in the development of risk management and resilience standards is occurring. The 'plan-do-check-act' (PDCA) structure is becoming more and more prevalent in standards. The ASIS standard clearly adheres to the PDCA structure, and this strategy is completely compatible with the plan, implement, measure, and learn (PIML) method to executing a risk management project that is described in Appendix C. Because it is a more complete and analytical method, PIML is favored over PDCA. In reality, after the'mandate and commitment' for the framework and the 'create the context' for the process stages (respectively) have been finished, both the framework and the risk management process are aligned with the PIML method. Advice on building resilience is becoming increasingly commonplace as its relevance is acknowledged more and more. For instance, the guidance given to organizations by the UK government's Cabinet Office is summarized in the box below[4].

Several Methods

The Canadian Criteria of Control (CoCo) framework, created by the Canadian Institute of Chartered Accountants, takes the stance that the organization's risk culture is the most crucial factor. Successful risk management should occur if the risk culture is sound. A person executes a task while being supported by capacity (knowledge, resources, supplies, and abilities) and directed by an understanding of the activity's purpose (the goal to be accomplished). To do the activity successfully over time, the individual will need to feel committed. The individual will keep an eye on both his or her own performance and the surrounding environment to learn how to do the activity more effectively and what improvements need to be made. Any team or workplace group can attest to the same. Control is essentially purpose, commitment, and

capacity, monitoring, and learning in any human organization. The control environment is referred to as the internal environment in the COSO ERM framework. This is comparable to the control environment that the CoCo framework takes into account. In order to identify the elements that need improvement, CoCo offers a systematic method of control environment analysis that permits a quantitative evaluation of the control environment. The following categories are often used to assess the risk-aware culture inside a company using the CoCo technique, despite the fact that there are several CoCo question variations[5].

There are other different risk management and internal control standards available globally in addition to the CoCo strategy. The standards' intended use and scope might differ. For instance, the UK's HM Treasury created the Orange Book as advice for central government agencies on risk management. The notion of Governance Risk and Compliance (GRC) has emerged, and this is viewed as a significant advance in standards. The strategy supporting the principle is based on the idea of the three lines of defense, whereby senior management, specialized risk functions, and internal audit are each given specific internal control and risk management duties. The separation of functions is the cornerstone of the general GRC strategy. Senior management is in charge of the organization's governance, while specialized risk functions are in charge of risk management tasks and providing assurance on sufficient

Internal Audit Provides Compliance

The very important and comprehensive King III corporate governance code was released in South Africa. The amended code maintains the importance of risk management and provides more specific instructions on how to implement it. The management is in charge of designing, implementing, and overseeing the risk management strategy while the board is in charge of risk governance and disclosure. King III outlines specific duties for risk management in regard to the duties of the company's board of directors. There are a variety of specialty standards that apply to risk management in addition to corporate governance requirements and risk management standards. Particularly, the IT industry has given rise to a number of respected and generally used standards. The Control Objectives for Information and Related Technology (COBIT) standard may be the most well-known of the bunch. The tasks are presented in a manageable and logical manner by COBIT, which offers best practices across a framework of domains and processes. The board should make sure that there are procedures in place to guarantee stakeholders get full, timely, relevant, accurate, and easily accessible risk disclosure[6].

Once Annex SL has been approved for standards, the major clause numbers and names of all management system standards will be equivalent. The following clauses make up the framework of management system standards that adhere to Annex SL after the introductory section. It's noteworthy to notice that, unlike how they are described in ISO, the structure does not clearly distinguish framework and process as independent components. Perhaps this explains in part why there are no efforts to convert ISO into the Annex SL format as of right now (November). However, the Annex SL framework allows businesses creating their own enterprise risk management strategies to design a strategy that is consistent with any other ISO standards already in place in the business, including the most widely used ISO standard for quality management.Risk specialists will be acquainted with several of the headings used in Annex SL,

including Clause. Organizational context. The purpose of clause is to explain the organization's purpose. The company must determine all stakeholders and their demands as well as external and internal challenges that may affect its planned results in order to adequately respond to this question. Support is similar to the risk architecture, strategy, and protocols (RASP) in reference to Clause, and to the leadership, engagement, learning, accountability, and communication (LILAC) components of embedded risk management in relation to Clause. The plan-implement-measure-learn (PIML) strategy outlined in this book is precisely equal to improvements. The plan-do-check-act (PDCA) methodology is comparable to the PIML technique and is utilized by many businesses[7], [8].

As the Annex SL format is being implemented, this implies that the obligation to plan and take actions to address risks and opportunities is now integrated within ISO on quality management and will become entrenched into other standards. The key takeaway for risk professionals is to work to ensure that the enterprise risk management program is completely in line with the Annex SL methodology as more management system standards are converted to the Annex SL format. This should increase the organization's willingness to support an enterprise risk management project. The majority of the management system requirements, such as the general process and management that will contain appropriate criteria to regulate the processes, are said to be held by operations. For enterprises that choose to adopt the structure of Annex SL while executing an enterprise risk management effort, the phases of the risk management process would be provided under Clause in the new format[9].

Risk Management in the Future

The book makes many references to the latest risk management trends. Undoubtedly, the creation of the ISO worldwide risk management standard represents a significant advancement for risk management professionals. Additionally, the introduction of improved corporate governance standards has raised the prominence of risk management in many nations. The global financial crisis' repercussions are still being felt, and issues about risk management's role in the crisis' avoidance and why it did not do more to help are still being raised.

The creation of improved reporting standards that are being imposed on companies of all sorts is another significant trend. Organizations that are listed on stock markets all around the globe are notably affected by this. Organizations that employ risk management information systems may profit greatly from their increased sophistication and development. There is still room for inquiry on potential advances in risk management in the future, despite all of these improvements and the practitioners' undeniably rising professionalism and skill. The development of "governance, risk and compliance" (GRC) has been brought up and it is a significant improvement in the way risk management operations are organized. Organizations are now in a better position to practice risk management thanks to the development of GRC and a greater knowledge of the advantages of the three lines of defense. Practitioners of risk management are conscious of the significant contribution their field provides and that risk management operations should be included with other management activities. There is always a chance that risk management and auditing efforts may combine in certain circumstances, turning these three lines of defense into only two.Instead of approaching risk management operations as a distinct management function requiring a

separate set of management information, firms must integrate risk activities across the board. Perhaps this is one of the main drawbacks of the risk register's widespread adoption in many companies. The risk register represents a snapshot of the organization's risk management operations, but there is a danger that it is not continuously examined. The risk register is often a static record that offers little assistance to organizational management. Perhaps the era of the risk register is over, and businesses should instead integrate risk assessment, risk recording, and risk action plans into the management data that is utilized to run their operations on a daily basis[10].

CONCLUSION

In conclusion, maintaining risk management activities that are proportional, aligned, comprehensive, embedded, and dynamic (PACED) is a problem for risk managers and risk management. However, as boards, senior management, managers, and workers become more aware with the theory and practice of risk management, the difficulties of achieving this are growing. The difficulty is in ensuring integration while preventing routineness from overshadowing the significance of risk management. In addition to being related to discussions of business delivery, budgets, and the business growth model, risk management activities also need to be tied to discussions of strategy, tactics, and operations. Management reforms often come and go. A certain strategy temporarily gains popularity before going out of style. Since risk management practices are already required in many industries, it is doubtful that this would ever happen to risk management. The global financial crisis has also prompted a thorough review of the advantages that risk management may provide and how these advantages might be realized. The succinct analysis that follows explains why risk management is important globally and why it is here to stay.

Resilience-based risk management is another alternate method of managing risks. Building organizational resilience to resist possible risks and disruptions is the main goal of resilience-based risk management. This strategy entails identifying crucial resources and operations and creating plans to guarantee their continuance in the case of an interruption. Strategic planning and performance management, for example, are becoming more and more linked with risk management. This integrated approach to risk management acknowledges that risk is a necessary component of attaining an organization's goals and that risk management should be a continuous process that influences decision-making at all levels of the organization. Overall, the evolution of alternative risk management strategies is being driven by the changing nature of risk management. These strategies enable firms to handle the new and complex risks they confront because they are more dynamic, adaptable, and interconnected.

REFERENCES:

[1] P. Rothman-Ostrow, W. Gilbert, And J. Rushton, “Tropical Livestock Units: Re-Evaluating A Methodology,” *Front. Vet. Sci.*, 2020, Doi: 10.3389/Fvets.2020.556788.

[2] A. K. Gupta, S. J. Grannis, And S. N. Kasthurirathne, “Evaluation Of A Parsimonious Covid-19 Outbreak Prediction Model: Heuristic Modeling Approach Using Publicly Available Data Sets,” *J. Med. Internet Res.*, 2021, Doi: 10.2196/28812.

[3] C. Gibson And A. Warren, “Resource-Sensitive Global Production Networks:

Reconfigured Geographies Of Timber And Acoustic Guitar Manufacturing," *Econ. Geogr.*, 2016, Doi: 10.1080/00130095.2016.1178569.

[4] M. R. Juniery Pasciolly, A. Mathur, And A. Seth, "Tctap A-053 Outcome Of Carotid Artery Stenting In Patient With Combined Carotid And Coronary Artery Disease," *J. Am. Coll. Cardiol.*, 2018, Doi: 10.1016/J.Jacc.2018.03.100.

[5] S. Evans, M. Buyse, J. Peron, And D. Follmann, "Invited Session 27-Pragmatic Benefit:Risk Assessment In Clinical Trials: A New Paradigm Using Pairwise Comparison Of Patients," *Clin. Trials*, 2018.

[6] P. M.R.J., M. A., And S. A., "Outcome Of Carotid Artery Stenting In Patient With Combined Carotid And Coronary Artery Disease," *J. Am. Coll. Cardiol.*, 2018.

[7] A. G. Renwick *Et Al.*, "Risk Characterisation Of Chemicals In Food And Diet," *Food And Chemical Toxicology*. 2003. Doi: 10.1016/S0278-6915(03)00064-4.

[8] L. Maciel, R. Ballini, And F. Gomide, "Evolving Possibilistic Fuzzy Modeling For Equity Options Pricing," In *Proceedings Of The 2016 Ieee Conference On Evolving And Adaptive Intelligent Systems, Eais 2016*, 2016. Doi: 10.1109/Eais.2016.7502372.

[9] T. W. Luke, "The Practices Of Adaptive And Collaborative Environmental Management: A Critique," *Capital. Nature, Social.*, 2002, Doi: 10.1080/10455750208565497.

[10] A. Hallunovi And E. Osmanovic, "Factoring As A New Possibility In The Financial Sector," *Int. Sci. J. Monte*, 2019, Doi: 10.33807/Monte.2.201908435.

CHAPTER 9

ROLE OF THE RISK ASSESSMENT CONSIDERATIONS

Dr.Anitha Nallasivam, Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- Dr.anithnalasivam@cms.ac.in

ABSTRACT:

Risk assessment is a crucial step in risk management that entails locating, examining, and assessing possible hazards that might have an influence on an organization's goals. When performing risk assessments, companies must take a number of factors into account to make sure they are thorough and successful. The identification of prospective dangers is a crucial factor in risk assessment. Organizations need to take into account both internal and external issues that might affect their goals. To detect prospective hazards that may not have been previously taken into account, this may include evaluating historical data, industry patterns, and new risks. The probability and possible effect of identified hazards are additional factors to take into account in risk assessment. Organizations must evaluate the chance of each risk being realized as well as any possible effects it could have on their goals. This necessitates a detailed risk analysis and knowledge of the organization's risk appetite.

KEYWORDS:

Economic, Enterprise, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

The risk assessment part of the risk management process is made up of risk identification and risk assessment. In order to identify the most important risks to an organization, project, or strategy, hazards must first be identified and rated. It is described as the total process of risk identification, analysis, and assessment in British Standard BS. Risk assessment is the primary risk management input into the creation of strategy since it focuses on better decision making. Corporate goals, stakeholder expectations, fundamental procedures, and important interconnections all carry potential risks. Risk assessment may be started with any of these aspects as the starting point. Identification of the important risks that might have an influence on the feature of choice is the goal of risk assessment. Risk assessment is crucial, but it is only beneficial if the results are utilized to guide choices and/or identify the right risk mitigation strategies for the particular kind of risk being considered. It need to be seen as the beginning of the risk management process and definitely not as a goal in and of itself.

Choosing whether to analyze the detected risk at the inherent level or the present (or residual) level is a crucial component in conducting a risk assessment. The safeguards that are already in place are not taken into consideration when assessing inherent risk. Internal auditors have suggested taking this course of action. An internal auditor will draw attention to the possibility that two risks with the same current or net value might have vastly varying inherent or gross values. Knowing when this is the case is crucial. The advantage of doing an inherent risk assessment is that the gap between the inherent level and the present level may be found. The

information is utilized by internal auditors to assist identify crucial controls and define audit priorities. This will provide an indicator of the significance of the current control measures. The value of the inherent amount of risk may be quite difficult to determine, despite the fact that this strategy may be effective.

Practitioners in health and safety, for instance, favor doing risk assessments while using the present controls. Although it is based on the presumption that the present controls will always function with the anticipated efficacy, this may be a simpler solution. For instance, the safety person would presume that the enclosure or cabinet is in excellent condition if an evaluation of an x-ray machine is being done, and the risk should be evaluated on that basis. The enclosure or cabinet will be easier for the internal auditor to identify as a crucial control component that has to be subject to regular examination.

Methods for Assessing Risk

When deciding how to do a risk assessment, there are various options available. Who to include in the risk assessment process will be one of the important considerations. The board of directors will sometimes conduct risk assessments as a top-down activity. Individual employees and local departmental management may also be included in risk assessments. This bottom-up strategy is equally beneficial. The chief executive officer's (CEO) viewpoint is crucial, particularly as it aids in defining the organization's general attitude toward risk. Without a doubt, the CEO will be able to provide a well-organized overview of the main dangers that the firm is now facing. The drawback of depending on the CEO's judgment is that external dangers are likely to be highlighted. CEOs will be worried about infrastructural and financial management risks, but these internal risks may not be their main focus or area of interest.

In general, the choice of risk assessment methods will have a significant impact on the organization's entire approach to risk assessments. Specific people must be involved in certain approaches, and risk assessments must be conducted in a specific way. It is critical that the strategy used be in line with the organization's culture. For instance, a workshop may not be the best method for risk assessments if a company doesn't often organize meetings and workshops. Additionally, if the organizational culture places a high value on reports and written materials, doing risk assessments in this manner can be the best option [1].

Voting software use has grown in popularity recently. This may be a highly acceptable method of doing risk assessments for businesses like media corporations who are acquainted with the technology. However, the employment of such technologies may be seen as gimmicks that lessen the value of the workshop by businesses that are not tech-savvy. In the risk assessment workshop, using the voting software may provide extra information. In terms of the possibility and consequences of a danger materializing, it is not only feasible to determine the majority stance, but it is also possible to determine the range of views. A wide range of perspectives should be investigated if they exist since they can indicate a misunderstanding of the danger under discussion.

Whether the risk assessment process should be carried out on a top-down or bottom-up basis is a crucial factor for companies. In other words, would top management oversee the organization's

risk assessment process, passing information to lower levels for confirmation, or will a series of risk assessment exercises begin at the operational level? Gives illustrations of the benefits and drawbacks of doing a top-down risk assessment approach. In a top-down risk assessment exercise, the risks associated with strategy, tactics, operations, and compliance (STOC) are often the main areas of attention.

Gives illustrations of the benefits and drawbacks of doing a bottom-up risk assessment approach. The business should choose the risk assessment protocols and processes that are most appropriate, as with so many other parts of a successful enterprise risk management project. The company should determine if visible senior management backing for the risk management project is more essential than the higher engagement of operational staff if the option is between top-down and bottom-up. In a bottom-up risk assessment exercise, the risks that are classified as compliance, hazard, control, and opportunity in that sequence are more likely to get attention. The risk manager will often conduct a mix of top-down and bottom-up risk assessments, gathering data from as many stakeholders as feasible. The larger time commitment needed from the risk management department to attend and/or organize a series of risk assessment activities is often the biggest barrier to carrying out a bottom-up activity.

Techniques for Evaluating Risks

The whole spectrum of risk assessment methods that may be applied are covered in depth in this standard. The primary methods of risk assessment that are used often are included, along with a short summary of each method. The use of checklists and questionnaires and brainstorming sessions, usually during risk assessment workshops, are perhaps the two most popular risk assessment techniques. The benefit of checklists and questionnaires is that they are often quick and easy to complete compared to other risk assessment methods. The drawback of this strategy is that any danger that isn't brought up by the right inquiries could not be taken seriously. a brief examination of the benefits and drawbacks of the most popular risk assessment methods. Given that risks may be linked to other organizational components in addition to or instead of goals, identifying the primary dependencies that the organization must deal with is a practical and straightforward method to analyze risks. The majority of employees in a company will be able to name the elements of that firm that are essentially crucial to its future success. A list of the organization's essential dependents will emerge from the identification of the elements necessary for success.

After that, key dependencies may be further examined by determining what could have an effect on each one. What may jeopardize each of these crucial dependencies, if a hazard analysis is being conducted?If control risks are found, it is possible to ask: "What may raise doubt about these crucial dependencies?What occurrences or conditions might improve the status of each of the main dependents, according to an opportunity risk analysis?The quantification of risk exposure is crucial for many businesses, and the risk assessment method used must be able to provide the necessary quantification. Financial institutions place a premium on quantification, and the kind of risk management they use is commonly referred to as operational risk management (ORM). The most popular risk assessment method is undoubtedly risk workshops. Discussions on the main dangers the company faces may be held via brainstorming sessions.

Each danger is seen and understood by everyone. The consequence of this, however, is that the older individuals in the group could dominate the discourse and it can be awkward and unwanted to disagree with them [2].

Several brainstorming models are often used in risk assessment workshops to facilitate organized dialogue. Depending on the degree of risk analysis needed, they may be qualitative or quantitative. The SWOT and PESTLE analyses are the two most often used qualitative brainstorming frameworks. A SWOT analysis examines the organization's advantages, disadvantages, opportunities, and threats. By analyzing opportunities in the external environment, the SWOT analysis has the advantage of taking the upside of risk into account. The SWOT analysis's ability to be connected to strategic choices is one of its advantages. There is a chance that not all of the hazards will be discovered, however, as there is no organized procedure for classifying risks.

The PESTLE study, which takes into account the political, economic, social, technical, legal, and ethical (or environmental) hazards posed by the business, is another typical qualitative technique. More information about the PESTLE risk categorization system. PESTLE is a tried-and-true framework for conducting brainstorming sessions during risk assessment workshops, with outcomes that can be seen. Many businesses may want to do a quantitative assessment of the likelihood that a risk event will occur. These quantitative analyses may be carried out using a variety of ways. Hazard and operability (HAZOP) studies and failure modes and effects analysis (FMEA) are the two most popular. These two methods are organized ways that make sure no dangers are overlooked. However, in order to conduct a precise quantitative study, a broad spectrum of expertise must be included. Manufacturing processes are the best candidates for using HAZOP and FMEA methodologies. Hazardous chemical plants and intricate transportation infrastructure, such as railroads, are often the subject of HAZOP investigations. HAZOP investigations are often conducted on complicated facilities, including as nuclear power plants. They may also be used to analyze a product's safety. These are both quite analytical and time-consuming procedures, yet they will be required in a variety of situations [3], [4].

Description of the Risk Matrix

The company must grade a risk after it has been determined to be substantial in order to determine the priority significant hazards. Although there are established methods for grading risks, it is also necessary to determine if there is room for future control improvement. Another factor that aids in the precise identification of the most major risks is examination of the potential for future cost-effective improvement. The risk probability and impact metrics that will be used throughout the enterprise must be established by the organization. a typical set of terms related to risk probability. provides impact definitions that are appropriate for usage in a normal organization. Four separate meanings are offered in both situations, preventing any inclination for participants in a risk assessment exercise to choose the middle choice. However, many businesses choose to provide more than four possibilities, both in terms of possibility and consequence. Depending on the organization's nature, size, and complexity, there may be a variety of possibilities [5].

The risk matrix comes in a wide variety of designs. The most typical form is one that illustrates the connection between the risk's chance of materializing and its effect, if it does. On the risk matrix, other aspects of the risk may be represented in addition to probability and effect. For instance, a risk matrix is often used to illustrate the potential for achieving greater risk improvement. The risk matrix in this situation will show the risk's level in relation to the extra steps that can be done to better manage that risk and, as a result, establish a target level for it. The conclusion of the risk assessment exercise may be recorded in the risk matrix, which will provide a straightforward visual representation of the key hazards that have been recognized or detected. Ranking the risks in accordance with the organization's risk appetite or predetermined risk criteria is also required when conducting a risk assessment exercise. If a risk has the potential to have an effect that exceeds the benchmark criteria for significance for that category of risk, it is considered substantial. During a risk recognition exercise, it will be decided which hazards are possibly important. It is essential to choose the:

1. The size of the eventuality, should the danger come to pass.
2. The extent to which the incident would affect the organization.
3. Probability that the danger will manifest at or above the benchmark.
4. Potential for additional control enhancement.

This will enable the prioritization of the important risks to be clearly identified. The majority of firms will discover that there are between and total hazards identified in a workshop. It is usual for the company to identify the number of priority major threats it faces when the risk evaluation is complete. Although many risk practitioners refer to this as the risk severity, the language used in ISO combines the likelihood and effect of a risk to determine the degree of risk. There are other more formulations that define concepts used to describe probability and effect. Depending on its size, makeup, and complexity, an organization will need to create its own definitions. Outlines general definitions of probability in terms of how often an event is likely to occur over the course of a year. Contains impact criteria that might be used in a hospital setting where patients' safety is the top priority [6].

Risk Awareness

It is common for various workshop participants to have varying perspectives on the risk while engaging in risk assessment activities. Divergent viewpoints may be accommodated in a variety of ways. Voting software may be used in various circumstances to determine the position held by the majority. This has the advantage of being an easy way to determine the viewpoint held by the majority of the group while also showing the range of perspectives. However, it is often helpful to go through the reasons why various individuals evaluate a danger in different ways. Finding a consensus on a shared stance is often feasible by examining the reasons why their opinions are different. This will have the advantage of leading to the identification and use of more suitable control measures. Individuals' perceptions of danger will be influenced by a variety of circumstances.

At various levels of seniority within the company, differing perspectives on the significance of a risk may exist. It helps the risk assessment process to get input from all levels of management so

that various risks may be seen from different angles. Better risk communication, a deeper knowledge of risks, and the selection of suitable and workable control mechanisms are all advantages of this method. A thorough understanding of the company is necessary to comprehend the dangers it faces and to carry out an effective risk assessment. It takes a lot of time and resources to perform an effective risk assessment that accurately identifies the important risks before moving on to determine the necessary controls. Members of the public often only have access to limited information on risk perception and are exposed to persuasive arguments from lobbying and other special interest groups. As a result, the public's knowledge and perception of risk may not be accurate or completely impartial. It is the responsibility of journalists and news reporters to portray news items objectively and impartially, which may be challenging when the audience is unaware of all the hazards [7].

Stance Toward Risk

uses a common risk matrix to provide an empirical representation of risk attitude. It illustrates the risk-averse organization's attitude toward risk. An increasing number of risk attitude matrices include four components. The Cs of comfort, cautiousness, concern, and criticality might be used to symbolize these parts. The organization's long-term approach to risk is reflected in its risk mindset. The four components of a risk appetite matrix may also have these adjectives linked to them to define the strategy for taking short-term risks. It is explored how risk appetite and risk attitude are related. There are fewer dangers that warrant concern for a risk-aggressive firm, therefore the board's 'universe of risk' will be highly constrained. Internal auditors often refer to the "universe of risk" when determining audit priorities. Working within such a small or constrained "universe of risk" increases the likelihood that the company will be affected by a substantial risk that has not yet been detected. Every stakeholder will have a unique "universe of risk," and the risk manager is likely to have a "universe of risk" that consists of all hazards that have previously been recognized as well as any developing risks that have just begun to surface.

Shows that there will be a certain amount of risk that the company is willing to accept and include into its fundamental procedures. This is due to the fact that, regardless of the risk's chance of occurring, it would have a negligible effect even if it did. Similar to the last example, there is a chance that a danger would manifest that is so unlikely that it is presumed it won't happen, even though it would be quite severe if it did. For instance, the majority of businesses do not take into account the effects of a jumbo aircraft crash-landing on their property. The global financial crisis is an example of a situation in which certain dangers were seen as being so improbable that they could be disregarded. Although some banks were dependent on the wholesale money markets, it was thought that the likelihood of these markets collapsing was too remote to warrant additional investigation or the creation of backup strategies for handling it [8].

A variety of dangers may develop over these minimal thresholds of acceptable probability and effect. In general, low likelihood/low impact risks are manageable, medium likelihood/medium effect risks need significant thought before acceptance, and high likelihood/high impact risks are intolerable. A set of "risk criteria" may be used to represent an organization's general attitude toward risk, and this is the method used by ISO. It is important to note that ISO does not specifically address risk appetite; instead, it discusses risk criteria. There are similarities between

the attitude toward food and the desire for food at a specific moment, but it might be difficult to distinguish between risk appetite and risk attitude. While hunger for food indicates an urgent need to eat, attitude toward food refers to a set of established or medium- to long-term requirements. The same methodology may be used to determine risk, with risk appetite being the more pressing need to accept risk in order to accomplish goals and risk attitude representing the defined risk criteria. When determining whether a risk is acceptable, organizations must consider each risk separately. As a sign of their attitude toward risk, various businesses will establish tolerance limits in different ways. The enterprise risk management strategy has a component known as a cumulative evaluation of risk, which is a practice used by many firms. After that, the business may evaluate if its total risk exposure is acceptable and compatible with its risk-taking stance. The fact that some people might be more concerned about a low-impact risk with a high probability of occurrence (like a car crash) than they will be about a high-impact risk that is unlikely to occur (like an earthquake) is important to consider when thinking about risk attitude, perception, and appetite. This methodological variation may have an impact on how important risks are prioritized throughout the risk assessment process.

Asking how probable it is that each risk will manifest above the threshold test for significance once all the potentially important hazards have been discovered is one method. Following that, the dangers might be ranked as high, medium, and low probability. The alternate strategy is to rank the potentially important hazards according to effect and probability. The hazards will then be broken down into three categories: high, medium, and low impact. These techniques vary in terms of attitude and perception. The first method is based on the likelihood that a risk will be considerable, while the second method is based on the effect a risk will have if it materializes. Neither of these techniques is superior to the other, and a board member's (or the whole board's) preference for one over the other may depend on their attitude toward risk as expressed in the organization's risk criteria. The effect that a risk will have on finances, infrastructure, reputation, and/or the marketplace (FIRM) is often used to quantify its impact. The effective management of high impact events' effects on the organization's strategy, tactics, operations, and compliance (STOC) is one of the key prerequisites for risk management [9].

The dangers of purchasing an automobile

Consider the choice to purchase a vehicle as an example that combines the concepts of risk appetite with hazard, control, and opportunity risks. The amount of money that will be invested in the chance to own a new vehicle, risk tolerance, and acceptance of uncertainty must all be taken into consideration when choosing which automobile to purchase. These elements together describe the risk tolerance needed to purchase and operate an automobile. The upside of accepting the risk of purchasing a vehicle depends on whether the advantages outweigh the expenses.

The desired advantages of automobile ownership should be determined if doing a risk-based assessment of purchasing a car is to assist with the decision-making process. This is the same as figuring out the goals connected to owning an automobile. It's important to take into account your real financial capability and aptitude to maintain a vehicle. The purchaser of a new car must ensure that the choice of vehicle won't result in more danger or expense than expected.

Insurance, breakdown, repairs, accidents, service expenses, insurance, as well as the purchase price and the projected yearly depreciation, are dangers connected to car ownership. Assume that a two-year-old, high-end vehicle has been chosen for purchase. The cost of the automobile will be far lower than that of a brand-new car, as well as the potential costs associated with depreciation. However, the cost of repairs and upkeep might be more expensive than for a brand-new car (manage hazards). For the majority of automobiles, the risk of accidents, theft, and repair costs will be comparable. Keep in mind that the opportunity risks increase the likelihood of achieving the advantages of automobile ownership. The hazard risks prevent obtaining these advantages, whereas the control risks raise ambiguity or doubt over accomplishing them [10].

CONCLUSION

Organizations must also take into account how well current measures are working to manage identified risks. This entails evaluating the effectiveness of current controls in reducing recognized risks and identifying any holes or weak points in the control environment. Another aspect of risk assessment is the effect of risk interdependencies. Risk interactions between one another and their possible effects on an organization's goals must be taken into account. The possible effects of outside factors like modifications to regulatory standards, technology breakthroughs, or political unrest must also be taken into account by organizations. Organizations must make sure they are appropriately prepared to handle these risks since these external occurrences might have a big influence on their goals. Overall, a deep and detailed awareness of possible risks and their potential effects on an organization's goals is necessary for successful risk assessment. Organizations may create a successful risk assessment process that allows them to manage risks pro-actively and effectively by taking into account the important factors mentioned above.

REFERENCES:

[1] L. Yu-Seong, L. Byung-Joon, and C. Yun-Young, “Flood Risk Assessment in Consideration of Regional Characteristics,” *J. Korean Soc. Environ. Technol.*, 2021, doi: 10.26511/jkset.22.5.10.

[2] S. M. Mahon, “Cancer risk assessment: conceptual considerations for clinical practice.,” *Oncology nursing forum*. 1998.

[3] S. Mestdagh *et al.*, “EFSA Guidelines on the environmental risk assessment of genetically modified animals in the EU: The process and risk assessment considerations,” *J. fur Verbraucherschutz und Leb.*, 2014, doi: 10.1007/s00003-014-0898-4.

[4] S. P. Teo, “Fall risk assessment tools-validity considerations and a recommended approach,” *Ital. J. Med.*, 2019, doi: 10.4081/itjm.2019.1196.

[5] J. W. Shevach, A. B. Weiner, R. N. Kasimer, C. H. Miller, and A. K. Morgans, “Risk Assessment and Considerations for Proper Management of Elderly Men with Advanced Prostate Cancer: A Systematic Review,” *Eur. Urol. Oncol.*, 2020, doi: 10.1016/j.euo.2020.03.006.

[6] N. J. Hewitt *et al.*, "Use of human in Vitro skin models for accurate and ethical risk assessment: Metabolic considerations," *Toxicol. Sci.*, 2013, doi: 10.1093/toxsci/kft080.

[7] H. Checkoway, P. S. J. Lees, L. D. Dell, P. R. Gentry, and K. A. Mundt, "Peak exposures in epidemiologic studies and cancer risks: Considerations for regulatory risk assessment," *Risk Anal.*, 2019, doi: 10.1111/risa.13294.

[8] F. Welle and R. Franz, "Microplastic in bottled natural mineral water–literature review and considerations on exposure and risk assessment," *Food Addit. Contam. - Part A Chem. Anal. Control. Expo. Risk Assess.*, 2018, doi: 10.1080/19440049.2018.1543957.

[9] S. Xu *et al.*, "Multiclassification method of landslide risk assessment in consideration of disaster levels: A case study of Xianyang city, Shaanxi Province," *ISPRS Int. J. Geo-Information*, 2021, doi: 10.3390/ijgi10100646.

[10] B. N. and Y. Athave, "Artificial Intelligence: Risk Assessment and Considerations for the Future," *Int. J. Comput. Appl.*, 2019, doi: 10.5120/ijca2019918529.

CHAPTER 10

DISCUSSION ON RISK CLASSIFICATION SYSTEMS

Dr Hemanth Kumar.S, Assistant Professor, Department of General Management,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id- dr.hemanth_kumar@cms.ac.in

ABSTRACT:

Systems for classifying and ranking risks according to their possible consequences and chance of occurring are an essential part of risk management. Organizations can efficiently manage resources thanks to risk categorization systems, which make sure that risks with the biggest potential effects get the most attention and resources. The three-level approach, which classifies hazards as high, medium, or low, is one of the most widely used risk categorization systems. A high potential impact and a high chance of occurrence are characteristics of high-risk events, whereas a moderate potential impact and a low likelihood of occurrence are characteristics of medium-risk events.

KEYWORDS:

Economic, Enterprise, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

The categorization of risks into short, medium, and long term despite the fact that it is not a codified system helps to identify hazards as being tied (mainly) to operations, tactics, and strategy, respectively. Although this difference is not exact, it may help with subsequent risk categorization. Strategic core processes will in reality face certain short-term risks, and operational core processes may face some medium- and long-term risks as well. Additionally, maintaining conformity with operations, tactics, and strategy is always necessary. The aim to reduce this kind of risk informs the attitudes of the majority of corporations toward compliance risks. A short-term risk has the potential to have an immediate negative effect on the goals, critical dependencies, and core operations. When the incident happens, these risks may instantly impair operations. Hazard hazards make up the majority of short-term risks, however this is not always the case. These risks may also be linked to cost control in the company, albeit they are often linked to unforeseen disruptive occurrences. The capacity of the company to sustain effective and efficient core processes that are concerned with the continuity and monitoring of everyday activities is often impacted by short-term threats. Risks associated with the near future must be reduced[1].

A medium-term risk has the potential to have an effect on the organization sometime after the incident. Figure 1 illustrates how the effects of a medium-term risk often become evident months or at most a year after the incident, rather than immediately. The capacity of the company to sustain effective and efficient core processes that are involved with the management of strategies, projects, and other change programmers is often impacted by medium-term risks. These medium-term hazards are often connected to initiatives, strategies, improvements, and other advancements. These intermediate-term dangers must be managed. A long-term risk has

the potential to affect the organization after the occurrence of the event. The effect often happens one to five years (or more) after the occurrence. Long-term risks often have an influence on the organization's capacity to sustain the key procedures related to the creation and implementation of effective and efficient strategy. Although these risks have to do with strategy, they shouldn't be seen as being only tied to opportunity management. More value may be lost due to risks that might jeopardize a strategy's effectiveness than could any risks to operations or tactics. Despite the fact that long-term risks might destabilize a company, it is important to accept the proper degree of risk as part of the plan.

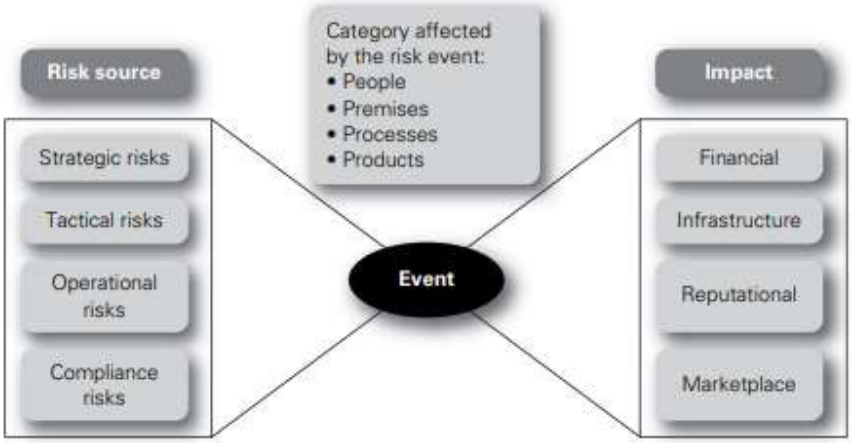

Figure 1: An illustration of risk management with a bow tie.

Dangers that are present over the short, medium, and long timeframes depending on their source. The organization's operations, tactics, and strategy all carry dangers. Since compliance risks are a separate category from operations, tactics, and strategy, they are also covered for the purpose of completeness. Embrace, manage, mitigate, and minimize (EM) are the appropriate responses to risks depending on whether they are caused by strategy, tactics, operations, or compliance (STOC). The bow-tie risk management graphic serves to highlight how risk factors might trigger unfortunate occurrences.

A hazard event will affect the aspects of the organization that may lead to disruption when it happens. Due to this, the event shown in the bow tie's center would be mentioned according to the organizational component that it has an influence on. These elements include people, locations, operations, and goods (Ps). It's important to remember that the Ps may also be used to categorize risks. These days, risk management is often represented with a bow tie. demonstrates how the three components of risk source, incident, and effect are represented by a bow tie. Risk sources are classified as strategic, tactical, operational, or compliance in this high-level representation. The FIRM risk scorecard is used to represent impacts, as shown in Table. .The event, as indicated by the organizational component that will be affected by the event, is at the center of the bow-tie.

Techniques For Classifying Risks in Nature

A system for risk identification is necessary in order to identify all of the hazards that a business faces. The organization can locate comparable hazards inside the organization by using formalized risk categorization methods. The company may determine who should be in charge of developing a plan for managing related or comparable risks thanks to the classification of risks. The organization will be able to determine the risk appetite, risk capacity, and overall risk exposure better in regard to each risk, set of related risks, or generic kind of risk by using suitable risk categorization.

There are several risk categorization methods available, but the FIRM risk scorecard offers this framework. The FIRM scorecard expands on the many facets of risk, including the impact's timeframe and type, whether it's a danger, control, or opportunity, as well as the organization's total risk exposure and risk capacity. The FIRM scorecard's categories allow for the categorization of risks as largely being of a financial, infrastructural, reputational, or market nature. The FIRM risk scorecard may be used as a model for identifying organizational goals, expectations of stakeholders, and, most crucially, significant dependencies. The scorecard is a crucial complement to the risk management methods and tools that are already in use. It is created by examining the potential effects of each risk on the major dependencies that underpin each fundamental activity. Utilizing the FIRM risk scorecard makes it far less likely to miss a serious risk, which supports thorough risk assessment [2], [3].

The company must choose which risk categorization method best meets its goals and criteria, as with many other risk management considerations. Risks may be categorized not only by the duration of their effect, but also by the type of the risk, the source of the risk, the nature of the impact, and/or the extent and nature of the repercussions. The risk categorization system that is most suited to an organization's size, nature, and complexity will be chosen by that company. For instance, banks and other financial organizations typically often divide risks into three categories: operational, credit, and market risks. The SWOT and PESTLE analyses are two additional frequently used risk categorization methods that may be utilized to build risk assessment workshops. Instead of the high-level overview provided, an operational version of the bow-tie depiction of risk management employs the bow-tie to symbolize the various causes of property damage and keeps the repercussions as financial, infrastructural, reputational, and market-related. The probable causes of property destruction include flood, fire, earthquake, and break-in.

Many businesses have trouble finding an effective method of risk categorization. This often occurs as a result of inadequate consideration being given to the nature of the risks that are being categorised. The risk management process is shown with a bow tie to show how risks may be categorized based on their source, the area of the company that is affected by the event, and the effect and/or consequences of the risk materializing. The operational, tactical, and strategic risks that the organization is exposed to are represented by the short-, medium-, and long-term categorization of hazards. According to the part of the organization that is affected, the kinds of disruption to organizations outlined in use a categorization scheme. This is the risk categorization system for people, premises, processes, and products (Ps).

The many risk classification systems classify hazards in ways that are comparable to one another. The FIRM risk scorecard refers to operational risk as infrastructure risk, for example, thus there are distinctions there as well. COSO has a limited perspective on financial risk and places a strong focus on reporting. The categories will be similar but not identical since the various systems were created by various organizations under various conditions. demonstrates that many classification systems include a mix of source, event, effect, and consequences categories when discussing various risk categorization methods.

the benefits of having a method for classifying risks. These advantages include offering the option to aggregate risks of a similar kind throughout the whole business, assisting in defining the scope of risk management inside the company, and providing a structure and framework for risk identification. The ISO makes no recommendations for a system of risk categorization. In conclusion, some benefits of using a risk categorization system include:

It is simpler to recognize risk accumulations that might jeopardize a crucial reliance or corporate goal and render them susceptible. Risks may be categorised to make it easier to determine who is responsible for better managing each category of risk. More organized and knowledgeable decisions may be made on the sort of control(s) to be imposed. Situations where the organization's risk appetite is being exceeded (or when the risk criteria are not being applied) are easier to spot.

According to the British Standard, the organization's size, purpose, character, complexity, and context should all be taken into consideration when deciding how many and what kind of risk categories to use. The maturity of risk management within the company should also be reflected in the categories. The risk categorization methods provided by the COSO ERM framework and the IRM risk management standard may be the most often utilized ones. The COSO risk categorization method, however, has a number of flaws and is not always useful. Strategic risks, for instance, may also be present in operations, reporting, and compliance. Despite these flaws, the COSO framework is widely used since it is the accepted and advised method for adhering to Sarbanes-Oxley Act obligations.

Risk Scorecard for FIRM

The FIRM risk scorecard's four sections provide a framework for categorizing the risks to the organization's most important dependencies. Every business should be concerned about its finances, infrastructure, reputation, and market performance, which is another principle reflected in the categorization system. The headings of the FIRM risk scorecard are as follows to offer a wider scope to commercial success:

1. F: Financial;
2. I: Infrastructure;
3. R: Reputational;
4. M: Market Place.

Reputational and market risks are seen as internal to the company whereas financial and infrastructural threats are external. Also, although reputational and infrastructural risks are more

difficult to assess, financial and market risks may be simply defined in monetary terms. Not everyone agrees that reputational risks should be included in the FIRM risk assessment as a distinct category of risk. It is often suggested that reputational risk should not be treated as a distinct risk category since reputational risk results from the occurrence of other hazards. However, if risk is viewed more broadly, it becomes clear that reputation is crucial. This is crucial for businesses looking to achieve "brand stretch," as it is commonly referred to, which is when they leverage their brand name to penetrate new areas. In any event, there is a more general claim that risks are a result of bigger business choices. There are risks associated with choosing a certain strategy, starting a project, and/or carrying on with current activities. Risks would not exist if the company did not carry out certain strategic, tactical, or operational operations.

For the examination of external hazards, the PESTLE risk categorization system is often considered to be the most pertinent. In this context, the term "external risk" refers to a situation beyond the organization's direct control, but one in which risk mitigation measures may be done. A SWOT analysis of the organization's strengths, weaknesses, opportunities, and threats (SWOT) is often advised in combination with the PESTLE risk categorization system. The PESTLE risk categorization method has the benefit of offering a clear understanding of the problems that need to be solved in the context of the external environment. Because the PESTLE method's external elements are so pertinent, the public sector may be where the PESTLE approach is most useful.

Cultural norms and expectations, population growth rate, age distribution, career attitudes, safety focus, and global warming are sociological factors. Technology developments that affect your goods or services, new technology, entrance hurdles in certain industries, and financial considerations like supply chain and outsourcing. Legal amendments to laws that may have an influence on things like taxes, import/export restrictions, quotas, resources, and jobs. Environmental and ethical considerations, even if many of these components will be social or economic in nature [4].

Regulation, Risk, Control, and Opportunity

It is not always beneficial to classify hazards using a single risk categorization scheme. Understanding the impact's timeframe alone may not be adequate, particularly if the impact's type is more significant. Because of this, using a straightforward approach to classify risks will always provide challenges. Each company must decide which risk categorization system(s) best fits its own requirements and the types of risks it faces. Risks must be categorized in accordance with their source, their effect, and their timeline. Consequently, a full picture may be provided by combining the FIRM risk scorecard with the categorization of risks as hazard, control, and opportunity risks. A personal risk matrix may be created that categorizes hazards according to the FIRM risk rating and also specifies whether they are short-term, medium-term, or long-term. This will provide a problems grid in an easily understandable manner that will help with the identification of all potential important concerns. The challenges that a person can encounter are shown in a finished grid example, allowing the dangers to be recognized [5].

Many risk categorization methods fail to take compliance issues into proper consideration. Risks may be divided into three categories: hazards, controls, and opportunities, as well as long-, medium-, and short-term risks. Because compliance hazards may not always fit into a categorization system based on timelines, it is possible that they will not be discovered if one of these classification methods is utilized. Because a trigger event is often necessary, compliance concerns therefore provide another challenge. In other words, a company may face a variety of compliance risks, but it may be difficult to pinpoint the specific compliance issue that would cause a problem. the proportion of operational, tactical, and strategic concerns for each of the four FIRM risk scorecard areas. It is clear that hazard risks are directly tied to infrastructure problems, while strategic risks are more likely to relate to market-related problems [6].

Additionally, organizations may create specialized risk categorization systems that are catered to their unique requirements and goals. This can include adding new classifications, including emerging risks or strategic risks. The accuracy and efficacy of the risk assessment process determine how well a risk categorization system works. Before classifying possible risks, organizations must make sure they have a complete grasp of them and their potential effects [7].

Organizations can efficiently prioritize risks and manage resources thanks to risk categorization systems. Organizations may create focused risk management strategies that allow them to manage risks pro-actively and effectively by classifying risks based on their potential impact and probability of occurrence [8].

With the exception of the IRM standard and the COSO framework, which provide strategic risk as a distinct risk category, the risk categorization methods covered in this paper may most readily be used to the study of hazard risks. Whether or not having a category of strategic risks is beneficial and required will be up to the company. The FIRM risk scorecard provides a way to categorize strategic and project or tactical risks based on the primary effect of the risk, should it come to pass. To choose the best course of action for each risk, categorization of hazards affecting projects is crucial, just as it is for other fundamental organizational functions. These elements provide a way to categorize project risks since the prerequisites of any project are that it should be completed on time, under budget, and in accordance with specifications. hazards that endanger the project's timetable, budget, and final specification, as well as hazards that will impact the project's performance or quality, might all be listed separately.

There is no universal risk categorization scheme that all kinds of enterprises may use. The many risks that banks are exposed to are often broken down into three primary categories: market risk, credit risk, and operational risk. For various kinds of hazards, a distinct risk management framework and architecture will often be used. Market hazards are dangers brought on by changes in the financial markets. The bank's assets and liabilities are susceptible to a variety of market volatility factors, including fluctuations in interest rates and currency exchange rates. The bank accepts market risk largely as an opportunity risk.

The credit risk is the probability that the money the bank owes to a customer will not be repaid. Simply put, credit risk is the potential for an unfavorable circumstance in which the customer does not repay the loan amount. It must be addressed largely as a control risk. Operational risk is

related to internal system, process, technology, and human failure as well as external hazards like fires and natural catastrophes. Operational risk is described by Basel II as "the risk of direct or indirect loss resulting from insufficient or failing internal processes, people, and systems or from external events." The necessity to quantify operational risk exposure, growing use of technology, and acknowledgement of the crucial role played by humans in financial sector operations have all raised the prominence of operational risk. Operational risk must be reduced since it mainly involves hazards.

CONCLUSION

In conclusion, risk classification systems are important tools that enable organizations to effectively manage risks and make informed decisions. By using various factors to assess the likelihood of a certain risk event occurring and the potential impact it could have, risk classification systems help organizations prioritize and allocate resources towards risk mitigation efforts. There are several types of risk classification systems, ranging from simple to more complex models, and each has its strengths and weaknesses. Organizations need to carefully consider their unique needs and goals when selecting a risk classification system that best fits their situation. Furthermore, it is important to note that risk classification systems are not foolproof and do not guarantee perfect risk management. These systems are only as effective as the data and assumptions that underlie them, and they should be continually reviewed and updated to reflect changes in the environment.

Overall, risk classification systems are valuable tools that can help organizations identify and prioritize risks, allocate resources effectively, and make informed decisions. However, they should be used in conjunction with other risk management strategies and should not be relied on as the sole means of managing risk.

REFERENCES:

[1] R. L. Kumar And S. Park, “A Portfolio Approach To Supply Chain Risk Management,” *Decis. Sci.*, 2019, Doi: 10.1111/Deci.12332.

[2] Q. Zhou, A. B. Li, Z. Q. Lin, And H. Z. Zhang, “A Nomogram And A Risk Classification System Predicting The Cancer-Specific Survival Of Patients With Initially-Diagnosed Osseous Spinal And Pelvic Tumors,” *Spine (Phila. Pa. 1976).*, 2020, Doi: 10.1097/Brs.0000000000003404.

[3] M. S. Irwin *Et Al.*, “Revised Neuroblastoma Risk Classification System: A Report From The Children’s Oncology Group,” *J. Clin. Oncol.*, 2021, Doi: 10.1200/Jco.21.00278.

[4] O. Vardar, C. Zhang, I. Canbulat, And B. Hebblewhite, “A Semi-Quantitative Coal Burst Risk Classification System,” *Int. J. Min. Sci. Technol.*, 2018, Doi: 10.1016/J.Ijmst.2018.08.001.

[5] Z. Tu, C. Li, T. Tian, And Q. Chen, “A Risk Classification System Predicting The Cancer-Specific Survival For Postoperative Stage Ib Non-Small-Cell Lung Cancer Patients Without Lymphovascular And Visceral Pleural Invasion,” *Lung Cancer*, 2021, Doi: 10.1016/J.Lungcan.2021.09.014.

[6] O. Akbilgic, M. R. Langham, A. I. Walter, T. L. Jones, E. Y. Huang, And R. L. Davis, "A Novel Risk Classification System For 30-Day Mortality In Children Undergoing Surgery," *Plos One*, 2018, Doi: 10.1371/Journal.Pone.0191176.

[7] B. Zhao *Et Al.*, "The Assessment Of Different Risk Classification Systems For Gastrointestinal Stromal Tumors (Gists): The Analytic Results From The Seer Database," *Scand. J. Gastroenterol.*, 2018, Doi: 10.1080/00365521.2018.1515319.

[8] H. Doi, K. Kuribayashi, K. Kitajima, K. Yamakado, And T. Kijima, "Development Of A Novel Prognostic Risk Classification System For Malignant Pleural Mesothelioma," *Clin. Lung Cancer*, 2020, Doi: 10.1016/J.Cllc.2019.08.003.

CHAPTER 11

A BRIEF DISCUSSION ON RISK ANALYSIS AND EVALUATION

Dr.R.Satish Kumar, Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.satishkumar@cms.ac.in

ABSTRACT:

Critical elements of the risk management process include identification and assessment of possible hazards to an organization's goals via risk analysis and appraisal. Risk assessment includes defining the right risk response and evaluating the magnitude of the risks, while risk analysis entails identifying prospective hazards, their probability, and their impacts. The risk matrix is one technique that is often used for risk analysis and appraisal. Organizations may identify risks based on their probability and possible effect using the risk matrix, a visual tool. This makes it possible for businesses to prioritize risks and create specialized risk management plans. Scenario analysis is yet another method for analyzing and evaluating risks. The process of scenario analysis is creating a variety of possible outcomes and evaluating each one's possibility and potential effect. This makes it possible for enterprises to recognize potential risks, estimate their effect, and create suitable risk solutions.

KEYWORDS:

Economic, Enterprise, Magnitude, Risk Matrix, Risk Management, Organizations.

INTRODUCTION

The degree of risk that a certain occurrence represents to an organization may be easily shown via the use of a risk matrix. The standard method for displaying the residual or current level of risk is a risk matrix. The net risk is another name for this. The vertical axis will often be referred to as effect when the risk matrix is used to show the present degree of risk. The gross or inherent level of risk, which is the amount of risk before controls are imposed, may also be represented using the risk matrix. The vertical axis of the risk matrix may sometimes be labeled magnitude when it is being used to show the inherent amount of risk.

Consequences are thought of in a somewhat different way. Impact is a term used to describe the organization's total degree of risk. The conceivable outcomes will result in this degree of risk or effect. As a result, the word "consequences" is used in a more general sense to convey additional information about the risk and how well it is being handled. A warehouse fire, for instance, might result in a significant loss with a large magnitude. The financial effect should be low if the company is adequately covered. However, if for instance more stakeholders in the area are impacted and the organization's image is harmed, the fire's effects might be serious.

the variety of problems that a person can encounter. Individuals would be able to determine the most important hazards they face in order of importance by using this "issues grid." The risk matrix depicts these dangers. The relative significance of the risks may be quickly determined

when the different hazards have been arranged on a risk matrix. The risk profile (or risk exposure) may then be evaluated in its whole to see if it falls within acceptable bounds and is compatible with the person's risk tolerance and capability. A risk matrix is a common tool used by large enterprises to summarize their risk profile. The risk matrix is quite helpful and has many potential uses. The sort of risk response that is most likely to be utilized may also be determined using this method. effect is not the same as magnitude since even if an event may have a large magnitude in terms of size, the effect and repercussions may be less severe. Another illustration: A road transport firm could completely lose one of its cars, yet, depending on the specifics, this might have relatively little overall effect on the organization. This will be particularly true if the business did not have enough business to fully use the particular kind of vehicle involved in the loss.

Risk Level, Both Present and Inherent

Many risk management experts evaluate risk at its present level, often known as the residual level. Internal auditors, on the other hand, like to evaluate the risk at its base level. Because there are benefits to taking into account a risk's inherent level when doing a risk assessment. It will be possible to determine how each control measure will affect the situation by taking into account the inherent level. the impact of restrictions on risk level. Control is an already-in-place measure that lowers risk from its inherent level to its present or residual level. It is clear that this control primarily affects the risk's chance of materializing. To lower the risk from the present level to the desired level, a new control will be implemented.

It is meant to have a substantial influence on the risk's impact but minimal impact on the chance that it will manifest. On the risk matrix, there are three categories of risk that are significant. The amount of risk that would exist if there were no controls in place is known as the inherent or gross level. The risk's current level, when just Control is in place, is the level at which it is present at the time of the risk assessment. The residual level is another name for this. The issue with using the term "residual level" to describe the present level of risk is that it implies that the level of risk is static and that the company is unable to adopt any more risk mitigation measures. The word "current level" is used often in this book because it gives the risk management process a much more dynamic sense. However, risk managers are more interested in the goal level of risk. Control is introduced in an effort to lessen the effects of risk so that the goal level of risk is contained inside the tolerate/comfort zone, which is the bottom left quadrant of the risk matrix [1].

Health and safety professionals often refer to the notion of reducing risk to a level that is "as low as reasonably practicable" (ALARP) when establishing the goal level of risk. One of the cornerstones of risk management for health and safety hazards is ALARP. It is preferable to manage risk until the advantages of adding more controls outweigh the costs, rather than until it is completely removed. Definitions of probability and impact must be agreed upon by the organization. Low, medium, high, and extremely high may all be used to categorize probability and impact. Depending on the kind of risk and the size, nature, and complexity of the organization, many businesses will need to be more precise than these general definitions. It is more crucial for an organization to define low, medium, high, and extremely high effect since

impact is used to characterize the spectrum of consequences. The benchmark test of significance and the criteria of impact utilized should be consistent.

Controlled Assurance

the desired outcome of a certain control measure. An organization cannot have complete assurance that controls will always be completely implemented and as effective as needed or desired. To have assurance that the control chosen has been correctly developed, implemented, and has the expected impact, controls must be audited. On a risk matrix, the degree of control confidence may also be shown. Greater result variability may be anticipated if the efficacy of a control is unknown. Using a circle or ellipse to represent a risk on a risk matrix instead of a single point on the matrix may show how this is to be done. By doing this, it is possible to indicate the degree of uncertainty or variability in the result in relation to both the probability and effect of the event occurring. The degree of trust that should be put in a given control should be taken into account when conducting a risk assessment and when assessing the success of risk management in general and risk control measures in particular. Internal audit's job is to test controls where there is little trust in their efficacy and to offer details on the expected degree of result variability, should a risk develop [2].

Internal auditors are in charge of ensuring that the right controls have been chosen and are operating properly in actual operations. When examining these criteria, internal auditors use the terms "effective" and "efficient" controls, respectively. In this book, the terms effective and efficient are also used in regard to the fundamental business operations. Internal audit plays a significant role in carrying out the testing of controls, and risk management professionals should also be aware of the significance of this task.

Management must be informed that there is enough control, and this information might come through management reports, internal auditing operations, or measurements of the results of projects and activities. The risk management paperwork should specify who is in charge of creating and implementing controls as well as assessing their efficacy and efficiency. In Paper, the relevant reactions to control and opportunity risks are discussed. Decision-making with regard to opportunities is defined in terms of the Es, which are options for reacting to opportunity hazards. It's vital to remember that although these answers are shown as the dominant or most probable response in each quadrant, some situations may call for the need of another response in addition to or instead [3], [4].

Depending on the situation, different and/or more replies may be necessary. For instance, high-impact/high-likelihood hazards may be impossible to prevent if they are included into mission-critical tasks. The firm won't be able to eliminate such hazards in this situation. The Ts of risk response are shown in a very straightforward risk matrix, however it is difficult to display since they meet in the middle. Since a little adjustment in a risk's possibility and effect might move it from the terminate quadrant into the tolerate quadrant, it is obvious that it cannot be as straightforward as indicated. This study is made more realistic by using a slightly modified technique.Being required to hold onto a risk that is known to be beyond of the organization's risk appetite or even risk capacity is a practical challenge for many businesses. For instance, despite

the fact that all practicable safeguards have been put in place, a firefighting authority may nevertheless have to accept situations in which firefighters would be exposed to a critical degree of danger that the organization must endure. It is typical to implement enhanced risk monitoring if businesses must accept risks that are at the critical level. This will allow the business to implement any improved controls as soon as they become available at the earliest opportunity.

Risk Importance

When doing a risk assessment, it is extremely normal to find 100 or more hazards that might have an influence on the goal, primary procedure, or crucial reliance under consideration. There are too many hazards to handle, thus a strategy is needed to cut down on the amount of risks that will be prioritized by management. A test for risk significance is necessary so that an organization can focus on substantial risks. the kind of benchmark testing that may be used to determine if a risk is serious is suggested. The benchmark test will probably be focused on financial or commercial value for risks that may have an effect on such areas. A benchmark test focused on the effect, expense, and length of the interruption is suitable for risks that might affect the organization's infrastructure or regular operations. The most probable benchmark for reputational risks will be based on the negative publicity that would be generated if the risk materialized. Depending on the kind of risk and whether it is a financial or non-financial risk, this may change. Finding a financial test of significance for big businesses may be done in a variety of ways. The test for risk significance should be consistent with the permission levels, which are often outlined in a formal document known as a "delegation of authority," since many firms will have authorization processes for spending money.

If a major company, complete board approval may be necessary for expenditures beyond a specific financial level. This shows how much money the organization views as important, according to the data. Other evaluation criteria include a proportion of the projected annual earnings or a percentage of the balance sheet (or reserves) value of the firm. Typically, testing for significance should be performed using percentages of yearly profit, balance sheets, or turnover. To determine if a risk is considerable in regard to the financial and marketplace risk sectors of the FIRM risk scorecard, financial limitations might be utilized. It can be more challenging to find a benchmark test for importance for the infrastructural and reputational components. Asking if the risk would interfere with daily operations for longer than, say, half a day, is one way to gauge the magnitude of infrastructure hazards.

The test for relevance for reputational hazards may be to examine how the occurrence would be reported. An paper that appears on the top page of a local or national newspaper may be a notice that a danger needs to be taken seriously. It's conceivable that an organization's external auditors may state that they will regard an amount of £million to be a considerable sum while completing the organization's books. Even though it could be a little less than the computation above, this would provide management of the firm advice to use that sum as the benchmark test of significance. The number of hazards that would need to be further considered might be reduced to approximately by using this test during a risk assessment workshop. Finding the likelihood that each of the potentially major risks would materialize at or above the financial threshold level would be the next step. The outcomes might be recorded and shown using a risk matrix [5].

Risk Tolerance

When a company decides how much risk to accept, there are a number of factors that are crucial. Different strategies will be used for various hazards. Control risks will lead to a control acceptance, opportunity risks will lead to an investment appetite, and hazard risks will lead to a hazard tolerance. The company will be exposed to all risks overall. This represents the entire amount of risk that the organization has assumed across all three categories. There will obviously be compliance hazards, although the majority of firms work to reduce these risks by integrating the required compliance controls into core operations [6].

The real risk that the company is incurring is known as risk exposure, and it may not be the same as the risk appetite that the board considers to be suitable for the firm. The risk capability of the company is yet another significant risk indicator. This gauges the level of risk the company should or can afford to accept. All of these methods of risk analysis have to be in line with how the company views risk. Simply said, the board's appetite for risk should be higher than or equal to the actual risk exposure that the business confronts, while being within the risk capacity of the organization. Certain financial institutions were exposed to a degree of risk that exceeded their ability to tolerate risk, which contributed to the global financial crisis.

A project that might use up all of an organization's resources would not be suitable. The organization's ability to tolerate risk will be influenced by its financial stability, the quality of its infrastructure, the strength of its reputation and brands, and the level of market competition in which it competes. The firm must have a bigger capacity for risk availability the faster the market is changing. The strategic alternatives may be constrained, for instance, if a business is dealing with a big shift in technology. When it becomes clear that streaming technology is taking control, think about a business that produces DVD players. The firm will have to create a new business model and deal with a big risk brought on by the shift in technology. It will need to develop new production tools, expertise, and distribution strategies. It's possible that the organization's resources and risk tolerance may not adequately cover the hazards associated with the organization's transition to the new technology. If such is the case, the company may need to investigate its strategic choices, such as looking for a joint venture partner, finding a buyer for the company, or just exiting the market. A concrete illustration of the effects of the global financial crisis is shown in the box below. The financial institution under discussion found that its risk exposure was higher than its risk tolerance. The financial firm subsequently issued a statement to shareholders after acknowledging the circumstance [7].

In this instance, the bank is making it quite obvious that its exposure to risk surpassed both the organization's risk appetite and its risk capacity. Organizations will often be put in situations where they must deal with dangers that, if they materialize, may be fatal. Some organizations could be subject to a number of distinct, even independent threats, any of which might be fatal. The task for the risk management function in these situations will be to concentrate on the conditions that might cause one or more of these hazards. In the scenario in the box, the bank was fortunate enough that none of the events that would have destroyed its balance sheet occurred as a result of the conditions that may have arisen [8], [9].

CONCLUSION

Based on its earnings power, the bank determines its risk capacity as the amount of risk it believes it can take on without harming its ability to pay dividends, implement its strategic initiatives, and, ultimately, maintain its reputation and continuous economic viability. It is based on a mixture of planned, predicted, and historical income and expense that have been modified for variable compensation, dividends, and associated taxes. Based on present and projected risk positions across the three main risk categories operational risk, business risk, and primary risks—risk exposure is an estimate of the possible loss.

The statistical loss metrics employed in the daily operational controls are expanded upon as far as practicable. When combining possible losses from risk positions in several risk categories to get an overall evaluation of the risk exposure, correlations are taken into consideration. A severe but conceivable constellation of events occurring over a one-year time horizon is used to evaluate the risk exposure. The board determines risk appetite and establishes an upper limit on total risk exposure. To determine if existing or planned risk limitations are reasonable, risk exposure and risk capability are compared. It is one of the instruments at their disposal to help management make choices on changes to the risk profile.

Normal risk exposure limits should not be exceeded, but this connection has not maintained in the current, exceptionally challenging market circumstances. The bank's significant net loss demonstrated that the risk exposures continued to exceed its risk capacity. Due to a lack of liquidity in the markets for securitized assets and much higher levels of volatility in international markets, risk exposure remained high. The considerable write-downs on risk positions and the reduction in risk exposure brought about by sales were countered by a concurrent decline in risk capacity brought on by lower-than-anticipated profit expectations as a result of the worsening economic outlook.

REFERENCES:

[1] M. Wulan And D. Petrovic, “A Fuzzy Logic Based System For Risk Analysis And Evaluation Within Enterprise Collaborations,” *Comput. Ind.*, 2012, Doi: 10.1016/J.Compind.2012.08.012.

[2] G. Montibeller And A. Franco, “Decision And Risk Analysis For The Evaluation Of Strategic Options,” *Support. Strateg. Fram. Methods Model.*, 2007.

[3] C. Zhang, B. Wang, S. Yang, M. Zhang, Q. Gong, And H. Zhang, “The Driving Risk Analysis And Evaluation In Rightward Zone Of Expressway Reconstruction And Extension Engineering,” *J. Adv. Transp.*, 2020, Doi: 10.1155/2020/8943463.

[4] J. H. Hall, “Risk Analysis And Evaluation Of Capital Investment Projects,” *South African J. Econ. Manag. Sci.*, 2001, Doi: 10.4102/Sajems.V4i2.2650.

[5] E. Kepenek And Z. Gençel, “A Tool For Comparative Disaster Risk Analysis And Evaluation In Urban Areas (Draes),” *Acad. Res. Community Publ.*, 2018, Doi: 10.21625/Archive.V2i3.361.

[6] R. Wirtz And M. Heisel, “Model-Based Risk Analysis And Evaluation Using Coras And

Cvss," In *Communications In Computer And Information Science*, 2020. Doi: 10.1007/978-3-030-40223-5_6.

[7] M. N. Nuriyev, J. Mammadov, And J. Mammadov, "Renewable Energy Sources Development Risk Analysis And Evaluation: The Case Of Azerbaijan," *Eur. J. Econ. Bus. Stud.*, 2019, Doi: 10.26417/Ejes.V5i3.P11-20.

[8] P. Cardoso, M. Flávia, And S. Kelen, "Risk Analysis Evaluation Of Piroxicam 20mg Capsules Manufacture Process By Fmea Technique," *Int. J. Drug Regul. Aff.*, 2018, Doi: 10.22270/Ijdra.V6i1.215.

[9] G. B. Bãbuţ, R. I. Moraru, And C. Dura, "Conceptual And Methodological Framework For Risk Analysis And Evaluation On Seveso Industrial Sites (Ii) Critical-Comparative Study And Development Of New Approaches Regarding The Risk Analysis And Evaluation Methods," *Qual. - Access To Success*, 2015.

CHAPTER 12

DISCUSSION ON LOSS MITIGATION AND RISK PROBABILITY

Dr.R.Satish Kumar, Professor, Department of Marketing,
CMS Business School, JAIN Deemed to-be University, Bangalore, India,
Email Id- dr.satishkumar@cms.ac.in

ABSTRACT:

Danger probability reveals how often a danger is anticipated to manifest. Additionally known as risk frequency. However, using "risk frequency" implies that the danger happens often. This book uses the broader phrase risk probability. Risk probability may be calculated on an inherent basis for every specific risk or at the present level of risk while taking into account the implemented control measures. History may provide a useful indicator of how probable a danger is to materialize in the case of hazards. A fleet of motor vehicles will inevitably have a history of mishaps and failures. There will be measures in place to lessen the possibility of these occurrences. A road haulage business should determine the probability of vehicle failures based on both intrinsic factors and existing controls.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Assessing the inherent risk of vehicle accidents is challenging, however, since it requires making assumptions about how the absence of controls may affect the chance of accidents. The organization will still need to examine how important the vehicle maintenance program is in reducing vehicle breakdowns and if the maintenance operations are cost-effective even if an evaluation of the breakdown probability at the inherent level cannot be done. The corporation could have driver-training policies in place with regard to auto accidents, and once again, the efficacy of these policies can be assessed by analyzing inherent and present levels of risk. Benchmarking the fleet's performance against the average performance of the industry will be a beneficial exercise whether risk levels are assessed at an inherent or present level.

The usage of seat belts in automobiles is an example of a control measure that affects the risk's size but may not affect its probability. Simply said, because the seat belt has no influence on the chance of an accident happening, the driver wears one to lessen the impact of one. The seat belt is worn by the driver as a safety precaution in case of an accident. A sports team will want to lessen the likelihood that a crucial player will be missing. It's possible that a player's improper conduct led to the absence, in which case consequences must be applied to that individual. As a result, the club could opt to establish a senior players' "code of behavior" that would require each player to commit to leading a proper, healthy lifestyle. Financial and other penalties would apply if the code of conduct was broken. The club may also determine that extra measures, like as fitness monitoring and social assistance for foreign players who have just arrived to the nation to join the squad, are necessary to decrease player absences. It may also be accepted that efforts

should be taken to set contractual restrictions on national teams' capacity to use their foreign players. These steps will be performed in addition to other loss prevention measures, such as providing outstanding medical facilities to provide timely medical attention and lessen the effects of injuries. Additionally, the business may buy insurance to shield itself from the monetary damages brought on by a player's absence.

The Level of Risk

It's crucial to minimize danger risk's severity. The inherent seriousness of the risk, should it come to pass, is sometimes referred to as magnitude for hazard hazards. Reduce the effect and subsequent events when the unfavorable event takes place to lessen the total hazard risk. A seat belt in a vehicle may lessen the effects of an accident, but it has no influence on how likely an accident is to occur. A major fire that causes a significant amount of property damage and is regarded as being very severe and costly is conceivable. To lessen the effect of a significant fire on an organization's finances, infrastructure, reputation, and market (FIRM), however, is necessary to lessen the intensity of the fire. The focus of impact-reduction measures will be on cost containment after the incident and damage limitation during the fire. The effects on the organization's strategy, tactics, operations, and compliance (STOC) are referred to as the repercussions. Loss control is focused with minimizing the severity, repercussions, and effect of an unfavorable occurrence[1].

Damage control is another crucial element of reputational risk management. An company must be able to safeguard its image after a major occurrence that garners media attention by ensuring stakeholders that it handled the situation responsibly. When there has been a catastrophic train or aircraft catastrophe, it is nearly always the case that the CEO or chairman of the corporation will attend to the site. There have been instances when a severe event has happened and the organization's handling of the media has been appalling. In these situations, it's possible that little thought was given to pre-event preparation, resulting in a failure to successfully reduce the harm to the organization's image at the time the incident happened. Cost reduction will also need to be a consideration for organizations. The business continuity plan (BCP) or disaster recovery plan (DRP) that the company put in place before the catastrophe happened is often the foundation for cost minimization after an event. The company will be in the best position to guarantee that the incident's total cost is kept as low as feasible if appropriate BCP and DRP are developed.

Control of Hotel Fires

Perhaps it's not surprising that developments in sprinkler systems have been a defining feature of recent years given the sustained focus on the danger of fire. The introduction of the suppression mode sprinkler has been the single most spectacular advancement in the field of fire. Standard sprinklers operated in control mode, keeping the fire under control until help could come and extinguish it. The fire may spread and emit a lot of smoke. The goal was to suppress the fire rather than merely manage it as hotel fixtures were increasingly vulnerable to smoke and water damage. The improved sprinklers led to less fire-affected areas, less smoke, and less destruction. Technology for sprinklers has advanced substantially. We now have early-suppression, fast-response sprinkler heads where there was just a single normal spray sprinkler head. Sprinkler

systems are being used in workplaces with low fire risks, such offices and nursing homes, as well as in more conventional industrial operations. Corporate involvement in loss prevention initiatives increased. For instance, hotels conducted two projects in the early s to demonstrate the effectiveness of plastic pipe in hotel room sprinkler systems. Prior to the successful testing, iron pipe was used for sprinklers, which proved more challenging to install than plastic and required that rooms be out of use for days while a re-fit was being done.

Danger

Fraud, health and safety, property protection, the effective functioning of IT systems, and accidents with the potential to harm reputation are among the hazards threats where minimizing the severity of the adverse event is crucial. Using the FIRM risk scorecard's framework, a list of the major dependencies that might result in hazard risks is provided. When hazard hazards manifest, steps must be taken to lessen their effect and severity while also reducing their size. Although loss avoidance will be the major emphasis of hazard risk management, effective hazard risk management also needs to take cost containment and damage limitation into account. In the insurance industry, there is a growing tendency toward handling claims in a way that is both efficient and economical. The motivation for this tendency is in part to push businesses to resume regular operations as quickly as feasible. In fact, some insurance providers refer to these kinds of programs as "cost containment." As was already indicated, lessening the impact of an event should be seen as a component of an organization's broader effort to adopt loss control. Because it will allow the firm to manage both the possibility and effect when a hazard risk materializes, an integrated approach to loss control is crucial. In actuality, cost conservation, damage mitigation, and loss prevention should all be included in loss control [2].

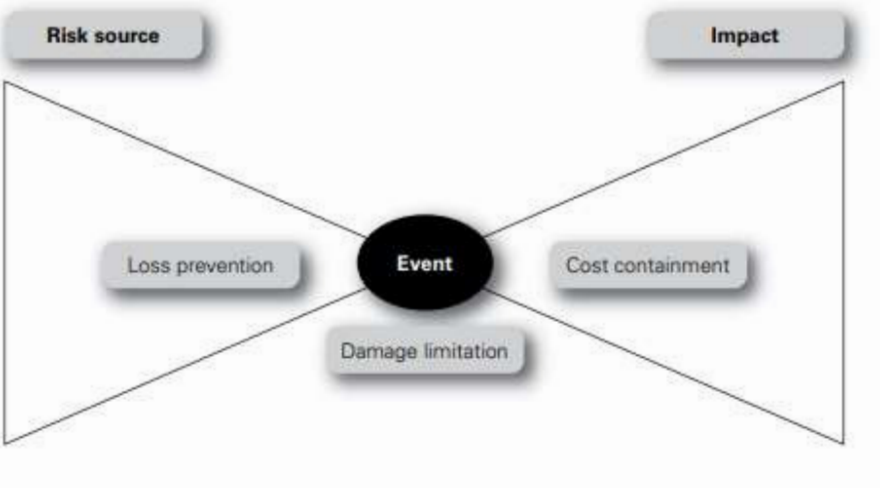

Figure 1: Loss control and the bow-tie.

Figure 1 illustrates that, despite companies' best efforts, hazards may still arise even if loss prevention is the most crucial aspect of loss management. Risks and hazards must be properly assessed in order to prepare appropriately for pre-loss, during-loss, and post-loss activities. Plans should be in place to guarantee that the incident's harm is kept to a minimal and that its financial repercussions are properly managed and limited. The three elements of loss control may be

represented by a bowtie. The company will have measures in place before the incident happens to try to avert loss. As the incident unfolds, precautions should be taken to reduce the harm that it is creating. After the incident, plans to lower repair costs and maintain business continuity should be triggered in order to limit costs. Plans for disaster recovery will be important at both the phases of cost control and damage limitation. More consideration is given to the connection between the three loss control components and the kind of control that will be chosen. Preventive, corrective, directive, and detective hazard controls are the several kinds that are detailed in Paper.

Loss Mitigation

Another approach to look at loss control efforts is as loss prevention, which will also be concerned with minimizing the amount of an event that does occur, is about decreasing the chance of an unfavorable event happening. The goal of damage limitation is to lessen the impact of the event when it does occur. If steps that can be taken when the event is really happening are planned, damage control will contribute more effectively. Cost containment aims to lessen the event's effects and repercussions. Cost containment will be concerned with getting repairs done for the least amount of money possible as well as with business continuity strategies to make sure the company can keep running when an asset is damaged.

Depending on the kind of risk posed by the hazard that is being assessed, different loss prevention strategies will be used. Loss prevention for hazards to health and safety relates to ceasing the activity altogether or making sure that, for instance, dangerous substances are no longer employed. Loss prevention approaches for threats to buildings include measures like the removal of ignition sources and the management, containment, and segregation of flammable or combustible items. Loss prevention strategies will also include smoking bans and other measures to lessen risky behavior among visitors to the facilities. Loss prevention strategies for fraud and theft concerns will include task separation and security labeling of pricey objects. Pre-employment screening is another fraud prevention approach. Risks to health and safety as well as fraud prevention are discussed in greater depth [3].

Damage Control

Damage control in connection to fire risks is widely known. Sprinkler systems are often thought of as a loss prevention strategy, but they are really the main control method for making sure that a fire only causes little damage when it starts. The use of fire shutters, the usage of fire segregation inside structures, and well-practiced systems in place to remove, separate, or otherwise preserve priceless assets are further damage-limitation variables connected to fire. After the fire at Windsor Castle, plans were made right once to evacuate priceless artwork from parts of the castle that had not yet been damaged by the fire. Despite the substantial attention given to health and safety regulations and other loss prevention measures, workplace accidents nevertheless happen. A clear damage control strategy is to provide proper first aid arrangements, and most businesses provide acceptable first aid facilities. There may be on-site emergency care options and even medical facilities for certain high-risk industry occupations. These medical institutions may sometimes have specialized facilities for treating patients connected to the

specific dangers present. Providing cyanide antidotes at companies where chromium plating is done using cyanide-plating solutions is one instance. The availability of emergency eye-wash bottles in situations where dangerous chemicals are handled is a more straightforward example [4].

In the Gulf of Mexico, the Deepwater Horizon oil disaster has taught us numerous risk management lessons. One of the major problems was how long it took to halt the oil leak. In order to stop the oil leak from happening, loss prevention procedures were put in place, and cost containment measures were adopted to control the cost of clean-up, recovery, and business continuity. It's possible that the damage control methods were not as effective as they should have been. Since the oil leak persisted for a few weeks, there was time to implement damage control procedures. However, it doesn't seem as if these actions had been thoroughly thought out in advance [5].

When a danger of a hazard materializes despite the steps made to minimize loss and to limit damage, it may still be necessary to mitigate the event's financial impact. For instance, meticulous plans for salvaging and plans for decontaminating specialized objects that have sustained water or smoke damage are two actions for reducing expenses connected with major fires. Making plans for specialized recovery services will also fall under cost containment in regard to a fire. Business continuity, disaster recovery, and crisis management plans, where necessary, should all include information on the steps that will be done to ensure that post-incident expenditures are kept to a minimum. Planning for business continuity and catastrophe recovery are subjects that are taken into consideration. What insurance firms refer to as "increased cost of operation" is another factor that should be taken into account when attempting to manage costs after an event. The majority of business interruption and property insurance coverage will cover additional operating costs. This might happen if a company has to outsource certain production tasks, or if it needs to do manufacturing tasks at a different factory that can be far away[6]–[8]. A company must take a variety of steps if it learns that defective products have been sold on the market. Prior to the incident, the company had to have created procedures for informing consumers of the existence of defective products on the market and how to spot them. The relevance of product recall in these situations is discussed in the box below.

CONCLUSION

In conclusion, risk likelihood and loss control are crucial ideas in the risk management process. Creating and putting into action strategies to avoid or reduce losses brought on by prospective hazards is known as loss control. A variety of loss prevention strategies are available to organizations, including risk avoidance, risk reduction, risk retention, and risk transfer. On the other hand, risk likelihood entails determining the possibility that a danger will materialize. This necessitates a detailed risk analysis and knowledge of the organization's risk tolerance. Organizations may identify risks, prioritize them, and create specialized risk management plans by evaluating the probability of prospective hazards. The reliability and accuracy of the risk assessment process determine how well loss control measures work and how well risk probability is assessed. Before designing loss control strategies and determining risk probability, organizations must make sure they have a complete awareness of prospective risks and their

potential effects. Effective loss control and the evaluation of risk possibility are crucial steps in the risk management process. Organizations may manage risks proactively and effectively, safeguarding their goals and limiting possible losses by establishing and putting into place effective loss control measures and determining the probability of prospective hazards.

REFERENCES:

[1] T. T. Duong, T. Brewer, J. Luck, and K. Zander, "A global review of farmers' perceptions of agricultural risks and risk management strategies," *Agriculture (Switzerland)*. 2019. doi: 10.3390/agriculture9010010.

[2] K. K. Karanth, A. M. Gopalaswamy, R. DeFries, and N. Ballal, "Assessing Patterns of Human-Wildlife Conflicts and Compensation around a Central Indian Protected Area," *PLoS One*, 2012, doi: 10.1371/journal.pone.0050433.

[3] Y. Wang and A. Sebastian, "Community flood vulnerability and risk assessment: An empirical predictive modeling approach," *J. Flood Risk Manag.*, 2021, doi: 10.1111/jfr3.12739.

[4] J. M. Mol, W. J. W. Botzen, and J. E. Blasch, "Risk reduction in compulsory disaster insurance: Experimental evidence on moral hazard and financial incentives," *J. Behav. Exp. Econ.* , 2020, doi: 10.1016/j.socec.2019.101500.

[5] C. Stockdale, Q. Barber, A. Saxena, and M. A. Parisien, "Examining management scenarios to mitigate wildfire hazard to caribou conservation projects using burn probability modeling," *J. Environ. Manage.*, 2019, doi: 10.1016/j.jenvman.2018.12.035.

[6] M. Nones, "Dealing with sediment transport in flood risk management," *Acta Geophys.*, 2019, doi: 10.1007/s11600-019-00273-7.

[7] N. Suray, E. Karpenko, M. Dubovik, Y. Shlyenov, and F. Sterlikov, "Risk management at educational institution," *Entrep. Sustain. Issues*, 2019, doi: 10.9770/jesi.2019.7.1(26).

[8] D. Elana, "Risk Management Process in Projects," *Rev. Gen. Manag.*, 2019.

CHAPTER 13

STUDY ON IDENTIFYING THE BENEFITS OF RISK

Dr Yavana Rani.S, Associate Professor, Department of Decision Sciences,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id-dr.yavanarani@cms.ac.in

ABSTRACT:

As it entails recognizing possible possibilities that may result from taking risks, defining the upside of risk is a key concept in the risk management process. The "risk-reward" trade-off, where companies must weigh possible costs and rewards of taking risks, is often referred to in this context. To determine the upside of risk, one method is to do a risk opportunity analysis. This entails locating possible possibilities that could result from taking chances and evaluating how they might affect the goals of the company. Organizations may create a risk management plan that optimizes the potential upside of risk by taking into account both the possible rewards and potential costs of taking risks.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

One of risk management's biggest issues is defining the upside of risk. In general, risk management contributes to the delivery of legal duties, assurance, improved decision-making, and effective and efficient core operations. Risk management professionals do, however, want to pinpoint a wider variety of advantages that may be brought about by effective risk management. These are often the unanticipated or larger than anticipated advantages of risk management. The term "upside of risk" may be interpreted in many different ways, and some of them are shown below. Practitioners of risk management hold the conviction that risk management has a positive impact on how the business runs, and they often refer to this impact as the upside of risk. Simply said, when the advantages from taking the risk outweigh any benefits that would have come from not taking it, the upside of risk has been realized. In other words, by engaging in the activities that exposed it to the risk or set of hazards involved, the company as a whole has benefited. By selling the undesirable by-product or finding a way to give the waste product more value and sell it as another product stream, for instance, a manufacturing business that creates waste by-products that pose a disposal issue may profit from the risk. This is an example of finding a business challenge and resolving it to get extra advantages that weren't anticipated and weren't otherwise accessible.

In plain English, the benefit of risk can simply be the payment for taking it in the first place. The benefit of taking that risk comes when the climber has successfully reached the peak and receives that reward. Climbing a difficult mountain may be risky. Another strategy is to state that risk management aims to get the greatest results while minimizing uncertainty or volatility. If this concept of risk management is adopted, then attaining the objectives of the company by accepting the risks that were built into the strategy, tactics, and/or operations that were engaged

is the upside of risk. The upside of risk may also be interpreted as meaning that the risk assessment workshop should concentrate on finding hazards that might have a positive consequence. Therefore, the risk assessment workshop would cover issues such as: "What circumstances might result in a better outcome than anticipated?A list of upside risks may then be created, and steps can be done to increase their likelihood of happening and/or to improve their effect and consequences when they do. The ability of the company to engage in activities that it would not otherwise be motivated to do so provides a more gratifying account of the upside of risk. In a corporate sense, this enables a company to take advantage of a business opportunity that a rival does not want to accept or thinks is too risky. This may be as a result of the organization's higher efficiency or the discovery of a development project that could change the organization at a low cost that the rival company had overlooked. On a strategic level, the firm may discover a way to target the business potential but just the profit part of that opportunity, which might result in this upside of risk.

Consider a commercial initiative that was successful under conditions where failure was possible as another way to see the positive of risk. This approach to the upside of risk relies on the company being willing to pursue a risky venture, even with adequate controls in place, that results in a positive outcome in circumstances where a competitor may not have been willing to take the risk. It is somewhat retrospective in nature and is based on the analysis: "that could have gone wrong, but it did not, and therefore we have enjoyed the upside of taking that risk."

The examination of the upside of risk, which considers the advantages of having a strong risk management procedure, is the last step. A risk management strategy may be regarded necessary in order to achieve the MADE advantages, particularly those associated to statutory requirements. In these conditions, some firms can see obtaining compliance with legal requirements as an upside of risk. The upside of risk is, to put it simply and especially in respect to hazard risks, that there is less potential for harm. Senior managers may not be persuaded to endorse a risk management project for this reason, however. The chance to explore a business opportunity that rivals would be hesitant to accept is perhaps the simplest to understand and appealing idea. Saying that rivals would be too risk-averse to pursue such a high-risk opportunity would also be a contributing factor in the reasoning. The prevalence of the positive aspects of risk has caused issues for those who practice risk management. From reduced potential negative to structured opportunity management, the range of assessments is broad and lacks emphasis. Such a broad and vague collection of ideas and strategies won't sway an organization's board of directors. It is obvious that the discipline of risk management has to get a deeper understanding of the benefits of risk and convince the board of that.

There may be room for the risk management guidelines to adopt a more unified strategy toward the upside of risk. Some risk management guidelines follow the strategy of expanding the four Ts to include the fifth T, "take the risk" and "become the Ts." The established rules sometimes miss the fact that a business will take an opportunity and reap the desired benefits rather than consciously taking a risk for its own purpose. A person who saw an opportunity and seize it is shown in the narrative in the box below. Except inasmuch as it was inherent in seizing the chance, he did not seek out, accept, or take the risk. It is true that those who are seen as taking

risks are really those who are prepared to go for possibilities that other people would view as being too dangerous. Their actions show that they are seizing the opportunity, not necessarily that they are relishing the dangers involved.

Opportunity Evaluation

If the company conducts opportunity evaluations, it will be more likely to successfully seize commercial prospects. Many consulting companies thoroughly assess each potential new client. The company will examine the new possibility and assess the potential for a profitable collaboration, additional revenue prospects, and the reputational advantages of having that prospective client as a client. Both new clientele and new company endeavors are candidates for opportunity evaluation. The goal of this opportunity review is to locate any potential new business prospects that may result from acquiring that customer. The study will also include any possible drawbacks of obtaining the customer prospect effectively. The chance that the company will inform the customer prospect that they do not want to submit a bid for the business must exist while doing such an opportunity evaluation.

Think about the possibilities available to a theater that notices less people are attending shows and chooses to look into ways to charge those who do continue to come more money. The alternatives may include general enhancements to the theater's catering services and the availability of organic foods in the theater's restaurant. There is also the potential to offer goods that are related to the specific performance. The theater may examine sponsorship agreements and engage in conversations with nearby companies in addition to looking at increased income from performances to determine what kinds of productions are most likely to get local support and sponsorship. In the future, an assessment of the degree of potential sponsorship might be part of the appraisal of any proposed new production. This strategy may increase revenue while also allowing the theater to present shows that would have been deemed too risky in the past[1].

Even though it may not be expressly recognized as a risk management strategy, opportunity management is being used by many firms. Opportunity management should ideally be integrated into processes for formulating and executing strategy and tactics, as well as for seizing business opportunities. Some businesses lack specific opportunity management processes for evaluating merger and acquisition possibilities as well as new business prospects. Many firms conduct a risk assessment workshop to discover and analyze opportunities and dangers simultaneously while looking for opportunities. demonstrates how a risk matrix may be used to document the results of such a risk assessment session. One example or explanation of how to record the output from the risk assessment workshop should be the precise design of the risk matrix and the descriptors of probability and consequence, which will differ across businesses.

The necessity for a diverse group of individuals to attend a risk assessment session that covers both opportunities and risks poses one issue. Opportunities tend to be connected with strategy and tactics, while hazards often pertain to operations and compliance. Similar to hazard risks, opportunities must be identified and analyzed before being evaluated and the actions or controls that must be taken are determined. The opportunities that have been found, examined, and noted

on the risk matrix will need to be subjected to the opportunity assessment technique mentioned previously in this section[2].

Index of Risk

A company's risk profile may be portrayed in a variety of ways. The most typical approach is to create a risk registry with information on the key risks it confronts. The risk register's main drawback is that it often only provides a qualitative assessment of specific threats. The overall risk exposure of an organization has to be measured, evaluated, and quantified by the organization. The creation of a comprehensive understanding of the organization's risk exposure is one of the characteristics of the enterprise risk management methodology. The method used to assess and quantify risk in operational risk management is similar to the method used to determine an organization's overall risk exposure. 'Riskiness index' is a concept that is introduced in this section. The goal is to provide a semi-quantitative strategy that provides a glimpse of the organization's overall degree of embedded risk. The organization's present strategy, ongoing initiatives, and the nature of everyday business activities are all taken into consideration when determining the overall degree of risk. This strategy may provide a chance to evaluate the effectiveness of risk management and monitor ongoing changes.

a series of inquiries that may be used to the creation of an organization's riskiness index. The categorizes hazards using the FIRM risk scorecard's organizational framework. An organization should be able to determine the amount of risk to its finances, infrastructure, reputation, and level of risk in the market by utilizing the riskiness index. The company may next look for additional controls to lower the degree of risk after completing the riskiness index. Therefore, the primary goal of risk management is to lower the organization's degree of riskiness without impacting its strategy, tactics, operations, or compliance (STOC). The benefit of risk is that it allows the company to adhere to the targeted STOC at the lowest degree of risk that is realistically and economically feasible. The risk exposure of the organization is represented by the degree of risk determined by the riskiness index. The board may then contrast this amount of risk exposure with the organization's capability for risk and its own attitude toward risk[3], [4].

inadequate senior management structure to establish 'risk-aware culture' and assist organization. Inadequate human resources, abilities, and availability, as well as worries regarding intellectual property. Inadequate physical resources to meet the organization's operational and strategic goals. Infrastructure for information technology (IT) lacks proper data security and/or resilience. Plans for business continuity are not strong enough to guarantee that an organization will continue to operate after a significant loss. Unreliable product delivery, transportation plans, and/or communications infrastructure.

Identification of the hazard risks that an organization is really taking is necessary to determine the riskiness index of that company. In other words, determining an organization's true risk exposure is aided by analyzing its riskiness index. The board of an organization may then determine if the portfolio of risks is within the risk appetite and/or risk capacity of the organization and consistent with the risk attitude of the board after determining the real degree of risk embedded within the company. The primary risks that the board is ready to accept in order

to achieve its strategic goals must be identified, together with their type and magnitude. After identifying the risks that the organization is taking by a process comparable to calculating the riskiness index, organizations should take care to ensure that the board does not simply conclude that the risks the organization is presently taking must be the same as the risks it is willing to take[5].

Advantages of the Plan

Every firm will have a mission statement, a list of corporate objectives, and a comprehension of the expectations of the many stakeholders. The organization's board will then need to create a plan that is both successful and efficient and will fulfill the purpose, goals, and expectations perfectly. The organization's board will need access to risk information to make sound strategic choices. A risk analysis of the suggested plan should be conducted, as well as a risk analysis of any workable alternatives. The likelihood that the strategy choices will be sound will increase with the availability of this risk assessment data.

Even less information is likely to be provided for opportunity risks in order to estimate risk probability. A firm could see a chance to gain a new customer or create and promote a brand-new product. To decide whether the new enterprise should proceed, a precise risk assessment of the probability of both positive and negative outcomes will be required. When a new product is introduced, it may be necessary to raise the possibility that a favorable occurrence may occur. Advertising and press coverage for the introduction of a new product must be maximized while yet being cost-effective. Therefore, steps should be done to raise media attention in the launch.

Strategic core processes combine the fields of risk management with strategic planning. In order to reach agreement at the board level on the few topics that might have a significant impact on the organization's long-term success, strategic planning is a methodical procedure. Strategic concerns are crucial, and choosing the wrong strategy or failing to execute one that has been chosen may be among the most damaging hazards to a business. The typical method for implementing a strategy is to design tactics, execute them via projects, and finally deliver them through operational core procedures. The business model of the company is represented by the operational core processes in use at a particular period, as is covered in greater depth[6], [7].

Activities for managing risks are created to guarantee the greatest result and lessen uncertainty. Risk management activities aid in the creation of an effective and efficient plan, which is the benefit of risk in strategy. Through the use of the used techniques, that plan will be put into action. These strategies will be created to enhance organizational core processes, ensuring that the company is employing the most effective and efficient ones possible. An approach to risk management that views risk as an opportunity is described in the boxed example. This method of managing the business shows a commitment to welcome risk's potential rewards.

Advantages of Projects

Every business must implement the appropriate core procedures. A core process may be thought of as a group of actions that fulfill a certain stakeholder expectation. The definition of core process given by business process re-engineering (BPR) practitioners is as follows. There is a

distinction between an effective method and one that is efficient. An effective procedure implies there are no delays or extra expenses. However, the technique may not be the best one to fulfill the needs in a cost-effective manner. A project will typically be started and change will be made where procedures need to be improved. When many projects are necessary, this is sometimes referred to as a program of work. When a company implements a project or program of work, the goal is often to increase the efficacy and/or efficiency of key processes[8].

The company should be able to guarantee that the project is more effectively implemented on time, within budget, and to specifications by doing an appropriate risk assessment of the desired change. It is necessary for projects to be well managed and for the company to have chosen the right projects or priorities in order to realize the upside of risk in project or programme management. Organizations often conduct a post-implementation evaluation to confirm that the project's anticipated advantages have been realized. Internal audit often conducts this evaluation, which is intended to make sure that the project was completed effectively, provided the necessary benefits, and was ultimately worthwhile. It is crucial that the company chooses initiatives during lean financial circumstances that not only succeed but also represent the best use of its limited resources as compared to alternatives that were not chosen.

Project risk management is connected to the use of strategies created to carry out the plan. Tactics implementation initiatives may only be allowed in certain companies if they lower risk. For instance, the project should be developed to make an activity more resilient if it may fail due to subpar IT infrastructure. By doing this, risks will be decreased and it should be feasible to quantify the advantages of operations that will be more productive due to better utilization of human resources and fewer IT system failures.

In conclusion, effective risk management in projects increases the likelihood that they will be completed on schedule, within budget, and with the requisite level of quality. As the project moves forward, risk management actions will aid with delivery while also assisting in managing a scenario in which the conclusion differs from what was anticipated. This varied result will show if the strategies were effective and the right project was chosen. As this is one illustration of the upside of risk, a negative difference will need to be reduced and a good difference will need to be welcomed[9].

Advantages of Operations

Effective and efficient operations are a vital necessity for enterprises. Effective operations should avoid unanticipated disruptions and make the most use of the organization's resources. The organization will profit the most from efficient processes that use the fewest resources and provide the highest output. Activities must also be efficient in the sense that they show the optimum method for carrying out the activities. For instance, traveling across a crowded metropolis in a vehicle or bus may be effective. The metro or subterranean system, however, is often the most efficient form of transportation in big cities. The company can offer the most effective and efficient activities, operations, and processes by evaluating risk management of operations. Delivering the most effective and efficient operations enables a commercial organization to outperform a rival, complete projects for less money, and yet turn a profit. The

provision of effective and efficient operations is crucial for public services. The majority of public services have delivery goals, which may be intricate and difficult. The provision of public services may be hampered by a failure to properly anticipate and manage risks. By introducing flexibility and resilience to the way services are provided, risk management's contribution will also aid in achieving long-term improvements in the quality of the provided services. It is possible to see this contribution by risk management as a component of providing the upside of risk.

In a competitive market, taking on risk sometimes comes at the expense of suppliers, rivals, or other third parties. To pursue the benefits of risk-taking, one must be mindful of a potential unanticipated drawback. If you decide against doing anything because it seems riskier now, the dangers might end up being higher. Additional facets of risk appetite and individual risk perception. It is critical that business choices about operational risk be made on an objective basis. Personal opinions and perspectives on risk might result in poor business judgment. One of the main duties of the risk manager is to make sure that correct risk information is readily available so that business choices can be made. The process of risk management begins with the context. The riskiness index presented offers a helpful framework for determining the organization's internal and external contexts. Setting the context requires taking into account the upside of risk as well as how chances will present themselves for the business and how to take advantage of them in connection to strategy, tactics, and operations[10].

CONCLUSION

Finally, it's critical to remember that there is potential gain in connection to compliance risks. There will be a regulator for certain groups, and the organization won't be able to function without a license. In these situations, a positive working relationship with the regulator often offers a risk upside. This will be particularly true if the organization tries to persuade the regulator to want more stringent oversight of activities that are regulated. In this method, the company will establish high standards that it can meet in the hopes that rivals will be put at a disadvantage if they too need to meet similar requirements but can't do so without incurring extra costs. The efficiency of current controls in controlling prospective risks and seizing potential opportunities must also be taken into account by organizations. This entails evaluating the effectiveness of current controls and locating any openings or vulnerabilities in the control environment.Determining the upside of risk is, in general, a crucial step in the risk management process. Organizations may create efficient risk management methods that allow them to maximize the advantages of taking risks while limiting possible costs by recognizing prospective opportunities and analyzing their potential impact.

REFERENCES:

[1] J. F. P. Bridges, V. F. Paly, E. Barker, And D. Kervitsky, “Identifying The Benefits And Risks Of Emerging Treatments For Idiopathic Pulmonary Fibrosis: A Qualitative Study,” *Patient*, 2015, Doi: 10.1007/S40271-014-0081-0.

[2] M. A. Kelley, H. Benz, S. Engdahl, And J. F. P. Bridges, “Identifying The Benefits And Risks Of Emerging Integration Methods For Upper Limb Prosthetic Devices In The

United States: An Environmental Scan," *Expert Rev. Med. Devices*, 2019, Doi: 10.1080/17434440.2019.1626231.

[3] M. Kelley, H. Benz, S. Engdahl, And J. F. P. Bridges, "Pmd42 Identifying The Benefits And Risks Of Emerging Integration Methods For Upper Limb Prosthetic Devices: An Environmental Scan," *Value Heal.*, 2019, Doi: 10.1016/J.Jval.2019.04.1038.

[4] S. H. Lee, "New Measuring Stick On Sharing Accommodation: Guest-Perceived Benefits And Risks," *Int. J. Hosp. Manag.*, 2020, Doi: 10.1016/J.Ijhm.2020.102471.

[5] S. Kim, G. Lee, And H. G. Kang, "Risk Management And Corporate Social Responsibility," *Strateg. Manag. J.*, 2021, Doi: 10.1002/Smj.3224.

[6] R. Ward, "Identifying And Assessing Benefit-Risk In Primary Care--A Family Physician's Perspective.," *Rheumatology (Oxford, England)*. 2010. Doi: 10.1093/Rheumatology/Keq059.

[7] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, And V. Weerakkody, "Blockchain For Next Generation Services In Banking And Finance: Cost, Benefit, Risk And Opportunity Analysis," *J. Enterp. Inf. Manag.*, 2021, Doi: 10.1108/Jeim-02-2020-0044.

[8] N. R. Gee, M. K. Mueller, And A. L. Curl, "Human–Animal Interaction And Older Adults: An Overview," *Frontiers In Psychology*. 2017. Doi: 10.3389/Fpsyg.2017.01416.

[9] S. L. Macdougall And D. Hurst, "Identifying Tangible Costs, Benefits And Risks Of An Investment In Intellectual Capital: Contracting Contingent Knowledge Workers," *J. Intellect. Cap.*, 2005, Doi: 10.1108/14691930510574663.

[10] A. Keyter, S. Salek, S. Banoo, And S. Walker, "Can Standardisation Of The Public Assessment Report Improve Benefit-Risk Communication?," *Front. Pharmacol.*, 2020, Doi: 10.3389/Fphar.2020.00855.

CHAPTER 14

AN OVERVIEW ON TOLERATE, TREAT, TRANSFER AND TERMINATE

Dr S.Yogananthan, Adjunct Faculty, Department of Decision Sciences,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id-dr.s_yogananthan@cms.ac.in

ABSTRACT:

Key risk management techniques that firms may employ to control possible hazards include tolerating, treating, transferring, and terminating. Depending on the organization's risk appetite and the kind of risk, each of these techniques takes a unique approach to managing risks. Accepting a danger's possible repercussions while not taking any steps to reduce it is known as tolerating the risk. If the expense of reducing the risk is thought to be higher than the possible harm, this strategy may be suitable for hazards that are low in probability or impact. Risk management entails taking steps to lessen a risk's probability or effects. This might include putting control mechanisms into place, such as creating new rules or processes or investing in new resources or technology. Treating risks may also include passing the risk to a different party, as in the case of outsourcing or insurance.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

By transferring risks, one party assumes responsibility for the possible repercussions of the risk. This can include getting insurance or contracting with other companies to do certain tasks. Where the expense of managing the risk internally is deemed to be too expensive or where the necessary knowledge is not internal, the transfer of risks may be suitable. Risk termination entails completely removing any possible negative effects. This can include discontinuing risk-related operations or leaving specific business sectors. When a risk's potential effect is thought to be too severe or when it is seen to be inconsistent with the organization's goals, it may be acceptable to terminate the risk.

1. The danger response Ts
2. The most important risks to a company are those that:
3. Significantly high or very significant influence in regard to the benchmark test for significance;
4. A very high or high possibility of materializing at or above the benchmark level;
5. High or very high potential for control improvement that is also cost-effective.

In general, only priority major hazards need to be addressed at the highest level of the business. But it is reasonable that boardroom discussion also focus on compliance issues. In reality, the board will anticipate that these compliance risks will be well handled and will only be provided with routine/annual reports summarizing risk performance or a special report in the event that a particular problem has occurred. To reduce compliance risks, the firm will try to implement

effective and efficient controls. Setting the benchmark test for significance at a level that reflects a major influence on the organization is recommended. After identifying the most important risks, the company must examine its controls and determine if any further steps are necessary. The spectrum of possible responses for hazards threats is sometimes referred to as the Ts. Risk response choices may be described using a wide variety of terms. In actuality, the more general word is "risk treatment," which is used by both British Standard BS and ISO. For instance, the British Standard describes risk treatment as the 'process of defining, selecting, and implementing controls'. The same definition of risk treatment is given by ISO: "Development and implementation of measures to modify risk." For the risk response step of the risk management process, the language from the Orange Book has been utilized in this book. The Ts may then be used to describe the alternatives for handling risk. Information on the alternate definitions that various publications employ is provided in Appendix B.

Without taking any more steps, the exposure can be bearable. Even if a risk is intolerable, there may be nothing that can be done about it or it may cost too much to mitigate it compared to the possible rewards. In this method, the vast majority of dangers will be handled. The goal of treatment is to take action (control) to limit the risk to an acceptable level while the activity causing the risk is still being conducted inside the organization. The best course of action for certain risks may be to transfer them. This may be accomplished by traditional insurance or another method, such as paying a third party to assume the risk. This choice is especially effective in reducing financial or asset-related concerns. Some dangers can only be managed or reduced to acceptable levels by stopping the activity. It should be highlighted that, in contrast to the private sector, the ability to terminate operations may be severely constrained under government. Each of the Ts is described briefly and given further details[1]–[3]. The four Ts of hazard risk management are as follows:

1. Tolerate.
2. Treat.
3. Transfer.
4. Terminate.

suggests that, depending on where the risk is located on a risk matrix, there is a dominating reaction in connection to each of the Ts. Tolerance is the primary reaction to low likelihood/low effect threats. Treating hazards with a high chance but low effect is the primary course of action. Transfer is the primary response to risks with low likelihood/high impact, and termination is the primary response to risks with high likelihood/high impact. To provide some context for the range of risks being considered, provides examples of the range of potentially important risks associated with the headings of the FIRM risk scorecard. The most probable reaction to the risk will then be indicated by where it falls on the risk matrix. The impact of the present controls will already have been assessed as part of the risk assessment process if it is conducted at the current level of risk.

Consider a theater that must adapt to the growing number of booking agents that want payment up front rather than after the play. Additionally, the theater recently suffered significant financial loss as a result of an actor's refusal to show up the night of the performance. As a consequence,

the theater has reviewed the contracts and appearance plans for performers and decided on replies that are suitable for all Ts. The theater may decide that it must put up with the new booking fee policies. It has also determined that in the future, it will only work with established agents and end its current agreements with an agency that has previously shown itself to be unreliable in order to treat/reduce the risk. In order to shift the expense of a performance that must be canceled because the actor is late, the theater may also look into the idea of purchasing insurance.

Accept Risk

The Guide defines risk tolerance as the organization's or stakeholder's willingness to accept the risk after risk mitigation in order to achieve its goals. adds that legal or regulatory (compliance) requirements may have an impact on a person's risk tolerance. The remark concerning legal or regulatory obligations is highly pertinent since businesses often have to accept a risk due to such regulations, even in situations when they wouldn't normally want to do so. It should be highlighted that tolerance is different from risk appetite in that tolerance pertains to a particular or individual risk. The quantity and kind of risk that an organization is prepared to take on or tolerate is referred to as its "risk appetite."

The terms "when an organization is willing to tolerate a risk" and "risk tolerance" are sometimes used interchangeably. The idea of tolerance often refers to a company's willingness to hold onto or tolerate a risk, even if it is more than the company would ordinarily choose to accept. The idea of risk tolerance is the other. In order to describe the range of risk that is generally accepted, many companies employ risk tolerance in the engineering sense. Draw the line around the risk tolerance in the middle of the worried zone and cautious zone. These zones specify the limits within which the company wants the degree of risk to be contained, similar to how engineers use the term tolerance.

An company could need to accept risks that are now at a level outside of its risk tolerance and comfort level. An company may sometimes even be required to endure risks that exceed its real risk tolerance. The group would be exposed at this time, albeit this scenario would not last. The company will tolerate a risk when it is seen to be within the parameters of its risk appetite. The strategy that will be used in regard to low-likelihood, low-impact threats is proven to be risk tolerance. However, a company may opt to accept high risk levels if they are related to a potentially profitable activity or a core procedure that is essential to the operation of the company.

It is uncommon for a hazard risk to be accepted or tolerated prior to the implementation of any risk management measures. In general, a risk is only considered bearable after all practical control measures have been implemented and the organization has decided to accept or tolerate the risk as it now exists. Because the risk's inherent level could have been intolerable, certain control measures might have been implemented. The goal of control effort is to shift the risk to the risk matrix's low-likelihood/low-impact quadrant. Risks are sometimes only allowed as a component of a plan when one risk is weighed against another. This is a straightforward explanation of mitigating or hedging risks, but from a commercial perspective, it may be a

crucial strategic choice. For instance, a private power provider operating in the northern areas of the US may have to accept the effect of temperature variance on electricity sales. The north/south combined operation will be able to moderate the variance in energy sales caused by changes in temperature by merging or forming a joint venture with an electrical company in the southern states. When demand in the southern states is low due to the cold, the combined operation will then sell more power in the northern states. In the summer, when demand for power in the northern states may be lower, the combined operation will sell more electricity for air conditioners in the southern states[4].

Reduce Danger

The company will want to address the risk when the amount of risk exposure (probability) connected with a certain hazard is high but the potential loss (impact) associated with it is low. In order for the new current level or goal level to be tolerated once the risk has been addressed, it is common practice to begin risk treatment with the risk at its inherent and/or current level. In an organization, measures to raise the bar for risk management will continuously be reviewed. On a personal level, risk reduction practices include using a seatbelt when driving or installing an intruder alarm in your home. It is commonly known that risk control criteria for physical (insurable) hazards have improved. Sprinkler systems for structures, improved building security measures, and personnel security screening are a few examples of risk improvement measures intended to better control hazard hazards. The company must consider both the consequences of the risk should it materialize and the treatment's influence on the chance of the risk materializing when determining the best risk management alternatives. It will be necessary to choose risk management strategies that are affordable, and a risk matrix may be used to display the impact of various control methods. The phrase used to describe treat risk has a problem. According to ISO, "treat risk" is the primary category under which a number of choices are available, including:

1. Opting not to begin or continue with the activity will help you avoid the danger.
2. Increasing or taking on more risk in order to seek a chance.
3. eliminating the risk's origin.
4. Changing the probability or the results.
5. Dividing the risk between two or more parties.
6. Reduce the risk by wise decision-making.

'Risk response' is often referred to as the key heading in risk management standards, and this paper follows that strategy. Tolerance, treatment, transfer, and termination are the alternatives that result from using risk response as the major heading. It is up to the company to create its own risk vocabulary, one that is compatible with the external, internal, and risk management environment, as is the case with other terminology-related concerns. Sometimes the language will be determined by the surrounding context. For instance, banks and other financial organizations must utilize the regulator's language. On occasion, the vocabulary used inside an organization is determined by its internal context. It is likely that the risk manager would be better advised to use the terminology that already exists within the organization rather than trying to introduce new terms or new meanings for existing terms if the terminology that has developed within the organization conflicts with the terminology in ISO [5].

Move the Risk

The company will want to transfer a risk when there is a low chance of it happening but a high chance that it could. A trusted method for transferring the financial toll of losses brought on by hazard risks and (to a lesser degree) control risks is insurance. In this research, the problems with using insurance as a method of risk transfer are more thoroughly examined.

In certain circumstances, the desire to remove or end the risk is directly tied to risk transfer. But many risks cannot be shifted to the insurance market, either because insurance premiums are too expensive or because the hazards in question are (traditionally) uninsurable. Both traditional insurance and contractual agreements may be used to shift risk. Finding a joint venture partner or another way to split the risk may also be an option. Therefore, risk hedging or neutralization may be seen as both a risk treatment option and a risk transfer option [6].

Risk finance includes the cost of risk transmission. Again, there are many meanings being employed. Both BS and ISO concur that risk financing entails the expense of contingent agreements for the supply of cash to handle the financial repercussions of a risk materializing. Insurance often provides these arrangements, making insurance money dependent on the occurrence of certain covered events. Considers that the supply of cash to cover the cost of risk treatment should be included in the cost of risk financing. In this book, the process of risk management includes resourcing controls as a distinct stage. This is one another illustration that there is no uniform or universal vocabulary of risk.

The word "risk transfer" raises yet another terminological difficulty. Risk transfer is should be preferred above risk sharing, according to ISO. The claim is that a risk can never be totally transferred and will always be shared to some amount, regardless of the parties' intentions. Although this study is correct, other variables will also have an impact on the language employed inside an organization. The insurance sector refers to risk transfer as a means of risk sharing. When the insurance manager in the organization prefers to use the terminology of risk transfer because that is the standard terminology used in part of the external context, which is the insurance market, it may be challenging for the enterprise risk manager to insist on the use of the phrase "risk sharing."

Reduce Risk

The company will want to terminate or remove the risk when it has a high probability and high potential effect. The corporation and/or its stakeholders may not be willing to accept the risks involved with doing business in a certain region of the globe or the environmental concerns related to continuing to use a particular chemical. In these situations, effective solutions would be to cease the process or activity, eliminate the risk, switch to a different activity, or outsource the risk-related activity. Although an organization may want to eliminate a danger, it's possible that the action that gave birth to it is essential to the company's continuous operations. In these situations, it's possible that the organization won't be able to completely eradicate or terminate the risk, thus other control measures will need to be put in place.

For public services, this is a particular problem. Although the company may face risks with a high chance and potential effect, it is powerless to stop the underlying operations. This can be the case because a governmental body or other public authority is required by law to engage in the activity. The company will need to implement control measures to the fullest degree possible while remaining cost-effective since the public service imperative may make it difficult to stop the activity. Such control techniques will most likely include risk treatment and risk transfer. The amount of risk will decrease when these control measures are implemented until it is at a point where the company can bear it. It may not be feasible to reduce all risks to a level that is consistent with the organization's risk appetite due to the fluctuating nature of hazards. In order to continue engaging in a particular activity, the company may discover that it must accept risks above and beyond its empirical risk appetite [7].

Strategic Risk Mitigation

The overall strategy for managing control and opportunity risks is comparable to the strategy used to handle hazard risks. The spectrum of possible alternatives, nevertheless, differs enough for each to be shown individually. It is important to keep in mind that projects often reflect and put into practice the techniques being used to accomplish strategy. The four Ts of risk management for hazards and the kinds of controls that are most likely to be connected to each kind of risk response for hazards. The various control kinds are discussed below. Almost all of this paper's focus has been on mitigating risk from hazards. The Ts stand for different ways to reduce the dangers from hazards. Suggests that a variety of solutions are available to handle opportunity risks. A thorough assessment of each viable strategy's degree of risk and potential return is necessary in order to develop and execute an effective and efficient plan. Exist, explore, exploit, and exit are the four Es of opportunity management. The organization's standing and the Es have a strong link. A start-up business will have more risk and lower potential profits. At this point, business possibilities will be investigated. Potential profits will rise as the organization expands, but the degree of risk will stay high. The company will strive for expansion, but if it feels that expansion is too sluggish or that the risk level is still too high, it may decide to stop certain activities.

After a time of expansion, the company ought to be getting a lot of profit for little risk. This stage is when the company will take advantage of chances up to the arrival of rivals. This business is established. Although many businesses opt to operate in mature, declining markets where risk exposure is minimal and potential rewards are also low, all mature enterprises are susceptible to the threat of decline. The Es may be used to manage strategic, opportunity, or speculative risks in a way that is consistent with the risk and reward information provided. However, for many firms, taking opportunity risks and creating strategic goals are the most crucial concerns. The risk management input into operations and projects is often more thorough and well-structured than the risk management input into strategic decision making.

The distribution of the dominant reaction types and control types throughout the four quadrants is comparable to how the Ts are distributed when utilizing hazard risk management. Living in a mature or falling market is comparable to embracing tactic ambiguity and enduring risky situations. Examining the choices for addressing hazard threats is comparable to exploring

opportunities. The variations in approach between the management of risks and uncertainties compared with the management of opportunities become most obvious when it comes to using opportunities and exciting opportunities. By considering risk appetite, the region of high risk and possibly high return is assessed in greater depth. An corporation can discover that although it has a good economic opportunity, it lacks the resources to take use of it. The company has three basic options in these scenarios. It can decide not to explore the opportunity because it lacks the ability or willingness for risk. It may try to share the opportunity or sell it to a company that does have the motivation, capability, and resources to take advantage of it. Because the business lacks the ability, finances, and risk appetite to pursue the opportunity and has been unable or unwilling to find a partner to purchase or share it, exiting the opportunity may be the best course of action. However, the majority of firms with a good opportunity will want to benefit from its discovery. Sharing the opportunity with, say, a joint-venture partner may be a better long-term alternative than selling it, which may result in a profit exit [8].

CONCLUSION

By entering into a joint venture, the organization's degree of risk will be lower, but the advantages will be shared. Business strategy, risk appetite, risk capability, and the availability of acceptable business partners will all play a role in this choice. Exploiting business possibilities may be feasible via risk sharing, employing strategies like outsourcing to share the risk with others in the supply chain, in addition to a joint-venture relationship. However, it has the additional refinement that when the firm seeks to grow, it will have the choice to leave if the organization's risk appetite and/or risk capacity are surpassed. Depending on risk appetite, this makes the Es method become the Es approach. The text box below gives an example of this strategy used for opportunity management, however the language is a bit different, as is often the case in risk management. In general, a number of variables, such as the kind of risk, the organization's risk appetite, and the resources available to manage the risk, influence the choice of the best risk management plan. Organizations may create a successful risk management strategy that allows them to handle possible risks proactively and successfully by taking into account the four primary techniques mentioned above.

REFERENCES:

[1] J. Doering, R. Kizys, A. A. Juan, À. Fitó, and O. Polat, “Metaheuristics for rich portfolio optimisation and risk management: Current state and future trends,” *Operations Research Perspectives*. 2019. doi: 10.1016/j.orp.2019.100121.

[2] E. Fisher, J. Hellin, H. Greatrex, and N. Jensen, “Index insurance and climate risk management: Addressing social equity,” *Dev. Policy Rev.*, 2019, doi: 10.1111/dpr.12387.

[3] B. G. Tavares, C. E. S. Da Silva, and A. D. De Souza, “Practices to Improve Risk Management in Agile Projects,” *Int. J. Softw. Eng. Knowl. Eng.*, 2019, doi: 10.1142/S0218194019500165.

[4] N. Etemadi, P. Van Gelder, and F. Strozzi, “An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity,” *Sustain.*, 2021, doi: 10.3390/su13094672.

[5] M. N. Meskovic and A. Zaimovic, "Risk Management Maturity, its Determinants and Impact on Firm Value: Empirical Evidence from Joint-Stock Companies in Bosnia and Herzegovina," *South East Eur. J. Econ. Bus.*, 2021, doi: 10.2478/jeb-2021-0019.

[6] S. J. Yu and J. S. Rha, "Research trends in accounting fraud using network analysis," *Sustain.*, 2021, doi: 10.3390/su13105579.

[7] E. Garbarino, G. Orveillon, and H. G. M. Saveyn, "Management of waste from extractive industries: The new European reference document on the Best Available Techniques," *Resour. Policy*, 2020, doi: 10.1016/j.resourpol.2020.101782.

[8] J. Ruiz-Canela López, "How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company?," *J. Risk Financ. Manag.*, 2021, doi: 10.3390/jrfm14030139.

CHAPTER 15

A STUDY ON THE RISK CONTROL TECHNIQUES

Dr Ravishankar S Ulle, Assistant Professor, Department of Decision Sciences,
CMS Business School, JAIN (Deemed to-be University), Bangalore, India,
Email Id -dr.ravishankarulle@cms.ac.in

ABSTRACT:

The risk management process must include risk control approaches because they assist companies in lowering the possibility or effect of prospective hazards. Organizations may manage risks using a variety of risk management approaches, including risk avoidance, risk reduction, risk transfer, and risk retention. By eliminating certain assets or behaviors that are linked to the risk, for example, one might completely remove the risk. This strategy may be suitable for hazards that are thought to have an excessive probability or effect, or when the expense of risk management is thought to be excessive. Implementing strategies to lessen a risk's chance or effect is known as risk reduction. To better manage the risk, this may include putting new rules or processes into place, as well as investing in new tools or resources. The creation of backup plans or other risk mitigation strategies may also be included in risk reduction tactics.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Transferring risk means assigning another party accountability for a risk's possible repercussions. This can include getting insurance or contracting with other companies to do certain tasks. When the cost of managing the risk internally is deemed to be too high or when the necessary knowledge is not internal, risk transfer may be suitable. Accepting a risk's possible outcomes while not taking any steps to reduce it is known as retaining the risk. If the expense of controlling the risk is thought to be higher than the possible harm, this strategy may be suitable for hazards that are low in probability or impact.

Varieties of Controls

There are several measures that may be used to reduce risk from hazards. To categorize these controls as preventative, corrective, directive, and detective is the most practical method. Gives a more thorough explanation of each of these four different hazard control methods. The preventative, corrective, directive, and detective (PCDD) control choices reflect a distinct hierarchy of controls in respect to hazard hazards. Examples of these four categories of controls in regard to health and safety hazards are shown on the risk matrix to show the link between these four types of controls and the dominant risk of reaction for various degrees of risks, which is shown in Figure 1.

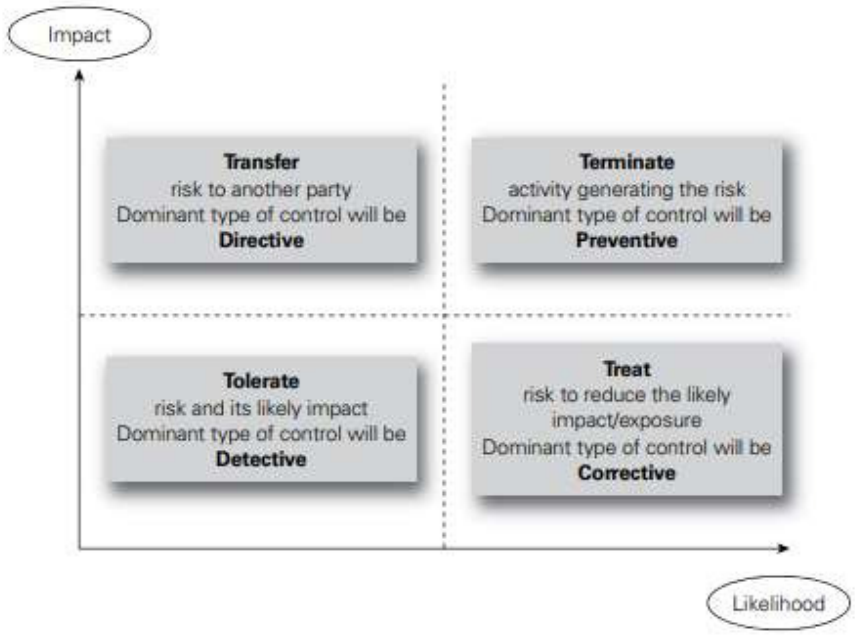

Figure 1: Types of controls for hazard risks.

Preventive (termination): These controls are intended to reduce the likelihood that an unwanted consequence would really occur. The more crucial it is to avert a bad consequence, the more crucial it is to put in place the necessary preventative measures.

Corrective (treat): These controls are intended to lessen any unfavorable results that have already been experienced and to reduce the potential for loss. They could also provide you a path to go if you want to get some compensation for harm or loss.

Insisting (transferring)

These measures of control are intended to guarantee the accomplishment of a certain goal. They work by offering individuals instructions on how to prevent losses from happening. They are significant, but they rely on workers adhering to recognized safe work practices. These controls are intended to spot instances when unfavorable results have occurred. They are only acceptable when it is reasonable to acknowledge that the loss or harm has happened since their impact is, by definition, "after the event." Preventive measures are intended to reduce the likelihood that a dangerous hazard occurrence may occur. Preventive controls make up the bulk of those applied in businesses in response to hazard hazards. Preventive measures for health and safety concerns include changing the activity to use a less hazardous substance or enclosing the activity to reduce employee exposure to dust or fumes. Examples of fraud risk prevention measures.

Corrective measures are intended to address problematic situations and lessen unacceptable risk exposures. Such controls provide a crucial approach for managing the risk such that its likelihood of happening and/or consequences are significantly reduced. In general, corrective corrections are intended to make a situation better. Machine guards are an example of a corrective control. Business continuity planning (BCP) and disaster recovery planning (DRP)

have generated discussion on how well they fit within the PCDD classification of various hazard risk controls. DRP and BCP are seen as directive controls by certain businesses, whilst others claim they are corrective controls. An alternate perspective is to argue that a DRP and BCP should be seen as a fifth kind of control as they are both involved with crisis management and cannot be simply categorized as PCCD types of controls. Actually, this debate is useless, just like so many other fights about language. If strategies have been thought out and put in place before the crisis, an organization will be in a much better position to handle it when it arises.

Generic Type of Control

Utilizing alternate facilities that were set up before the crisis occurred is sometimes a part of crisis management. These can be considered remedial controls. In any situation, crisis management will require giving the people involved instructions on how to act in the event of a crisis. These restrictions can be considered directive ones. Detective controls often focus on identifying situations when a risk has manifested at a relatively low level with little effect and repercussions. DRP and BCP clearly pertain to situations when hazards have manifested at a crisis level. DRP and BCP should not be considered detective controls as a result [1]. The function of the four different kinds of controls is conveniently shown by the bow-tie diagram of the risk management process. Actions that are conducted in advance of the incident are related to preventive controls. Due to their nature, detective controls pertain to events that have already happened. Loss prevention, damage reduction, and cost containment may all require the use of corrective and directive controls. The three stages of loss control are as follows. The relationship between the different kinds of controls and the risk management process's bow-tie appearance, as shown in figure 2.

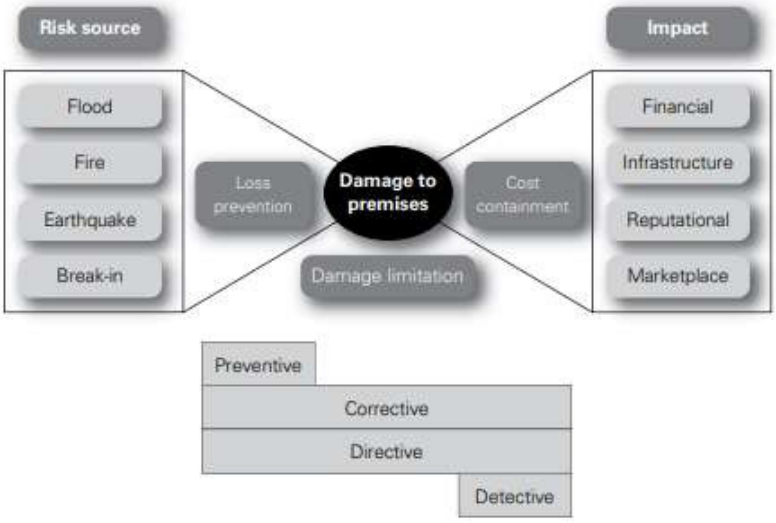

Figure 2: Illustrate the Bow-tie and types of controls.

The purpose of directive controls is to guarantee that a certain result is obtained. Directive controls, in terms of health and safety, would comprise instructions/directions provided to workers to follow, for a while using personal protective equipment. Directive controls include training on how to react to a certain risk occurrence and specific instructions and procedures.

Directive controls can refer to the steps that must be followed in the case of a loss to lessen the harm and keep the expenses under control. Detective controls are intended to spot situations when an unfavorable consequence has taken place. In order to prevent the situation from becoming worse, the control is designed to recognize when certain undesired occurrences have occurred. Conducting a post-incident review is an illustration of detective controls in a project. The sequence of preventative, corrective, directive, and lastly detective represents a clear hierarchy of control efficacy. Clearly, the most effective controls are those that prevent problems from occurring, then those that address unfavorable situations [2][3], [4].

A lesser degree of control is giving staff training and instruction, and detective controls merely serve to validate that a negative occurrence has taken place. It is important to recognize the value of DRP and BCP. They are complementary to detective controls since they are both cost-containment strategies created to guarantee little disturbance once a hazard risk has manifested. However, as DRP and BCP are post-loss processes, they do not neatly fit into the PCDD categorization scheme for controls. BCP and DRP are a fifth type of control in certain categorization schemes for controls. In order to develop a comprehensive set of risk responses, an organization will employ all four kinds of controls, as shown in the example in the box below. To lower traffic accidents, the road transport corporation will use all four categories of regulations.

Implementing the Ts

Consider a road transport corporation that wants to lower the number of traffic accidents per million miles traveled and the tools available to do so. The following decisions may be made by the firm after considering the preventive, corrective, directive, and detective control hierarchy: To avoid drivers having to drive recklessly in order to make it on time, the scope for implementing preventative measures includes reviewing vehicle route and providing realistic delivery schedule predictions. A few of the corrective actions that will be implemented include improved maintenance practices and better ways for drivers to report problems with their vehicles. Enhanced directive controls will be based on defensive driving instruction and the distribution of a vehicle driver's manual with straightforward, practical guidance. The use of tachographs in the cars already provides some investigative controls, but the business may elect to add a regular assessment of drivers' licenses to look for penalty points [5]. Routine vehicle inspections to find and report damage and a study of fuel usage to identify drivers with an aggressive driving style are additional controls that the transport firm may assess. The business is then in a position to implement planned and quantifiable loss-control programs to lower the fleet's total operating costs.

DISCUSSION

Risky-Hazardous Areas

Although a straightforward risk matrix may be used to show the Ts of hazard response, the possibilities are not always obvious. It is clear that the risk matrix's intersection point for the choices tolerating and terminating risk is there. It is illogical to claim that a little increase in a risk's probability and possible effect would fundamentally alter the organization's strategy for

dealing with that specific risk. The comfort zone is mostly used for low-impact, low-likelihood situations. It is clear that there is a certain degree of potential influence that will always fall below acceptable bounds. Similar to this, there is a threshold of risk probability that is consistently thought to be so low that it will not occur.

But when risk possibility and possible consequence grow, a decision must be made about whether the risk should be allowed. In the cautious zone, judgment is necessary, and steps are often done to manage and/or transfer the risks there. The organization's risk appetite is represented by the line dividing the cautious zone from the worried zone. Together, the cautious zone and the worried zone show the level of risk's allowable variability, and they may be interpreted as an organization's tolerance for the amount of risk's allowable volatility. A crucial point is reached when the risk probability and possible effect continue to rise. The company will be worried about accepting such risks once they cross the critical line and will want to stop exposure to them. In certain cases, the company won't be able to eliminate these risks since they could be necessary for the organization's operations or because they're part of a high-risk, high-reward plan that the board has chosen.

Preventive Measures

A succinct explanation of the makeup of preventative measures. Preventive controls are the most crucial kind of risk management, and all businesses will use them to manage certain hazards. The future of the organization and the continuance of certain operations may not make it desirable, nor is it cost-effective, to prevent or eliminate all hazards.

Separation of duties, where no one is allowed to act without the approval of another while paying an invoice, is an example of a preventative control. Additionally, spending controls should stop one person from placing an order and then approving the payment for it. Preventive controls in terms of health and safety include getting rid of the risk and offering a less dangerous replacement. For instance, a less dangerous equivalent may be utilized in place of a hazardous chemical used in cleaning operations. Preventive controls provide the benefit of eliminating the risk, hence negating the need for further consideration of it. In practice, this may not be a financially sensible choice, and it might not even be practical. The drawbacks of preventative measures include the possibility of outsourcing or replacing positive operations with ones that are less effective and efficient[6].

'So far as practically possible' is how health and safety professionals define the phrase "elimination of hazardous activities." Achieving anything to the extent that it is realistically possible requires weighing the benefits of the accomplished risk reduction against the cost in terms of time, difficulty, and money. For instance, the installation of support beams and supports may lower the danger of collapse in underground mines. However, the expense of providing these supports must be weighed against the amount of risk reduction that would be accomplished in that specific mine to determine the extent to which this is practically achievable.

Corrective Measures

a succinct explanation of how corrective controls work. After it has been determined that preventative controls are not technically possible, operationally desirable, or cost-effective, corrective controls are the next course of action. Corrective measures are capable of achieving a fully satisfied outcome in which the existing level of risk is decreased to a level that is consistent with the organization's risk appetite. Correctional controls are shown in the administration of workplace health and safety. A fairly well-known method of corrective control is engineering confinement using barriers or guards. Passwords and other access controls might be seen as corrective measures when it comes to fraud exposures. This group of controls also includes frequent supervisory changes and staff rotation [7].

Many remedial measures have the benefit of being straightforward and affordable. Additionally, they do not demand that current techniques and processes be abandoned or changed to more efficient ones. The controls may be put into place within the parameters of current operations. The drawback of certain corrective controls is that it may be difficult to quantify or verify the cost-effectiveness of the marginal advantages that are realized. Corrective measures are sometimes over-engineered, increasing the expense relative to the benefit received. It is the responsibility of risk management experts, internal auditors, and workers to determine whether costly and/or inadequate remedial measures have been put in place. Corrective controls are often implemented as a result of regulatory obligations. From the perspective of the organization, this could not be desirable and might result in increased expenses or inefficiencies. To meet the minimal legal criteria, it is up to the organization to make sure that the proper degree of corrective control is attained.

Corrective control design and execution are often the subject of heated debate and even dispute. For instance, installing sprinklers as a corrective control that will operate in the event of a fire and lessen the damage caused by the fire is sometimes discussed with building occupants. Sprinklers shouldn't be used in computer rooms, according to tenants of buildings with computer systems. Fire engineers would often refute the arguments by stating that "water causes damage, but fire destroys" even if they are aware that water may damage computer equipment. Although this analysis is accurate because sprinklers do prevent complete devastation, it is always important to carefully assess the drawbacks and unforeseen effects of adding more controls [8].

Direct Commands

gives a succinct explanation of the characteristics of directive controls. Organizations will be acquainted with the directive controls since employees will need to be instructed on how to do certain activities correctly. Documented processes, together with knowledge, training, and instruction, may be seen as directive controls if activities carry a certain amount of risk. Therefore, regardless of the existence of other kinds of controls, directive controls are likely to be in place for the majority of risks. The obligation to wear personal protection equipment while engaging in potentially hazardous tasks is an example of a directive control. In order to guarantee that the equipment is utilized appropriately, staff members will need to be educated in its proper usage and will need some degree of oversight.

The benefit of directive controls is that the personnel may get regular staff training and instruction during which the risk control needs can be communicated. However, directive controls, particularly when it comes to threats to health and safety, constitute a low degree of control that may need ongoing monitoring to verify that the proper processes are being followed. Directive controls will always be a part of the overall risk management strategy used by every business, despite the fact that they are an unsecure and unreliable technique of risk control on their own. For every company, creating processes, procedures, and protocols is crucial. However, there is a chance that the organization will be more open to claims of inadequate risk management if the designed processes are not put into use. The organization's development of comprehensive risk control processes is a sign that hazards exist and must be controlled. The organization won't be able to justify itself by saying that it was unaware of the hazards if the processes aren't put into place, however. It is clear how important and valuable directive controls are. The paper talks about business continuity planning and the need of giving staff clear instructions on crisis management as the first priority, followed by recovery from the catastrophe, and then assuring company continuity. According to the discussion in the paper on insurance and risk transfer, contracts, including insurance policies, are also a kind of directive control. All contract outlines in writing how parties are to behave in the event that a certain set of circumstances, like an insurance claim, occurs.

The fact that directive controls are often implemented as an instant reaction to an unanticipated occurrence is a crucial component of these controls that is sometimes missed. The hierarchy of controls is a representation of the desired scenario under current conditions. The sequence in which additional restrictions are added, however, may alter somewhat after the unexpected has been discovered. If the occurrence poses an immediate danger, particularly if it poses a safety concern, the first reaction is likely to entail imposing directive controls and/or preventative controls. This quick action will then make it possible to create and put in place remedial controls once the new set of circumstances become obvious and/or stabilize [9].

Investigatory Controls

An outline of the types of detective controls. Detective controls, as implied by the name, are those methods used to determine whether a danger has manifested. Even if it is not always satisfying, it is sometimes acceptable to discover a threat after it has already developed. Other safeguards could sometimes fall short of totally eradicating the possibility of a danger coming to pass. Detective controls, such as checking inventory or assets to make sure they haven't been taken without permission, are an example. Exercises in bank reconciliation may find fraudulent transactions. Additionally, post-implementation evaluations might identify project-related lessons that can be used moving forward. The review and monitoring activities carried out as part of the risk management process are directly tied to detective controls.

CONCLUSION

One benefit of detective controls is that they are often easy to use. In any event, they are crucial in many situations when the company has to be alerted quickly when another risk management strategy has failed. The drawback of the detective controls is that by the time they are

discovered, the danger will already have occurred. Of course, one may argue that the existence of investigative measures will dissuade some people from seeking to get around other risk controls. Scam detection is often only achievable after the scam has already occurred. However, there are significant benefits to fraud detection early on, since this may help to lessen the form and breadth of the crime and close the door to future fraudulent acts of a similar sort. Introducing new financial controls at a charity is covered in the text box. There is room for the application of investigative controls even in health and safety measures. There are risks connected to certain employment tasks that may result in lifelong and catastrophic health problems. Employees will be recognized with these occupational ill health disorders early and additional exposure may be prevented by using detective controls to recognize the early signs. Early diagnosis of lung illness from dust exposure, skin disorders like dermatitis, and eventually deafness brought on by industrial noise exposure are a few examples of these sorts of controls in health and safety.

REFERENCES:

[1] L. Yu, C. Chen, Z. Niu, Y. Gao, H. Yang, and Z. Xue, "Risk aversion, cooperative membership and the adoption of green control techniques: Evidence from China," *J. Clean. Prod.*, 2021, doi: 10.1016/j.jclepro.2020.123288.

[2] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for Risk-based access control model for IoT," *Internet of Things (Netherlands)*, 2019, doi: 10.1016/j.iot.2019.100052.

[3] N. A. Manab and N. A. A. Aziz, "Integrating knowledge management in sustainability risk management practices for company survival," *Manag. Sci. Lett.*, 2019, doi: 10.5267/j.msl.2019.1.004.

[4] M. Vij, "The emerging importance of risk management and enterprise risk management strategies in the Indian hospitality industry: Senior managements' perspective," *Worldw. Hosp. Tour. Themes*, 2019, doi: 10.1108/WHATT-04-2019-0023.

[5] W. O. Anyim, "Internal Control and Risk Management System in University Libraries: Applications, Techniques and Limitations.," *Libr. Philos. Pract.*, 2020.

[6] M. Urbański, A. U. Haque, and I. Oino, "The moderating role of risk management in project planning and project success: Evidence from construction businesses of Pakistan and the UK," *Eng. Manag. Prod. Serv.*, 2019, doi: 10.2478/emj-2019-0002.

[7] A. J. Card, J. R. Ward, and P. J. Clarkson, "Generating Options for Active Risk Control (GO-ARC): introducing a novel technique," *J. Healthc. Qual.*, 2014, doi: 10.1111/jhq.12017.

[8] N. Z. Elden, M. S. R. B. A. Hamid, C. B. Cheong, S. S. A. Al-Shami, A. Elzamly, and M. Doheir, "New theoretical framework corporate social responsibility: The case of islamic development bank's sustainable social program," *Opcion*, 2019.

[9] A. Elzamly *et al.*, "Assessment risks for managing software planning processes in information technology systems," *Int. J. Adv. Sci. Technol.*, 2019.

CHAPTER 16

FUNDAMENTALS ROLE OF INSURANCE AND RISK TRANSFER

Manjula Jain, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-jainmanjula776@gmail.com

ABSTRACT:

Risk transfer and insurance are essential elements of risk management plans for both people and businesses. Risk transfer, as opposed to insurance, includes transferring the risk of future loss to another party via contracts or other agreements. Insurance entails doing this in return for a premium. An overview of insurance and risk transfer, as well as their significance in risk management, is given in this paper. The list of important insurance categories includes life, health, and property and casualty insurance. It describes how insurance plan's function and how they may be altered to fit the particular requirements of people and organizations.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

One of the key risk management strategies for hazard hazards is risk transfer. This transfer, which often goes via insurance, is known as risk financing. The core tenet of insurance is that the insurance company has a contractual obligation to pay a certain amount of money should particular conditions or occurrences materialize. Insurance policies may provide that the insurance provider must cover direct losses incurred by the insured. This first-party insurance covers both bodily injury and property damage. Other forms of insurance obligate the insurance company to compensate third parties that suffer harm or lose money as a result of the insured's actions. Third-party insurance comprises public/general liability and third-party automobile insurance. Contracts for insurance are made in the best possible faith. It follows that the insured party must provide all information pertinent to the insurance arrangement. The insurance company or underwriter has the right to stop offering insurance coverage and to stop paying claims if this information has not been provided.

The employment of insurance as a risk transfer method is not without its benefits and drawbacks. The fact that insurance offers indemnification against an anticipated loss is one of its benefits. Insurance helps lessen the uncertainty around potential hazard situations. Due to the possibility that the loss might exceed the cost of the insurance, it could benefit the insured financially. Finally, insurance may provide access to specialized services in the cost of coverage. These services might include loss prevention guidance. The drawbacks include the frequent delays encountered in receiving payment of an insurance claim and the potential challenges presented by accurately estimating the financial consequences of the loss. The amount of the coverage that has been obtained and the precise terms and conditions of the insurance contract may be in

question. Finally, the insured can find it challenging to determine the right extent of indemnity for liability risks. Underinsurance and the consequent inability to fully pay claims might stem from this. When a company wants to shift the financial burden of a risk occurrence, there are options outside insurance. Alternative risk transfer or alternative risk financing approaches are other names for alternatives to insurance. Options for risk financing that an organization has are as follows:

1. Standard insurance.
2. Risk transfer via a contract.
3. Insurance businesses with captives.
4. Risk pooling in mutual insurance firms.
5. Financial instruments and derivatives.
6. Substitute risk financing techniques; and
7. Bonds for single premium insurance.

The financial effect of the losses may be decided to be retained in part by the organizations. Risk retention may be accomplished by creating a captive insurance firm, choosing not to cover a particular risk exposure, or accepting a high excess or deductible on an insurance policy. Several businesses with comparable risk exposures can want to establish a combined captive insurance company. This is often described as risk pooling or founding a mutual insurance business. A risk-sharing or risk-transfer strategy is insurance. It stands for a risk-related after-the-fact cost minimization approach. In situations where liability insurance is legally required or catastrophic losses are probable, insurance is crucial for low-probability/high-impact risks like asset destruction or the payment of liability expenses. Insurance is provided for the cost of putting disaster recovery plans and business continuity plans into place as well as for asset repairs. In order to offset the higher operating costs, insurance may also be acquired.

Background of Insurance

It is possible to trace the origins of insurance all the way back to Chinese and Babylonian commerce. There is evidence that by the mid-twenties, marine insurance had spread across the European maritime states. The current insurance sector was created somewhat recently, as a result of the Great Fire of London. In London, a coffee shop named Lloyd's was established. This venue served as a gathering place for parties looking to insure cargoes and ships as well as those looking to finance such endeavors [1].

The insurance industry has evolved quickly throughout the years. Insurance policies were signed by people whose names and the amount of risk they were willing to accept were written underneath the insurance proposal before incorporated corporations were created. Large fires were often the key calamities that sparked the growth. The Chicago Fire of demonstrated the expensive nature of fires in metropolitan places and the need for insurance. There was a large fire in New York in. The box on the next page goes into more information about the 1993 Chicago Fire. Some insurance plans also included protection for dependents in the event that the household's primary breadwinner passed away. Through the century's development of friendly or benefit organizations, these agreements took on a more structured shape. The history of liability

insurance is relatively recent, going back just maybe a few years. Many nations now have mandatory liability insurance laws, which have only been in place for a few short years. In most nations, mandatory liability insurance is often limited to motor third party, employers' responsibility, or workers' compensation [2].

DISCUSSION

Behind a Chicago house, a cowshed caught fire. The summer had been exceptionally dry, and the fires swiftly spread from home to house before spreading to neighboring streets. The commercial area was engulfed by the flames as it swept from the south-west to the north-east. Chicago, which was formerly the world's center for the production of timber, was mostly made of wood. The financial district of Chicago was spectacular. The city prospered as a result of the railroad's growth and the post-American Civil War economic boom. But the blaze tore across the city's four square miles, destroying factories, shops, railroad stations, hotels, theaters, and banks in addition to other structures. Nearly all of the city's printing and publishing was destroyed by flames as they torched ships in the Chicago River. Chicago's reconstruction was a huge undertaking. American and European insurance firms responded to the challenge and came up with the funds required to cover the losses. Chicago's libraries received thousands of donated books as well as $million in relief contributions from American and international cities. Soon after, Chicago started to draw businesspeople, entrepreneurs, and renowned architects who discovered ways to profit from the restoration operations [3].

Many forms of Insurance

The many insurance coverage options that a company may need. Generally speaking, an organization will want to get insurance coverage for three reasons. The following are some reasons to get insurance, in conclusion:

1. Required contractual and legal duties;
2. Profit and loss protection for the balance sheet;
3. Asset protection for and benefit to employees.

Organizations may choose to obtain insurance in addition to the required education. This choice will be made in light of the risk assessment and if the kind and degree of risk fall within the organization's risk tolerance. When determining whether to get insurance, other crucial factors to take into account include the premium cost and the scope of the insurance coverage. Insurance is often obtained to cover low probability/high magnitude hazards like floods, storm damage, and large fires. Think about the insurance requirements of a publisher. The business is aware that it must get vehicle third-party insurance and employers' liability insurance in order to comply with regulatory requirements. The wholesalers also mandate that the corporation acquire libel and slander insurance for magazine distributors. The firm must buy property damage, business interruption, credit risk, and goods in transit insurance in order to safeguard the balance sheet and profit and loss account.

The publisher may also choose to provide life, critical sickness, and private medical insurance to employees, in addition to personal accident and travel insurance. Directors' and officers' liability

(D&O) insurance will be obtained on behalf of the company's directors. The organization made careful to implement an insurance policy that only offers coverage when it is required, suitable, and economical by doing this review in cooperation with insurance brokers [4].

Assessment of Insurance Requirements

A checklist that businesses may use to determine what kinds of insurance are necessary. There are many different insurance options, and the particular activities and characteristics of the organization will help determine the level of insurance that should be obtained. Even when an organization has elected to buy a certain form of insurance, there are situations when it may not be offered at a reasonable price due to a scarcity of insurance capacity.

In recent years, companies have started to look at the whole spectrum of risks they confront. The amount of insurance that a business wants to buy has been carefully reviewed as a consequence of the enterprise risk management approach to risk. It may not be prudent to obtain insurance for only those few risks, for instance, if a project has large risks but insurance is only available for a small number of risk exposures. For some firms, the usage of insurance as a risk control tool has decreased as a result of the enterprise approach to risk management. One of the characteristics of the insurance market is that insurance premiums vary greatly throughout the course of various market cycles. Over a period of maybe a year, the market will cycle between soft market conditions (low premium) and harsh market conditions (high premium). Organizations will often purchase less insurance and rely more on a captive insurance firm when premium costs are high. Organizations will buy more insurance when premium prices are low because it is more cost-effective [5].

The insurance premium that the organization must pay determines the cost of insurance. The amount of self-insurance required by the policy, including any excess or deductible, makes up a second factor in the price. This implies that, in the event of a claim, the organization will be required to cover the first portion of the claim prior to obtaining any funds from the insurance provider. Limitations, warranties, and exclusions are often included in insurance plans. These will specify the conditions under which claims will be rejected. The company buying the insurance must thoroughly investigate these coverage concerns to make sure that there is sufficient coverage. The only benefit of purchasing insurance is the promise that, should one of the foreseeable occurrences take place, claims would be paid. When choosing which insurance company to choose, it will be crucial to consider the history of that insurance business with regard to the settlement of claims and its reputation.

One insurance provider may not be willing to extend coverage up to the full value of such assets for extremely big firms with significant assets. The capacity that the insurance company is willing to supply in proportion to the value of the assets or exposure that needs to be protected is something that the organization will need to consider when purchasing insurance. In addition to insurance, many insurance firms provide other services. These might include support with business continuity planning and loss control services. The insurance firm's skills in these areas may have a significant role in the decision of which insurance company to choose. The financial stability, reputation, and competencies of the insurance provider are becoming more crucial

factors for insurance consumers. Because of the way insurance companies function, they collect premium payments at the start of the policy but do not have to make claims payments until some, sometimes a long time, after the incident or loss. For insurance businesses, this results in a favorable cash flow situation and the chance to generate investment income [6].

However, the diversification of insurance firms into higher-risk financial ventures has caused several of them to suffer substantial losses and have their financial standing downgraded. Additionally, investment income has decreased due to low interest rates and the underwhelming performance of the stock markets. As a result, while choosing an insurance provider, consumers need to pay more attention to the financial health or credit rating given to various insurance providers. Insurance claims and their critical significance in connection to insurance have previously been mentioned. The only reasons an organization purchases insurance, apart from regulatory and customer needs, are to pay for the higher cost of operation, recoup the expense of fixing the harm, and restart the firm after a loss. The third-party injured party will file the insurance claim with regard to third-party insurance. Insurance claim management may be a meticulous and forensic process. Claims management sometimes entails intricate legal processes including specialized engineers and accountants. Property damage claims may be simpler to calculate, but business interruption claims may be extremely difficult to assess and agree upon. If a company has developed proper business continuity plans, both the amount of the insurance claim and the interruption to operations will be significantly minimized. In terms of risk management, relying just on insurance to cover all losses is insufficient. Every corporation should consult its business continuity plans to make sure that measures are in place to guarantee the least amount of interruption in the event that an unfavorable event occurs [7].

Concerns around insurance policy compliance are becoming more and more prevalent. The majority of nations have enacted insurance premium taxes, which must be paid on a national level when a business has assets spread across many nations. Taxes may sometimes be due on a municipal or regional level, with the proceeds going to the fire department in the area. The production of the insurance contract prior to the start of the policy term has also been a source of compliance problems. 'Contract certainty' is a term that is often used to describe the timely issue of insurance policies. Concerns about compliance also include whether a policy is acknowledged, recognized, or accepted in every nation where the corporation does business. The activities of captive insurance businesses may sometimes be constrained by this. An insurance policy created by a captive insurance firm or another non-admitted insurer may not be recognized as legitimate in certain countries.

Insurance firms with captives

An entity that is not normally engaged in the insurance industry owns a captive insurance firm. By utilizing its own internal financial resources to finance certain kinds of projected losses or insurance claims, a captive insurance firm serves the objective of providing insurance capacity for the organization. The firm that owns a captive insurance company is sometimes referred to as the captive's parent company or just the parent company. Captive insurance firms are often situated in a place with a supportive legislative and accounting environment that promotes the formation of captive insurance companies. Ireland, Guernsey, the Isle of Man, Gibraltar, Malta,

Luxembourg, Bermuda, and other jurisdictions serve as home bases for captive insurance businesses. Captive insurance firms may have a very diverse range of characteristics. Theoretically, such a corporation may create insurance contracts for clients in other nations, although regulatory considerations relating to non-admitted policies would need to be properly taken into account. A captive insurance firm is more likely to function as a re-insurer, giving insurance protection to the primary insurance provider chosen by the organization. Through this arrangement, the organization's insurance company, also known as the fronting insurer, is given the ability to be reimbursed for specific claims up to the financial limitations or risk retention levels established with the captive insurance company.

The organization will take deductibles or excesses on its many classes of insurance, and they may change per class of insurance. This is a typical financial structure for a complicated insurance program. Following that, the captive insurance firm will accept the subsequent amount of loss up to an agreed maximum for each single loss as well as up to an agreed limit for total or cumulative losses during the policy year. The portion of higher losses that exceeds the captive insurance company limit will subsequently be paid by the main or fronting insurer. Once the cumulative totals for the captive have been exceeded, the fronting insurer will be liable for covering all losses. The main or fronting insurer for statutory types of insurance will be liable for covering the full amount of the claim. In the event that the captive insurance company is responsible, the fronting insurer will then recoup the funds from the captive insurance business. Although the fronting insurance business often avoids this by delaying payments until it has received money from the captive insurance firm, it might still pose a credit risk.

Captive Insurance Firms' Function

Some captive insurance providers provide insurance for the parent firm as well as taking on business from outside clients. Extended warranty insurance plans provided by sellers of electrical products are a classic illustration of a captive insurance firm offering third-party insurance. Another example is the establishment of a captive by travel agencies to provide clients travel insurance in the event of cancellation. The consumer will acquire a policy from a reputable insurance provider, but the captive will finance the insurance via reinsurance of the fronting insurer. The travel agency should make money from its clients and get additional revenue as a result of putting up this agreement. The following are some benefits of captive insurance companies:

Because captive insurance businesses often set lower rates, savings in total insurance costs may be realized. Access to reinsurance markets, where premium prices and risk capacity may be beneficial, is possible for the captive insurance firm. It is possible to increase risk awareness and concern for loss prevention by exposing people to the expense of insurance claims. The captive insurance firm is able to provide more insurance coverage than what is given in the commercial market. A captive insurance firm may provide certain tax advantages, albeit they have diminished recently [8].

The following are some drawbacks of captive insurance companies:

Insurance claims that would have previously been settled by the commercial insurance market will now be exposed to the captive. To guarantee the captive insurance company's proper solvency, the parent organization must provide money. When a captive pays significant losses, the losses are added to the parent company's balance sheet and are eventually covered by the company. Captives writing business in other regions will likely be conducted on a non-admitted basis, which might provide regulatory challenges. The administration of the captive by staff at the parent head office may entail significant administrative expense, time, and effort. The text box below is an illustration of how captive insurance company benefits are perceived. Guernsey, Ireland, and Malta are just a few of the many acceptable jurisdictions for captive insurance firms [9].

CONCLUSION

The relevance of risk transfer and its different forms, such as indemnity provisions, hold harmless agreements, and insurance contracts, are also covered in the paper. The paper describes how risk transfer may assist people and businesses in managing hazards that cannot be avoided or diminished. The paper also emphasizes how crucial it is to comprehend the restrictions placed on risk transfer and insurance. It illustrates how risk transfer may not always be feasible or advantageous and how insurance plans may have exclusions and restrictions that may not cover all sorts of losses. In general, the stresses the significance of risk transfer and insurance as crucial elements of risk management techniques. It emphasizes how important it is for people and organizations to comprehend the many insurance and risk transfer choices available, to tailor their coverage to their unique requirements, and to be fully aware of the limits of these techniques.

REFERENCES:

[1] O. S. F. Olajide Solomon Fadun, “Insurance, A Risk Transfer Mechanism: An Examination Of The Nigerian Banking Industry,” *IOSR J. Bus. Manag.*, 2013, doi: 10.9790/487x-07493101.

[2] E. J. Treby, M. J. Clark, and S. J. Priest, “Confronting flood risk: Implications for insurance and risk transfer,” *J. Environ. Manage.*, 2006, doi: 10.1016/j.jenvman.2005.11.010.

[3] Diara Md. Jadi, Norlida Abdul Manab, and ShahrulNizam Ahmad, “Insurance as a Risk Transfer Mechanism in Small and Medium Enterprises (SMEs),” *Int. SME Conf. (ISMEC 2014)*, 2014.

[4] A. Kiohos and M. Paspati, “Alternative to Insurance Risk Transfer: Creating a catastrophe bond for Romanian earthquakes,” *Bull. Appl. Econ.*, 2021, doi: 10.47260/bae/811.

[5] F. Kong, “How to understand the role of insurance mechanism in a global pandemic?,” *Int. J. Environ. Res. Public Health*, 2021, doi: 10.3390/ijerph18136743.

[6] V. Njegomir and R. Maksimović, “Risk transfer solutions for the insurance industry,” *Econ. Ann.*, 2009, doi: 10.2298/EKA0980057N.

[7] R. Hohl, Z. Jiang, M. Tue Vu, S. Vijayaraghavan, and S. Y. Liong, "Using a regional climate model to develop index-based drought insurance for sovereign disaster risk transfer," *Agric. Financ. Rev.*, 2021, doi: 10.1108/AFR-02-2020-0020.

[8] H. Fu, J. Li, Y. Li, S. Huang, and X. Sun, "Risk transfer mechanism for agricultural products supply chain based on weather index insurance," *Complexity*, 2018, doi: 10.1155/2018/2369423.

[9] J. P. Sarmiento and A. M. Torres-Muñoz, "Risk Transfer for Populations in Precarious Urban Environments," *Int. J. Disaster Risk Sci.*, 2020, doi: 10.1007/s13753-020-00252-3.

CHAPTER 17

STUDY OF THE BUSINESS CONTINUITY MANAGEMENT

Aditya Sharma, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-adityahr2018@gmail.com

ABSTRACT:

Business continuity management (BCM) is a process that ensures an organization's critical operations continue to function in the event of a disruption. This process involves identifying potential risks to the organization, developing plans and procedures to mitigate those risks, and testing and maintaining those plans to ensure they remain effective. This provides an overview of business continuity management and its importance to organizations. Risk assessment, business effect analysis, recovery plans, plan preparation, and testing and maintenance are among the BCM's essential components that are included in the. It illustrates how these components combine to provide a thorough BCM framework that aids businesses in efficiently managing and mitigating risks.

KEYWORDS:

Enterprise, mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Business continuity planning (BCP) and disaster recovery planning (DRP) are topics that have recently attracted a lot of attention. Around the globe, many standards have been released. This exemplifies the significance of BCP as a crucial component of risk management. The potential for substantial disruption presented by catastrophic weather occurrences, terrorist attacks, civic situations, and the worry of a flu pandemic have all escalated anxiety. BCP, to put it simply, is how an organization is ready for any future catastrophes that might threaten its viability. The variety of crises that should be addressed will vary from local occurrences like fires to regional disruptions like earthquakes or incidents involving national security, and it will also encompass global occurrences like terrorism and pandemics.

A comprehensive management process that identifies potential threats to an organization and the effects on business operations those threats, if realized, might have. It also provides a framework for constructing organizational resilience with the capability of an effective response to protect the interests of its key stakeholders, reputation, brand, and value-creating activities. A well-defined, tested, and documented disaster recovery plan should be in place in the event of a critical crisis, such as the loss of access to facilities or the failure of a significant portion of an organization. Such plans typically cover the provision of alternative premises (if necessary) and other facilities, as well as outlining plans for communications with employees and with other

stakeholders like suppliers, customers, and the media during a crisis. Such plans invariably center on recovering access to IT systems and data, but they also frequently cover the provision of alternative premises (if needed) and other facilities.

Building on this, business continuity plans include longer-term strategies for returning to "business as usual" in the immediate wake of a catastrophe. A business continuity strategy is crucial for minimizing the effects of a risk occurrence. Plans for minimizing incident-related harm and keeping recovery costs in check should be part of the strategy. Plans for disaster recovery are one kind of BCP. The organization will require emergency procedures in the event that a computer system malfunctions or data becomes damaged in order to guarantee that the data can be retrieved and/or that the organization can continue to operate.

A more comprehensive requirement for a specialized strategy to handle any crisis that may arise as a consequence of an operational catastrophe could also exist. A crisis plan will also be concerned with external stakeholders and actions to manage the associated stakeholder reaction and expectations, which is the main distinction between a disaster recovery plan and a crisis management plan. The disaster recovery plan will primarily be concerned with actions to restore the organization's infrastructure.

Because the computer systems process orders, schedule printing, and handle billing, IT systems are essential to the running of a printing business. In the event of a significant IT breakdown, it could be desirable for such a corporation to make arrangements for a mobile emergency computer facility to be accessible. If this choice is made, a contract should be made with a third-party organization for a replica computer to be transported to the business's location in a trailer. The second computer would then be attached, and the operations would be managed by the trailer's second computer. The availability of data from backup drives, which should be made at least once per day and perhaps more than once per day, will be crucial to the success of this arrangement. The nature of business continuity and disaster recovery in terms of the sorts of controls that they represent has been heavily debated. While the Scottish Government views these measures as directive, HM Treasury in the UK views them as corrective. Disaster recovery plans may be thought of as controls that are mainly focused on limiting damage, while business continuity controls are more concerned with cost containment [1].

Perhaps it is not fundamentally relevant to debate whether disaster recovery and BCP should be seen as kinds of control. The crucial point is that business continuity and disaster recovery plans are concerned with the conditions in which the event is occurring or has already happened. In that sense, DRP and BCP may be seen as reactions for when the event happens and do not assess how probable the occurrence is to occur. The usage of seat belts in automobiles serves as an example in daily life. For protection in case of a traffic collision, passengers in automobiles wear seat belts. The wearing of seat belts is obligatory in many nations, and passengers are not obliged to consider their likelihood of being involved in a car accident when determining whether to buckle up for a given trip.

Today, many companies hold the belief that BCP should be divided into three parts. The crisis management plan should be activated as soon as a big event occurs to guarantee an adequate

reaction to the crisis and, in particular, to guarantee that stakeholders are informed of the situation. To minimize the reputational harm caused by the occurrence, this will need efficient communication with all parties. The firm will subsequently attempt to recover from the incident by putting its disaster recovery strategy into action. However, the business will still need to take into account the continuing crisis management when the disaster recovery plan is put into practice. The company has to make sure that the disaster recovery plan's execution is seen as the second, though sometimes overlapping, and stage of reacting to the crisis. In certain cases, the disaster recovery plan won't even be ready for implementation until the current crisis has been resolved[2].

The organization will be able to focus on the third and more general operational problem of business continuity after crisis management measures are well under way and the disaster recovery plan has been implemented. A significant traffic collision that blocks a major road or highway is an illustration of this three-stage process. The emergency services' first reaction will be to deal with the crisis, which might entail injuries to individuals as well as, under some conditions, a car fire and/or other traffic moving too quickly in the direction of the event. The disaster recovery phase, which includes removing the damaged cars and/or fixing the road surface and crash barriers, may be put into action after the immediate crisis has been handled. Reopening the route or dealing with the business continuity issue can only be done once these two steps have been finished.

The necessity for crisis management measures would extend to the road haulage or transportation firm involved in the event if the road traffic accident included commercial vehicles or if it was claimed that a driver from the specified company caused the incident. To show social responsibility and to guarantee minimal reputational harm, the corporation should implement its crisis management strategy. The road haulage firm could decide to take action in the midst of the crisis to assist other parties, such as the families of any drivers who may have suffered injuries as a result of the occurrence. Provides a timeframe and cost example for catastrophe recovery; this is covered later in this paper. The whole duration of interruption (from point A to point D) and maybe beyond is covered by the requirement to guarantee competent crisis management and good communication with stakeholders [3].

DISCUSSION

Creating the Reaction

The risk profile may be raised by enhancing operational practices and processes, introducing alternative business strategies, utilizing risk financing tools (such as insurance), and developing BCPs easily when using several management systems. The wording "actions to address risks and opportunities" has been substituted for "preventive action." Setting goals, keeping track of performance, and establishing measurements that link business continuity with strategic management thinking are all given far more importance by ISO. The following are the guiding concepts that should be included in every effective BCP:

1. Comprehensive
2. Cost-effective

3. Practical
4. Effective
5. Maintained;
6. Practiced.

To guarantee that the plan can completely resume regular company operations, it is crucial that the BCP encompass all of the organization's activities and facilities. The plan's cost-effectiveness and proportionality to the risk exposures are also crucial. Staff and anyone engaged in the plan's implementation must find the BCP to be usable and simple to comprehend. Overall, the BCP must be successful in that it will establish roles for ensuring the prompt return to regular operations and recognize the necessity of certain business components or services [4].

The BCP has to be tested, maintained, and practiced in order to ensure that it will be successful. The intended functioning of the strategy must be understood by every employee, and training will need to be given. The business continuity strategy should be improved upon by taking into account the lessons discovered during testing and practice. To make sure that business continuity plans are suitable and successful, testing is a crucial step. Testing plans, however, may be time-consuming, expensive, and disruptive in certain cases. It is even clear from the simplest of examples—a fire evacuation practice from a building that testing new processes will always interfere with business as usual.

Enduring Business Success

Gaining a detailed knowledge of the company and its connections with both internal and external parties is the first step in effective BCP, DRP, and crisis management. Identifying the organization's goals and major dependencies will be a part of attaining this insight. Understanding core organizational roles and locating significant resources are crucial. It is necessary to identify business risks and make judgments about the likelihood that they will materialize before developing a BCP plan. Understanding how risks affect the firm is also essential. These evaluations should then be used to decide which risks should be addressed first and to determine the possibility and consequences of those risks materializing. Making choices on the right risk responses will be necessary for creating and executing a BCP and the proper controls for each of the identified hazards. The Ts of hazard risk management have previously covered the variety of risk responses that are accessible. The choice of whether to tolerate, treat, transfer, or eliminate each of the key dangers will need to be made.

A business continuity management (BCM) culture must be developed and ingrained inside the company, which calls for effective communication. The business continuity operations will need the participation of all stakeholders, who must also comprehend the rationale for the creation of the BCP and DRP. It is crucial to stress the role that each employee plays in preventing accidents that might cause significant disruption. The mission-critical activities, together with the most important roles and responsibilities, should be recognized while creating the BCP. These might be created as detailed checklists and instructions. By developing a program to test the plans, evaluate them, and alter them as required, as well as train people to better understand the plans, it is crucial to exercise, maintain, and review the BCP. At the very least once a year, as well as

after a test of the plans, BCP and DRP should be evaluated. Additionally, any lessons learned from an occurrence should be integrated into the plans.

An illustration of the value of BCP is the flu pandemic of in. In numerous nations throughout the globe, organizations and people received advice and direction. The essential ideas in that advice are outlined in the box below, along with the real-world effects of the flu pandemic on business continuity. Many nations agree that a pandemic is among the most destructive events that may happen to a nation. This example is based on a broadcasting company that experiences a significant interruption at its primary broadcasting facility at time point A. Broadcasting will restart quickly thanks to the catastrophe recovery strategy, although it could only be an emergency broadcast. On the timeline, the emergency broadcast begins at position B. The organization will be able to start full broadcasting of its regular service from a different site after a brief time of emergency broadcasts. For instance, the broadcaster may relocate the London broadcast facilities to Manchester studios. But doing so will result in the loss of the Manchester capacity. Point C, the relocation to Manchester, saw a significant improvement in the quality of service, but since the Manchester broadcast facility was lost, it is no longer at the prior standard.

Since the event, there has been an increase in operating costs. The expense of completing the catastrophe recovery plan will be followed by additional charges for emergency broadcasting and finally the relocation to Manchester. During the time when broadcasts are made from Manchester, additional expenses will be incurred for staff housing in temporary quarters and more sophisticated technical equipment. A typical series of events for a company experiencing a significant crisis. The degraded service level will last for a while, and there will be an increase in operating expenses. If the additional operating costs do not exceed the indemnity term (the length of the interruption) specified in the insurance policy, insurance could be available to cover them. Unless particular expenses or losses are defined and covered, it is doubtful that insurance coverage will be available to cover any losses connected with a lower level of service from the time the event occurs until the point of complete recovery[5].

Impact analysis for business (BIA)

The completion of a business impact analysis (BIA) is essential to ensure that suitable business continuity plans and catastrophe recovery plans are in place. The effect of an interruption to each business function will be evaluated by the BIA in order to determine its criticality. The identification of suitable continuity techniques for each function will need the use of this knowledge. The risk assessment that is conducted as part of the entire risk management process is comparable to the BIA. The crucial distinction between a BIA and a BCP, however, is that a BIA places more focus on determining the relative relevance and criticality of each function than it does on identifying the potential events that could jeopardize that specific function. As a result, the risk assessment and the BIA are connected and may be completed concurrently. The risk assessment will assist in identifying the threats to the accomplishment of the business continuity goals. For a television corporation, achieving broadcasting continuity over % is probably the goal and could even be mandated by the licensing authority. An organized and methodical strategy is necessary for both risk assessment and BIA.

The following three goals for the business impact study are distinct ones:

Determine which tasks are mission-critical and how long it will take to recover if they are interrupted. The period during which the important functions must be resumed after the disruptive incident will be determined by this identification activity. Determine the probable effect and the resources needed for recovery within the agreed-upon timeframe. It is necessary to determine the business needs for recovering the crucial function. To establish the foundation for a business continuity plan, ascertain if the probable effect is within the organization's risk appetite. Additionally, it is necessary to specify the technological prerequisites for recovering the crucial function. The causes of disruption could serve as the foundation for the business impact study. Ps Conducting a BIA will become easier as the causes of disruption to an organization's activities are recognized. However, a business impact study' main emphasis would probably be on organizational processes and how they could be impacted. This appears particularly pertinent given that the ongoing nature of corporate operations protects the interests of important stakeholders, as well as the reputation, brand, and value-creating endeavors [6].

ERM and business continuity

Enterprise risk management (ERM) and BCP have a clear connection. ERM is concerned with the risks that the whole company faces, while BCP emphasizes the need for business continuity plans. The BCP method examines the consistency of operations across the whole business. Of course, maintaining continuity is a component of an ERM strategy. Therefore, it should be understood that although BCP is a component of ERM, it is not the whole of ERM activity. The business continuity and disaster recovery efforts should, however, be carried out as part of a larger ERM endeavor, where appropriate, since there is a strong resemblance in approach. The continuance of effective and efficient core business operations is the goal of both strategies. There is greater discussion on enterprise risk management. The foundation of ERM is that the risk assessment process is focused on the stakeholder expectations and the fundamental organizational procedures that fulfill those expectations. ERM's goal is to guarantee that the fundamental procedures are upheld. BCP is likewise built on the continuation of essential business operations. The focus of ERM is different in that it looks for risks that might affect the effectiveness and efficiency of key processes. The goal of BCP is to identify the crucial business operations that must be preserved in order to ensure the survival of the company. There are many similarities between this kind of ERM and BCP, and the techniques are complimentary.

One of a pharmaceutical company's primary functions is to always have prescription medications available. This fundamental process may be approached using an ERM strategy, and the risks that could cause disruptions can be found. The pharmaceutical business will have effectively merged the ERM and BCP techniques with a focus on meeting stakeholder expectations by adopting this risk management strategy. In addition to being a key part of business continuity, scenario planning also has wider implications for the effective implementation of enterprise risk management. The appraisal of the balance sheet capital that a financial institution would need in the case of challenges comparable to the global crisis is a part of scenario planning for financial institutions. 'Stress testing' is the term used to describe this kind of scenario preparation for financial institutions, and it is often a particular mandate of banking regulators.

The organization's internal and external contexts, as well as the business impact analysis, must be considered during scenario planning. Additionally, there is a close connection between crisis management and scenario preparation. Planning for disaster recovery and business continuity can account for predictable events, but it may be challenging to anticipate every potential catastrophe. As a result, one of the benefits of scenario planning is that it foresees very rare events and then pushes top management to come up with effective solutions. The organization's resilience may then be increased by implementing the lessons learned through scenario preparation. An method to scenario planning that the UK government's Cabinet Office supports in respect to the interruption of national infrastructure, such as the energy supply network, is described in the text box above.

Public Emergency

In many nations, local governments are required to make sure that local companies continue to operate in the case of a serious civil disaster. A natural calamity, such as floods or an earthquake, might cause the situation. As an alternative, it may be brought on by terrorism, unrest, an epidemic, or a pandemic. The ISO set of standards are related to social resilience, and their growing significance is also taken into account [7].

Numerous civic agencies provide business recommendations to help them with their BCP. For instance, the US government's website has useful information. Additionally, a number of trade organisations and small company associations provide useful advice on BCP, including what to do in the event of a civic emergency. Most municipal governments are required by law to react to civil emergencies. Facilities and equipment that might be beneficial in the case of a civic emergency may be found in factories and warehouses. Retail stores will also stock food and other items that may need to be distributed as emergency supplies. Food, bottled water, clothes, and blankets are among the supplies that may be beneficial in a civil disaster. Additionally, in the case of a civil emergency, such as the widespread floods that have increased in frequency in various European nations, schools and other public buildings may be needed as accommodations. Local disaster management agencies will gain from organizations being encouraged to establish plans to maintain business continuity since there will be fewer concerns and challenges for them to consider when the event arises [8].

CONCLUSION

The paper also emphasizes the need of incorporating BCM within the organization's broader risk management framework and the significance of senior management support for BCM. It addresses the advantages of BCM, such as its capacity to reduce interruption, uphold stakeholders' and customers' trust, and guarantee compliance with legal and regulatory standards. The paper also highlights the value of communication in BCM. To ensure that everyone is aware of the organization's BCM plans and processes, it underlines the need of excellent communication with stakeholders, including workers, customers, suppliers, and regulatory agencies. Overall, the paper highlights the crucial part that business continuity management plays in assisting businesses in efficiently managing and mitigating risks. To maintain the continued efficacy of the BCM process, it emphasizes the significance of a thorough BCM

structure, senior management support, integration with overall risk management, and good communication with stakeholders.

REFERENCES:

[1] A. M. Corrales-Estrada, L. L. Gómez-Santos, C. A. Bernal-Torres, and J. E. Rodriguez-López, "Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review," *Sustain.*, 2021, doi: 10.3390/su13158196.

[2] M. Labus, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, and S. Popović, "Adaptive e-business continuity management: Evidence from the financial sector," *Comput. Sci. Inf. Syst.*, 2020, doi: 10.2298/CSIS190202037L.

[3] D. Filipović, M. Krišto, and N. Podrug, "Impact of crisis situations on development of business continuity management in Croatia," *Manag.*, 2018, doi: 10.30924/mjcmi/2018.23.1.99.

[4] H. Chen, D. Tse, P. Si, G. Gao, and C. Yin, "Strengthen the security management of customer information in the virtual banks of hong kong through business continuity management to maintain its business sustainability," *Sustain.*, 2021, doi: 10.3390/su131910918.

[5] N. Suresh, G. L. Sanders, and M. J. Braunscheidel, "Business Continuity Management for Supply Chains Facing Catastrophic Events," *IEEE Eng. Manag. Rev.*, 2020, doi: 10.1109/EMR.2020.3005506.

[6] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," *Saf. Sci.*, 2016, doi: 10.1016/j.ssci.2016.06.015.

[7] F. Schätter, O. Hansen, M. Wiens, and F. Schultmann, "A decision support methodology for a disaster-caused business continuity management," *Decis. Support Syst.*, 2019, doi: 10.1016/j.dss.2018.12.006.

[8] M. Kato and T. Charoenrat, "Business continuity management of small and medium sized enterprises: Evidence from Thailand," *International Journal of Disaster Risk Reduction*. 2018. doi: 10.1016/j.ijdrr.2017.10.002.

CHAPTER 18

AN OVERVIEW ON CORE BUSINESS PROCESSES

Aditya Sharma, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-adityahr2018@gmail.com

ABSTRACT:

An overview of core business processes is essential for organizations to ensure that they operate efficiently and effectively. Core business processes are the key activities that an organization performs to deliver its products or services to customers. These processes are critical to the success of an organization, as they directly impact its ability to achieve its strategic goals and objectives. The main components of core business processes include planning, execution, and control. Planning involves identifying the goals and objectives of the organization and developing a strategy to achieve them. Execution involves carrying out the plan by allocating resources, managing activities, and delivering products or services. Control involves monitoring and evaluating performance to ensure that the organization is achieving its goals and objectives. Effective management of core business processes can help organizations to reduce costs, improve quality, increase efficiency, and enhance customer satisfaction. It also enables organizations to respond more effectively to changing market conditions, regulatory requirements, and customer needs.

KEYWORDS:

Enterprise, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Organizations often create distinct papers for their business and strategic goals. It is crucial to look at both of these sets of goals and consider how they relate to one another in order to make sure that risk management contributes fully to the business. Business goals often have an association with the organization's yearly budget. This budget will include information on expected sales as revenue and sales costs as expenses. The company's defined business delivery model, or business model for short, will serve as the foundation for the business goals of the organization. For instance, a membership group would look for sponsorship from companies that provide its members services. The business strategy and the yearly business goals will be fundamentally based on this kind of sponsorship money. The membership body will need to project revenue from sponsorship and membership subscriptions, as well as decide what services will be provided to members in exchange for their membership fees and what advantages will be provided to sponsors in exchange for their sponsorship fees.

The resilience and effectiveness of the business model are related to the risks that are tied to company goals. Events that might jeopardize sponsorship and membership revenue as well as events that could interfere with the provision of services and benefits should both be taken into

account when conducting a risk assessment of the yearly budget. The core of a business aim often has something to do with the company as it is right now. The crucial components of a company development model are listed in the box below. It is important to keep in mind that, as was covered in Paper, a company will have a current version of their business model. The yearly business plan and the company goals serve as the framework for the business model. In accordance with its long-term vision, the company will also have plans to improve and develop its current business model. By putting such short-term techniques into action, the current company model is created. The current operations, or "where the organization is now," determine the current business model. The majority of businesses are aware that the current business model cannot be sustained indefinitely. The firm will need to evolve if it is to meet its aims year after year. These advancements can include looking into more sponsorship possibilities, providing novel services and goods that will bring in more revenue, and enhancing the effectiveness of the current company strategy. The primary focus of this paper is the creation of the business model in order to achieve strategic goals, which may be referred to as the business development model.

It is vital to take into account a streamlined company growth model in order to situate risk management within the framework of business operations. Clearly stated fundamental components of a company growth model. An organization's first step is to choose the strategy it wants to implement. The organization's mission statement, business objectives, and stakeholder expectations will all be taken into account while determining the strategic goals. The organization has to develop a plan that will enable it to fulfill its mission statement. In other words, the organization's plan must be successful and efficient.

DISCUSSION

The tactics that will carry out the overarching plan must be determined once it has been developed. Projects or work programs will be necessary if the plan calls for modifying existing core processes or introducing new core processes. The organization's strategies should make sure that fundamental procedures are effective and efficient in order to get the required results in the most economical way. The continuation of regular, effective operations without any unforeseen disruptions is the intended condition of the organization with regard to operations. lays out the steps that were previously explained. One way to think of the strategy is as "where the organization wants to be." The company's operations review will gather data on "where the organization is now," and the strategies will outline "how the organization will get there." The business concept is being developed in three stages, with events at its core. In several instances, these

Model for Business Growth

Events will reflect potential dangers that could occur. The reporting of operational outcomes, as seen in Figure 1, is the other element of this company growth paradigm. The company may track progress achieved in relation to the strategy, tactics, operations, and compliance via actions and occurrences, which might be positive, negative, or mundane. These behaviors and occurrences have an influence on the organization's capacity to maintain fundamental business activities that are effective, efficient, and compliant. The firm will use compliance core procedures to

guarantee that it complies with its legal and contractual duties, even when they aren't addressed expressly. Operational core processes and compliance core processes should both serve as the foundation for all organizational activity[1]. A strategy-based approach based on opportunity management will be needed for strategy identification. It will be vital to manage control risks and pay attention to uncertainties while delivering strategies, which is often done via projects. The successful management of hazard risks will demand special attention to the delivery of effective and efficient operations.

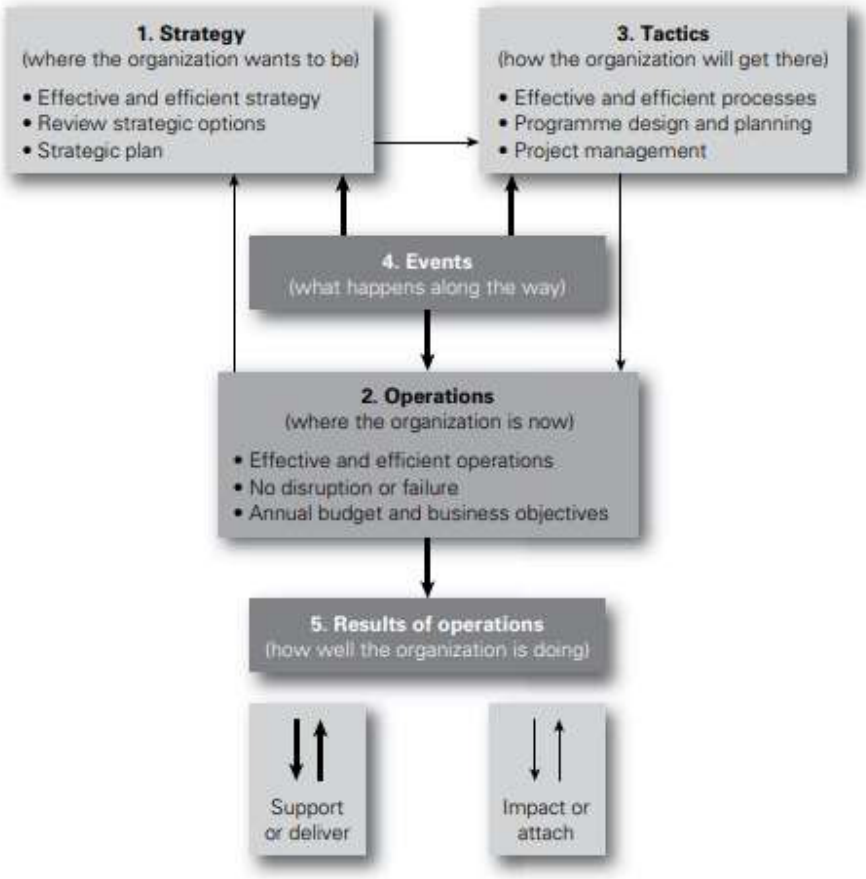

Figure 1: Illustrate the Business development model.

Business Process Types

Existing business procedures inside an organization may be enough for achieving the firm's goals in terms of producing the necessary revenue and managing expenditures. The goals must be related to regular business processes within the company in order to guarantee that risk management has a sufficient input into the achievement of business objectives. Organizations sometimes fail to set up "business as usual" goals, however. The majority of goals often relate to the execution of the organization's strategic strategy and are annualized change objectives. In conclusion, goals that address strategy, tactics, and operations must be thoroughly articulated for risk management to effectively contribute to an organization's success [2].

A core process is one that is essential to the organization's ongoing performance (or even survival). The organization's core processes make sure it can accomplish its purpose, meet its corporate goals, and meet the expectations of its stakeholders. Each fundamental process adds value and is made to meet at least one stakeholder expectation. Core processes may be divided into four categories. These procedures were created, put into place, and are being monitored to guarantee the following:

1. The creation and execution of a strategy.
2. Project, project management, and improvement management.
3. The maintenance and supervision of normal activities;
4. Measures that are intended to guarantee compliance.

An activity is a specific job or task that is integrated into the procedures that meet the expectations of the stakeholders. Although the procedures themselves are planned and meant to benefit the company, the inclusion of more tasks will raise costs. Therefore, the task is to create efficient and effective core procedures. After stakeholder expectations have been defined, core procedures may be implemented to guarantee that these expectations are met to the standard that the company has determined is suitable. No company will be able to completely satisfy all stakeholder expectations to the degree that is sought. This often occurs as a result of conflicting expectations among various stakeholders. The following procedures inside the organization's core are likely to have flaws or holes in them:

There can be issues with how strategy is created and implemented. Due to these flaws, the company won't be able to maintain its position as the industry leader. They cause a leadership gap to develop. The administration of methods, like as projects and product or service improvements, may have flaws. Due to these flaws, the company won't be able to compete. They cause a disparity in the level of competitiveness. There could be flaws connected to failing to maintain normal operations' efficiency, continuity, and monitoring. Due to these flaws, operations won't be able to remain productive. They result in a gap in efficiency. There could be flaws in the actions intended to satisfy the organization's legal obligations. Due to these flaws, reputation will not be preserved.

Techniques and Strategy

Business strategy, which is based on strategic judgments about the company's future, is a declaration of what the business hopes to accomplish and how it intends to do it. The company may fulfill its purpose, goals, strategy, and plans by developing a thorough business strategy. The ultimate goal of risk management input into strategy is to guarantee that the strategy and strategic choices are effective and efficient and will provide the intended results [3].

Risk assessment is likely to be the key risk management input into corporate strategy. This is important for the development of strategy. It is important to examine the risks associated with both the current approach and any new ideas. If there are distinct strategic possibilities, then each of the workable options should be assessed for risk separately. Some businesses operate in a highly competitive industry that is going through considerable technical advancements. Under these conditions, the firm faces large risks, and crucial strategic choices must be made. These

choices are often influenced by technological advancements that pose problems for how the company provides consumer solutions. Technology shifts may need significant and risky investment decisions, and these choices determine the strategies that will be used. Due to unproven new technology or the existence of substitute technologies, investment choices may be speculative.

It is necessary to do a risk evaluation of the strategic choices, which should include a SWOT analysis and analyses of stakeholder expectations, current customer requirements, and employee skill sets. The corporation may have joint ventures, job outsourcing, subcontracting, or investments in new technology as strategic possibilities. The board will have the best knowledge possible to make sound strategic choices if risk assessments of strategic alternatives are thorough. Events and other situations that can make it more difficult to implement the plan successfully should be noted during the risk assessment. If any of these risks materialize, the business will then be able to determine which controls should be implemented to minimize the potential effect [4].

Strategic goals often have to do with the growth of a certain industry and the standing of the company within it. The growth of particular brands and reputation improvement so turn into opportunity hazards for the company the essential value of reputation and brand. The company will implement the business plan using tactics. To guarantee the efficacy and efficiency of operations, tactics must be properly chosen, put into place, and managed. They should also provide reliable financial reporting and conform to relevant laws and regulations. Core business operations that are effective, efficient, and compliant are the desired result.

Projects are responsible for bringing about changes to fundamental business procedures; this book's paper discusses the significance of risk management in projects. When starting a project, the organization must be worried about the risks that might prevent it from being completed on schedule, within budget, and according to specifications. The success of improvements to key processes that the project is intended to offer, however, is another factor to take into account when considering a project. If the necessary gain in core process effectiveness and/or efficiency is not realized, it is of little use to have a project completed on schedule, under budget, and in accordance with specifications. For instance, a successful project could install a new business software system, but if the new software system is insufficient or does not provide all of the extra advantages expected, the improvement in company core processes might not have been realized.

Risk assessment, risk response improvement, and the review and monitoring processes will be the major risk management inputs into strategies and initiatives. Finding the required controls is the goal of a risk assessment of a project. The efficacy and efficiency of the controls must be evaluated once they have been put in place. In general, the goal is to make sure that initiatives and techniques are productive and efficient in and of themselves. Effective strategies imply that the fundamental procedures are suitable for providing the desired results. Though totally efficient, established core processes may not always represent the best or most suitable options for the business to use. Change will be needed in the form of projects created to guarantee that the strategy is carried out in order to ensure that fundamental processes are completely functional. The firm will guarantee that it continues to satisfy consumers, investors, and other

stakeholders by creating more efficient core operations. The company strategy and business goals may need to alter in order to guarantee that efficient core processes are in place.

Operation that is Effective and Efficient

Operational efficiency that is safeguarded against unforeseen interruption is the overarching goal of risk management input into operations. A hazard risk materializing is likely to result in an interruption of activities. A significant competitive advantage or improved ability to offer value for money will be given to the business by the design of effective operational core processes that are free from disturbance. The way a company manages its risks may have a significant effect on how it conducts business. The continuation of continuous effective core business operations is crucial to every level of the risk management process. Critical inputs include risk identification and evaluation (risk assessment), responding to important risks, resource restrictions, response planning, reporting on risk, and review and monitoring. In conclusion, thorough risk management input is necessary for operations to be effective and unhindered. The delivery of effective operations depends in large part on internal audit. Internal auditors talk about the value that internal auditing operations contribute on a regular basis. This additional benefit pertains to the assessment of control efforts, particularly in light of operations. The controls that are in place must also be effective and efficient, in addition to the processes themselves [5].

Internal audit efforts are crucial to delivering the right level of risk assurance and, when necessary, confirming compliance. Effective and efficient operations are essential for all companies. It is crucial that current activities continue to be carried out as effectively as feasible under challenging financial and economic conditions. Whether the yearly budget, which contains the annual business goals, is achieved depends on how well operations are run. Increasing operational efficiency will help to ensure the organization's success. Development of activities to use fewer resources, which may include cost-cutting, may be done to provide more efficient operations.

If operations are built on the wrong fundamental activities or organizational processes, there is no value in their being efficient. For instance, it could be conceivable to plan a highly effective way to drive yourself to your destination, making the activity of driving as efficient as possible. However, it's possible that traveling by rail might make the trip more efficient. It is feasible to rent a cab and get to your location pretty effectively in the majority of crowded cities throughout the globe. Nevertheless, using the underground or metro system may be a more efficient option for travel since it will probably be faster and less expensive.

In Paper, the business model is covered in greater depth. It describes the customer offering that the company provides and is supported by the financial and reputational stability of the company (CORR). In Paper, the business model (represented by the abbreviation CORR) is discussed in further depth. The operational core processes and current (or past) activities of a company are therefore represented by the business model. By increasing the effectiveness and efficiency of operational core processes, strategy and tactics will be created to strengthen and improve the business model. It is crucial to remember that the business model depicts how an organization's operational core operations are currently functioning [6].

Ensuring Adherence

The justifications for engaging in risk management activities are categorized as required, assurance, decision-making, and core procedures that are effective and efficient. The STOC acronym stands for strategic, tactical, operational, and compliance procedures. The motivations for risk management and the efficacy and efficiency of key processes are inextricably linked. Organizations satisfy mandatory standards because stakeholders want them. Regulators, customers/clients, and financiers are stakeholders who have the authority to enforce conditions that must be met. Mandatory standards must be met, and the business will do this by making sure that it has effective and efficient core compliance procedures in place. For the majority of firms, failing to adhere to stakeholder standards may have serious consequences. In the worst case scenario, not adhering to a license's necessary conditions might lead to the regulator rescinding the license, endangering the organization's ability to continue operating. There will nearly always be a variety of approaches to satisfy the stakeholder-imposed required criteria. There will be hazards even if the basic compliance processes need to be effective and efficient, and risk management input will be crucial when building the compliance processes, protocols, and procedures. This is an illustration of how assistance from risk management professionals can help a business accomplish compliance in a manner that's not only efficient but also effective enough to provide it a competitive edge.

Many firms have a highly compliant culture and a strong willingness to uphold the legal requirements imposed upon them. This is a good quality that supports the organization's ethos, but if compliance is not attained effectively and efficiently, resources will be squandered and the company will suffer from a competitive disadvantage. The establishment of effective and efficient core compliance procedures that accomplish compliance in the most economical way is one of the responsibilities of risk management specialists. For instance, the majority of firms will be subject to mandated health and safety rules that are imposed by law and upheld by a regulator. If they think there will be no repercussions or that they can "get away with it," some organizations may object to the legal requirements put on them and try to evade compliance. A company with a more sophisticated approach to risk management, as demonstrated, will take the stance that complying with health and safety regulations will not only increase operational effectiveness, but a strong safety record may also be a factor in obtaining new contracts and clients [7], [8].

CONCLUSION

Operational reports show how well the plan is being carried out. Data must be continuously accessible so that management may react and alter the fundamental business procedures as needed. The information from operational reports may also be utilized to create reports on the organization's performance for stakeholders. However, the company must choose what information will be shared with stakeholders and how it will be presented. It is necessary to implement the proper control actions to guarantee correct reporting and disclosure. The Sarbanes- Oxley Act (SOX) in the United States lays forth obligations that are mainly concerned with the accuracy of financial disclosures to shareholders. The risk assessment of the reporting lines and the data-handling methods is the primary contribution of risk management to

performance reporting. The oversight of reporting processes has received more attention as a result of the SOX responsibilities. External auditors must certify the accuracy of financial reports and the financial reporting processes in accordance with Section of SOX. The company development model has elements that may be used to attain personal success and strategic goals. Numerous books have been written on the behaviors that guarantee career success and the character attributes of those who achieve great success. A quick checklist of procedures to guarantee professional advancement is provided in the box below. Furthermore, the paper emphasizes the importance of technology in supporting core business processes. It highlights the role of technology in automating processes, improving data management, and supporting decision-making.

Overall, the paper emphasizes the critical role of core business processes in the success of organizations. It highlights the importance of understanding and optimizing these processes to enhance efficiency and effectiveness, improve customer satisfaction, and support the achievement of organizational objectives.

REFERENCES:

[1] X. Liu, "The role of enterprise risk management in sustainable decision-making: A cross-cultural comparison," *Sustain.*, 2019, doi: 10.3390/su11102939.

[2] F. M. Trombeta, N. P. Ramos, and S. C. M. Bocchi, "Experience of nurse entrepreneurs in long term institutions for elderly people," *Rev. Bras. Enferm.*, 2020, doi: 10.1590/0034-7167-2019-0619.

[3] M. De Martino, "Value creation for sustainability in port: Perspectives of analysis and future research directions," *Sustain.*, 2021, doi: 10.3390/su132112268.

[4] S. Chalupa and M. Petricek, "The application of business process management in the hospitality industry: A case study," *IBIMA Bus. Rev.*, 2020, doi: 10.5171/2020.301930.

[5] M. Howard, P. Hopkinson, and J. Miemczyk, "The regenerative supply chain: a framework for developing circular economy indicators," *Int. J. Prod. Res.*, 2019, doi: 10.1080/00207543.2018.1524166.

[6] E. Demaj, X. Hysa, and A. Sadaj, "Digital Transformation in the Drugstore Industry: A Case Study," *Eur. J. Econ. Bus. Stud.*, 2020, doi: 10.26417/ejes.v6i1.p63-73.

[7] R. Harrison, A. Parker, G. Brosas, R. Chiong, and X. Tian, "The role of technology in the management and exploitation of internal business intelligence," *J. Syst. Inf. Technol.*, 2015, doi: 10.1108/JSIT-04-2015-0030.

[8] M. M. Lialestani, A. Khamseh, and R. Radfar, "Digital Transformation Model, Based on Grounded Theory," *J. Inf. Syst. Telecommun.*, 2021, doi: 10.52547/JIST.9.36.275.

CHAPTER 19

A BRIEF STUDY ON REPUTATION AND THE BUSINESS MODEL

Manjula Jain, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-jainmanjula776@gmail.com

ABSTRACT:

The success of a firm is significantly influenced by its reputation, which is a crucial asset. A firm may attract consumers, retain staff, and win the confidence of stakeholders with the support of a solid reputation. On the other side, a bad reputation may significantly affect a business's bottom line and its capacity to meet its goals. This paper offers an overview of the value of reputation and the business model and investigates how companies may successfully manage their reputation. The essential components of a company model and their connections to reputation. It emphasizes how crucial it is to comprehend consumer wants, provide value, cultivate close bonds with stakeholders, and preserve a favorable reputation in the marketplace.

KEYWORDS:

Business Model, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Every firm will have a business plan that outlines how it will provide its customers' offerings. Organizations that fall within the public sector, the third sector, or would otherwise classify as non-profits will still have a way to carry out their vision and/or mission statement. The organization's business model serves as the method of providing the well-defined customer offering. In conclusion, clients obtain the organization's product because it makes use of the resources at its disposal. The organization's adaptability and the plans in place to maintain the organization's sustainability serve as the foundation for the customer offering. Depicts the CORR (customer, offering, resources, and resilience) elements of the business model. These elements are each covered in further depth in and may be summed up as follows:

Consumer analysis covers consumer segmentation, hiring and keeping employees, and how goods or services will be supplied. Offering is used to describe the advantages that are provided to consumers in conjunction with their value proposition. Resources include partnerships, networks, and the organization's data, competencies, and assets. Reputational resilience of the company is based on ethos and culture, while financial resilience is based on expenses and income. The business model is significant because it illustrates how the fundamental operational and compliance procedures interact to provide the customer experience. Organizations must comprehend their business models in order to conduct a SWOT analysis a study of a business model's strengths, weaknesses, opportunities, and threats. The company will be able to examine the effectiveness of the current arrangements and identify risks by conducting a risk assessment of the current business model.

Items that make up the Business Concept

Events that can prevent the service from being delivered efficiently, as well as chances to boost compliance and operational effectiveness. It is crucial to remember that the business model describes operational and compliance operations and reflects the current methods for delivering the customer product. The firm will be able to find solutions for business model and/or customer offering enhancements by doing a risk assessment of the current business model. The organization's desired strategic position will be represented through the development of a revised business model. It will be necessary to develop tactics for putting that plan into action. Business models may be quite intricate and dependent on many other factors, such as suppliers and facilities that are outsourced. The current business model has to have its flaws and inefficiencies addressed, and analyzing the business model is one more technique to conduct a risk assessment. The next section discusses the value of resilience within the business model. Reputation and ethical trading are other aspects of the company strategy that are crucial. Within the supply chain, corporate social responsibility is a significant factor for many firms. An organization may evaluate its supply chain and find embedded risks, such as ethical hazards that might harm the company's image, by analyzing its business model [1].

Managing risks and the Business Model

A risk analysis may be performed on each part of the business model. The business model shows how the company achieves its goals and objectives as well as its vision and mission statement. Even though the product is at the core of the business model, determining which client group the offering will be directed at is often the first step. There are risks involved in locating, securing, and providing customer service and support to clients. The establishment of distribution paths and channels is crucial to the providing of the customer offering. The core of the company model and an essential component is the offering itself. It is crucial that the product makes use of the resources and competencies that are already at its disposal in order to provide the target customer with a value position and associated advantages. A variety of hazards are represented by the type, usage, and structure of the resources, and they should be assessed as part of the business model's risk assessment. The organization's tenacity and reputation are crucial components of the business strategy. There are many different business model alternatives, yet some do not sufficiently highlight the organization's reputation.

Later in this paper, we'll take into account the organization's reputation as well as its culture and ethics. A component of the industry in which a firm works is reputation. A company's reputation is often regarded as its most crucial component. An organization will want to maintain and/or improve its reputation, therefore reputation also has a sustainability component. All company models must be financially viable, which is often reflected by the financial viability of resources and the need to balance expenses and income sources. Environmental factors may be seen as part of sustainability, which often has a broader context. The risk assessment must take into account the organization's sustainability needs as well as its business strategy. Risks associated with compliance as well as hazards or operational risks will be the main topics of assessment of the business model. Operational risks must be reduced and compliance risks must be kept to a minimum in order to develop an effective and efficient company model [2], [3].

An organization must determine if the current business model is sustainable after identifying the model and doing a risk analysis. A new or modified business model will need to be found if it is thought that there is room for improvement. Realizing this improved business model becomes the organization's strategy. The organizational methods that are used to transform the business model in order to accomplish the strategy will be put into practice via projects and/or work programs that bring about the necessary adjustments. It will be necessary to manage the risks involved with applying methods as well as the strategic risks connected with changing the company model. This book uses the term "EM" to describe to the entire strategy of accepting strategic risks, managing tactical risks, mitigating operational risks, and reducing compliance risks. A good business model must be effective in acquiring new consumers and enticing them to engage in more meaningful interactions with the firm so that the connection can be maintained and strengthened. Therefore, improvements to the company model must not only attract new consumers but also help keep current ones while maintaining a high level of customer satisfaction.

DISCUSSION

Good Company Governance and Reputation

The criteria of an organization's overall corporate governance include corporate social responsibility (CSR). Good CSR practices may boost reputation and increase stakeholder value, and all kinds of firms should be aware of this. On the other hand, mishaps, occurrences, and losses related to lax social responsibility requirements may lead to negative publicity and reduce shareholder value. Having high standards for corporate social responsibility is important, and doing so may benefit the firm in the following ways:

1. Promoting and increasing trust, reputation, and brand.
2. Luring, inspiring, and keeping talent.
3. Controlling and reducing risk;
4. Enhancing operational and financial effectiveness;
5. Granting the company a permit to operate;
6. Creating fresh business prospects;
7. Improving the operational environment's security and prosperity.

There are many different ways to define corporate social responsibility. It is widely acknowledged that CSR is a broad agenda that includes businesses looking at ways to enhance their effect on local economies, society, and human rights as well as their social, environmental, and economic impacts. The CSR agenda also includes taking into account fair trade problems and fighting corruption. Several organizations used to refer to social, ethical, and environmental (SEE) issues before the phrase "corporate social responsibility" gained popularity. All of the topics that were previously on the SEE agenda are now on the CSR agenda. CSR is unquestionably a problem for huge global corporations, small, locally-based firms, and the public sector. In fact, it applies to all kinds of businesses, including charities. The following is the definition of corporate social responsibility provided by the European Commission: The idea of corporate social responsibility holds businesses accountable for their effects on all relevant

stakeholders. It is the ongoing commitment made by business to act ethically and responsibly, promote economic growth, and enhance the lives of the employees, their families, the local community, and society at large.

Risk management and CSR

The Table outlines the range of challenges that CSR addresses. The breadth of subjects includes anything from health and safety worries to more general issues about employees, clients, suppliers, the community, the environment, and the goods and services offered by the company. The risk management and CSR agendas overlap significantly and are both fairly wide.

The topics included in the, such as workplace health and safety and environmental impact, are often risk-based. However, managing these problems only as risks won't adequately advance the CSR goal. However, this is an excellent place to start. Corporate social responsibility as well as social, ethical, and environmental issues are often considered in risk assessment workshops. Risk managers should seize the chance to apply risk management methods and tools to a wider agenda while evaluating the CSR agenda. It is possible to apply the risk management strategy, which entails risk assessment, identification of control mechanisms, and auditing of compliance, to corporate social responsibility as well as the larger corporate governance agenda [4].

The majority of businesses see CSR as a danger to their image and its constituent elements as hazards. Such companies would believe that in order to meet these standards, they must modify their fundamental practices. This might be a good place to start for many organizations. However, what first seems to be a risk due to a danger might subsequently change to a risk due to a control and become an opportunity. Organizations should work to increase their degree of sophistication in respect to CSR, just as they do in other risk management areas. After completing the CSR requirements, firms should consider the options that are open to them. For instance, it is increasingly normal for supermarkets to sell items that were acquired via 'fair trade' methods in order to increase sales.

Concerning corporate social responsibility, it is probable that the public's viewpoint will prevail over that of many corporations. Therefore, CSR-related problems provide a fantastic chance for a firm to create corporate social responsibility strategies and initiatives that address public opinion. The business will benefit from its positive image if it approaches the CSR agenda as a dynamic, proactive collection of concerns. Stakeholders exist in many organizations that they may not necessarily desire. There is little doubt that this applies to a number of energy corporations. Environmental pressure organizations actively monitor the search for minerals, coal, and oil. Environmental pressure groups are legitimate participants in these organizations, even if they are "unwanted stakeholders," and they have a significant impact on their operations. Pressure organizations for the environment have demands that are squarely on the CSR agenda.

The major stakeholder groups in an organization's CSR agenda are its employees, clients, suppliers, and the general public. Everyone has a stake in how firms behave when their behaviors have an influence on the environment when it comes to CSR problems related to the environment. The report below, which was posted on the website of environmental advocacy organization Greenpeace, serves as an illustration of the influence that a pressure group may

have. This paper focuses on ethical trading and Shell's planned disposal of the Brent Spar oil storage facility in the middle of the supply chain. As a significant corporate risk, failure to guarantee adequate ethical behavior is becoming more widely acknowledged. Newspaper papers that detail bribery and other types of dishonesty may seriously harm a company's image and future earnings. Organizations may be investigated and exposed for unethical business and/or unfair treatment of suppliers as a consequence of easy access to information on the internet. If the unethical behavior turns into unlawful activities, the organization may be threatened. There might be substantial repercussions for engaging in illegal behavior and supporting acts that violate the organization's governance guidelines. Both immoral and unlawful, there is a perception that it is necessary to bribe authorities in certain areas. Unethical trade may have a negative impact on the organization's reputation, future profitability, and relationships with consumers and suppliers in a number of different ways [5], [6].

The procurement of goods made under socially undesirable labor conditions is another aspect of the supply chain that might give rise to claims of unethical business. Additionally, poor product quality and inability to provide value for money may harm a company's image and be linked to unethical business practices. Products that don't meet contemporary safety requirements might cause significant negative PR and reputational harm. A sports team should consider the restrictions that may be put in place on the importer to make sure that it only purchases goods from ethically produced sources when deciding that it wants all stuff sold to supporters to be ethically sourced. The importer's regular CSR report might be demanded by the club as a condition of the contract. The following details will be included in this report:

1. Specifics of the importer's policy about the suppliers' ethical behavior;
2. Verification of the manufacturing contract's terms and conditions;
3. A statement that manufacturers never subcontract work without permission;
4. Information on employee training, accident and absence rates, and compensation;
5. The findings of audits and actual inspections of industrial facilities.

The club may then urge other clubs in the league to follow suit by telling supporters that all products are produced ethically. As a result, the club will be promoted as having strong knowledge of corporate social responsibility. Positive coverage of CSR-related problems may be quite advantageous for a company. This will be particularly true if the group works in an area where people are wary of it. Because of how the public views the corporate world and/or the company, they may not be sympathetic to a cause. An ethical policy may be advantageous for a company that works in a field that is not generally well-liked by the public. If the company additionally conducts an ethics audit, the value of the ethics policy will be highlighted.

Gaming and gambling, for instance, do not enjoy complete popular acceptance. Therefore, businesses in this field should collaborate with rivals to develop social responsibility guidelines for problem gambling in order to improve the industry's image. The ability to show that a particular company goes above and above the basic requirements specified for the industry may therefore be used to its advantage. In addition to producing a separate CSR supplement, many firms increasingly incorporate commentary on corporate social responsibility in their annual reports and financial statements. The organization may benefit from the CSR agenda by

producing a report on its efforts in support of corporate social responsibility. A CSR agenda will have progressed from the necessity to reform to the point where the business can show that it does comply when an organization has a good narrative to share about CSR accomplishment. The firm must now show that following a CSR agenda allows it to operate better and more effectively meet stakeholder expectations as the next step in this evolving sophistication [7].

The value of reputation

Organizations place a lot of importance on reputation. In fact, it's sometimes argued that an organization's reputation is its most precious asset. Organizations should be mindful to grasp the foundation of their reputation since it is so crucial and can be lost so quickly. Although reputation is dependent on the size, character, and complexity of an organization, it is helpful to give reputation greater structure. The components of reputation have been extensively studied. The components of reputation are also represented as a spidergram along with these. The following is a list of the four major elements of reputation (CASE):

1. Capabilities, comprising resources and a goal.
2. Operations, including accounting procedures.
3. Standards for services, goods, and assistance.
4. Ethics, which includes principles and morality.
5. Identifying the elements of reputation

Reputation is a factor on the FIRM risk scorecard and is often seen as a result of other things that happen. The benefit of having a good reputation is that consumers or clients will want to do business with that company. Organizations should thus carefully consider both their own reputation within the sector in which they operate and the reputation of the industry as a whole. Many businesses consciously plan steps that will improve their reputation and help them succeed more.

An organization should possess the skills required to develop a strategy, put it into action, maintain operations, and guarantee compliance. An explicit declaration of goal, aim, or commitment should represent the capabilities. An organization's operations are influenced by the industry in which it competes. Additionally, the organization will need to have the resources and stability in its finances to fund its operations. From an internal standpoint, an organization is defined by its skills and activities taken together. The firm will provide a variety of services and goods, and service delivery standards will play a crucial role in the organization's reputation. The company will also have corporate principles that show its honesty. Monitoring performance in order to learn and achieve ongoing performance improvement will, in some ways, display integrity. The company will be able to map its entire reputation within the context of the industry it works in by using a chart like the one presented. An organization should be able to map its current condition for each of the four segments, or eight qualities, in a rating of to, denoting bad, sufficient, outstanding, and exceptional. The firm will then have the ability to pinpoint the industries that pose the most risks to its image.

Lack of sufficient internal resources to guarantee good governance and/or provide high-quality services and goods. Negative publicity affects the business sector in which the firm works.

Customers have less inclination to do business with the company because of the organization's weakening finances. Lack of innovation in services and goods causes people to shop elsewhere. Loss of customer support or a decline in the quality of goods and/or services. Failure to respond to client concerns in a fair and honest manner. In this paper, the significance of reputation has generally been discussed, with corporate social responsibility serving as an illustration of one of its primary pillars. But reputation is more complicated than merely a matter of commercial ethics. Customers often do business with a company even when they don't think its business strategy is especially ethical. Although reputation has only received a brief analysis and discussion in this work, its fundamental significance is widely recognized, particularly in regard to risk management.

All companies understand the value of a strong brand and reputation. Many businesses that interact directly with customers have worked to establish a reputation for reliability and moral conduct. This is not a new invention for many firms; rather, it forms the foundation of their consumer offerings. The excerpt from Unilever PLC's Annual Report and Accounts in the text box below highlights the value of reputation [8].

Structure, Tactics, and Procedures

The risk architecture, strategy, and protocols (RASP) for an organization are covered in this section. The RASP gives information on the organization's risk management framework, which helps in defining the risk management context. We go into further depth about the major components of the risk architecture, strategy, and procedures. The risk management policy statement is the most significant part of the RASP. The organization's overall risk management approach will be outlined in the RM policy. Other parts of the overall risk management handbook include the roles and duties of risk managers as well as the procedures that must be followed.

The risk framework that underpins the risk management process is created by the risk architecture, strategy, and procedures. The risk management framework should include goals, a mandate to manage risks, and a commitment to doing so, according to British Standard BS. It should also include organizational arrangements, such as plans, relationships, accountabilities, resources, processes, and activities (architecture), and it should be integrated into the organization's overall strategic and operational policies and procedures (protocols). The risk framework as outlined in ISO is equal to the risk architecture, strategy, and procedures. The risk architecture, strategy, and procedures effectively serve as the organization's context for risk management. The risk strategy component will often be presented as a one-page description of the objectives the business has for risk management. This one-page declaration is referred to as the risk management policy by ISO. In many firms, the risk management policy will be included in a wider risk management document. A set of risk management guidelines will often be used to record the risk processes used by major enterprises. Depending on the organization's size, nature, and complexity, several sets of rules may be necessary. The following sorts of documentation will need to be maintained:

1. Records of risk management administration.

2. Plans for risk mitigation and enhancement.
3. Recommendations and event reports.
4. Reports on risk performance and supervision.

The risk register is one of the common papers created by corporations as part of their risk management programs. There are several operational, project, and strategic uses for risk registers. The paper discusses the fundamental format of the risk register as well as its anticipated structure. It is very vital for risk management and internal audit to operate together. Assessment of risk and identification of current and new controls are the foundations of risk management knowledge. The examination of controls and the testing of their efficacy and efficiency fall within the purview of internal audit. Risk management and internal audit must work closely together for a risk management effort to be implemented successfully. The specifics of how this close cooperation would be accomplished in reality should be included in the RASP [9].

CONCLUSION

The risk architecture outlines the organization-wide dissemination of risk-related information. The general goals that the company is attempting to accomplish in relation to risk management are specified in the risk strategy. The systems, norms, and practices known as risk protocols are implemented in order to carry out the specified risk strategy. The risk management framework includes the risk architecture. The organization's entire risk governance mechanisms include the risk management framework. Furthermore, the paper discusses the importance of transparency and communication in reputation management. It highlights the need for businesses to be open and honest with stakeholders, communicate regularly, and respond quickly and effectively to any issues or concerns. Overall, the paper emphasizes the critical role of reputation in the business model and the need for businesses to manage it effectively. It highlights the importance of understanding the key elements of the business model and how they are linked to reputation, establishing a reputation management framework, and promoting transparency and communication to build and maintain a positive reputation in the market.

REFERENCES:

[1] L. W. W. Mihardjo, Sasmoko, F. Alamsjah, and Elidjen, “Mediating role of co-creation strategy on the relationship between business model innovation and corporate reputation: A case study on Indonesian telecommunication firms,” *J. Tech. Educ. Train.*, 2019, doi: 10.30880/jtet.2019.11.04.008.

[2] Q. A. Ma and O. Osiyevskyy, “Maximizing the strategic value of corporate reputation: a business model perspective,” *Strateg. Leadersh.*, 2017, doi: 10.1108/SL-05-2017-0043.

[3] L. W. W. Mihardjo, Elidjen, F. Alamsjah, and Sasmoko, “The role of corporate reputation & distinctive organization capability in developing business model innovation: Case study of indonesian ict firms in facing industry resolution 4.0,” *Opcion*, 2018.

[4] T. T. Van Nguyen and T. D. Nguyen, “The Relationship between Green Marketing Strategy , Corporate Reputation and Business Performance : An Empirical Investigation in Tourist Companies in Vietnam,” *Int. Res. J. Adv. Eng. Sci.*, 2020.

[5] K. Singh and M. Misra, "Linking Corporate Social Responsibility (CSR) and Organizational Performance: the moderating effect of corporate reputation," *Eur. Res. Manag. Bus. Econ.*, 2021, doi: 10.1016/j.iedeen.2020.100139.

[6] D. Vidaver-Cohen, "Reputation Beyond the Rankings: A Conceptual Framework for Business School Research," *Corp. Reput. Rev.*, 2007, doi: 10.1057/palgrave.crr.1550055.

[7] A. MOTOC, "Family Business Image and Reputation. A Model of the Influencing Factors, Actions, and Effects," *Manag. Dyn. Knowl. Econ.*, 2013, doi: 10.25019/mdke/7.4.04.

[8] M. Sageder, C. Mitter, and B. Feldbauer-Durstmüller, "Image and reputation of family firms: a systematic literature review of the state of research," *Review of Managerial Science*. 2018. doi: 10.1007/s11846-016-0216-x.

[9] J. Lv, Z. Wang, Y. Huang, T. Wang, and Y. Wang, "How can E-commerce businesses implement discount strategies through social media?," *Sustain.*, 2020, doi: 10.3390/SU12187459.

CHAPTER 19

Risk Management Policy for a Council

Satyendra Arya, Associate Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-satyendra_arya17@rediffmail.com

ABSTRACT:

Any business, including local councils, must identify, evaluate, and manage any risks that might have an influence on their goals. A risk management strategy offers a framework for managing risks by outlining who is responsible for what and how risks should be identified, evaluated, and controlled. An outline of the key components of a council's risk management policy is given in this paper. The significance of having a risk management policy in place is examined, along with the necessity to comply with legal obligations and safeguard the organization's image. The defines the essential components of a risk management policy, including the framework for risk management, the roles and duties of those participating in risk management, and the procedures for finding, evaluating, and managing risks.

KEYWORDS:

Business, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Good management practices and corporate governance both depend on effective risk management. This strategy statement highlights the measures taken to guarantee that the council recognizes and addresses the major risks it confronts. In order to allow decisions to be based on thorough risk assessments and ensure that the appropriate measures are taken at the appropriate time, the council has introduced proactive risk management systems. The council's ability to successfully manage its risks may have a significant influence on the accomplishment of its primary initiatives, priorities, and service delivery to the community. The risk management plan supports the council's goal of being a top-tier organization.

The goals of this tactic are to:

The council should fully include risk management into both its strategic and service planning procedures. Ensure that personnel who have operational responsibility for risk comprehend and use the risk management framework. Share the council's risk management strategy with relevant parties. By making the most of opportunities and reducing dangers, make sure the advantages of risk management are achieved. Make sure risk management is uniform across the council.

Management of Risk

The identification and treatment of hazards are the main goals of effective risk management. It lessens the chance of failure, raises the chances of success, and decreases ambiguity in reaching goals. Risk management need to be an ongoing, dynamic activity that permeates the council's policies and service delivery. By minimizing hazards and maximizing the use of opportunities, learning from previous actions informs choices that will be made in the present and the future. A more bold but measured approach is then encouraged by celebrating and reporting effective risk management [1].

Risk Management

The term "risk architecture" refers to an organization's structures and procedures for managing risk. Lines of communication for reporting on risk management concerns and incidents are established by the risk architecture. It is crucial that the risk architecture emphasizes that the risk's owner is still responsible for risk management. A precise definition of risk management duties is necessary so that risk management may be effectively integrated into an organization's fundamental procedures and daily activities. Additionally, as part of the analysis of any important risk, responsibility for managing that risk must be explicitly assigned to the following areas:

1. The creation of risk criteria and a plan;
2. Adoption of the established guidelines and practices;
3. Checking for adherence to the established requirements.

The committees responsible for risk management and the connections between those committees may be identified using a diagrammatic representation of the risk architecture. The paper discusses the significance of an organization's risk architecture and offers illustrations of common risk architectures. Details of the different committees' terms of reference will be included in the risk architecture. This will provide information on the composition and duties of the different committees. The risk architecture should detail how information about risks is shared across the relevant committees. The interaction between the numerous committees that have been created inside the company is shown by the risk architecture. The committee's composition and duties will need to be defined in appropriate terms of reference. The risk architecture will also specify the reports that each committee receives and the reports that those committees are obligated to provide. Making ensuring risk escalation processes, including suitable whistleblowing options, are ingrained inside the business is a key component of the risk architecture.

Organizations should make a distinction between the risk procedures that are included in the risk management handbook and those papers or reports that are meant to track and monitor changes and improvements when evaluating the range of documentation that needs to be created. While other paperwork, like the risk register, should be a dynamic record of activities that are planned or already in progress, the risk management handbook may be thought of as a static record of processes and procedures. The risk register should be regarded as the action plan for risk management.

Risk-Management Approach

In terms of risk management, it's critical for a business to have a well-defined strategy. The risk management policy statement will outline the organization's risk management approach. The plan must be founded on the organization's entire approach to risk and risk management. The need that risk management input be included in strategy, tactics, operations, and compliance (STOC) will be a crucial part of that risk plan. Important choices on the organization's risk appetite will need to be taken in order to build the risk management plan. More information on risk appetite is provided in Paper. The organization's potential investment, acceptance of controls, and risk tolerance will all be factors in determining the risk appetite[2].

It is crucial that the risk appetite stays within the organization's overall risk capacity. The method for calculating the risk capacity will need to be decided. Additionally, consideration must be given to how the organization's overall risk exposure will be tracked and incorporated into decision-making procedures. Operational risk management includes the measurement of an organization's overall risk exposure. Important decisions must be made regarding the risk management initiatives that will be planned and implemented to meet the needs of the risk strategy, as well as decisions regarding the design and implementation of the risk processes that the organization will adopt. The organization's goals for risk management will be described in depth in the risk management plan. The plan could include the specifics of the targeted degree of risk maturity as well as the information on the amount of contribution anticipated from risk management. The organization's overall operations and the anticipated contribution from risk management activities will be established by the risk management strategy, which also determines how risk management activities are matched with one another.

Protocols for Risk Management

The mechanisms for executing the policy as well as risk management duties will be included in the handbook. In a series of risk procedures and recommendations, which are discussed later in this paper, risk management protocols will be laid out. It will be necessary to create written procedures and processes for assessing the risks to strategy, projects, and operations. The company will also need to create guidelines about the frequency, type, and accountability of risk reporting. The risk management procedures often need to be reviewed annually to ensure they are maintained current. The level of record keeping necessary should also be included in the risk guidelines. The vast variety of risk management paperwork that may be required gives a general overview of the many kinds of papers that could be suitable. The variety of actions conducted under the guise of risk management are described in risk management protocols. The protocols outline the tasks that must be completed as well as how they will be carried out. Guidelines for risk management often specify the requirements that should be met. They sometimes provide information about the restrictions that are in place. This will be particularly accurate for recommendations that identify handbook for risk management [3].

DISCUSSION

The amount of risk management paperwork that each firm produces will vary greatly. According to the risk management principles, the documentation created should be in proportion to the

amount of risk experienced by the firm. Whatever is created must be organized in a manner that fits the organization and is consistent with the other activities that happen there. The risk management policy is included in the manual's first section. The box on page provides an example of a risk management policy statement for a council. The policy outlines the organization's risk management plan. It sets the organization's risk management context and serves as a statement of purpose. The organization's risk management process should be successfully implemented thanks to the risk management policy [4].

The organization's risk management process and structure are fully described in the risk management handbook, together with all roles, duties, protocols, and rules related to them. An example of appropriate manual information for risk management. The handbook should attest to the methods for carrying out the tasks as outlined in the organization's risk standards. To make updating them easier, the risk guidelines could be created as a distinct group of papers. The organization's risk management strategy, also known as the risk management policy, will be included in the risk management handbook. Additionally, the risk management handbook will outline the methods and practices that will be implemented to track performance as well as the channels for reporting and disseminating risk management-related information. In essence, it will outline the environment in which risk management actions are conducted. It will be necessary to create a variety of risk management protocols or recommendations.

The risk protocols provide greater details about how the risk protocols need to be used and understood. The risk management procedures may be thought of as the guidelines for managing risks. They will often demand that records be kept, such the risk register. The comprehensive risk management protocols or guidelines will include the following: Even if the overall risk management approach doesn't change, many firms discover that it's still important to update the risk management handbook every year. This is done for a variety of reasons, including the need to make sure that risk management processes and strategies are up to date with industry best practices. The business has the chance to choose the risk priorities for the next year and make sure that the important risks are given the right amount of attention by updating the risk management handbook, including the risk management policy, every year. By releasing an updated risk management policy each year, the company may guarantee that the board is paying attention to risk management and that it is recognized as a dynamic activity that needs ongoing monitoring.

Documents for Risk Management

The breadth of policies or procedures that a company may need to develop for risk management. This list is not intended to be comprehensive; other protocols, rules, or processes may be required depending on the precise nature of the company and the risk management plan it is using. An organization may define specific processes on a variety of risk management subjects and lay out the risk management priorities for the next year by creating a risk management handbook, which includes the policy statement. The risk management paperwork should include, for instance, the yearly health, safety, and/or environmental policies and procedures that many firms generate. Significant hazards that demand frequent or even ongoing management attention are faced by several enterprises. This is especially true when it comes to hazard concerns, where

it's important to regularly update things like business continuity plans, disaster recovery plans, and health and safety policies and procedures [5].

The risk guidelines will often be placed in writing for many firms. Other businesses will use a looser approach to include risk management into managerial tasks. Details of the organization's risk management structure will often be included in the risk guidelines. Additionally, the risk guidelines must provide specifics about the risk strategy and risk practices. Details of the managers' (internal) control obligations should also be included. The value of the steps taken throughout the risk management process. Each of these actions generates a variety of outputs; the necessary outputs are included in the risk recommendations. The policies should outline how risk control decisions will be made, carried out, and audited, but they need not contain a list of risk control or loss control standards. In actuality, physical control standards and needs cannot be included in risk recommendations for a broad collection of businesses. Each unit, division, or department should establish its own guidelines for risk management, including those related to environmental protection, physical security, information security, health and safety, and fire safety. Due of the diversity of the many organizational units, this may be suitable.

The methods for achieving embedded risk management in the company should be specified in the risk guidelines. Within the constraints of the risk guidelines, strategy, standards, and processes need to be established. The company and the kind of risks it encounters will determine the framework for the risk guidelines. The variety of risk management records that a business may be required to keep. A variety of risk management records must be kept in order to properly incorporate risk management. These documents will describe specific risk management actions, such as:

1. Administration of risk management.
2. Plans for risk mitigation and improvement.
3. Reports on the event and suggestions.
4. Reports on risk performance and certification.

When the organization's planning cycle and the cycle of risk management activities are perfectly matched, embedded risk management will be realized. Risk guidelines are primarily intended to assist managers in comprehending the organization's risk management framework. This knowledge will guarantee that managers give risk implications the attention they need while making choices. The risk guidelines for the company provide managers useful advice on how to carry out their risk management duties. The company will be able to prove that the risk recommendations have been successfully implemented by keeping the relevant documents. The paperwork for risk management administration should include (at the very least) the components. The maintaining of risk management records is not intended to become unduly bureaucratic or onerous.

However, sufficient records must be preserved to ensure that information is available for decision-making, that managers can get the appropriate guidance, and that auditors can receive proof that relevant controls have been successfully applied. The significance of maintaining records is shown here. The main justification for doing a risk assessment is to check existing

controls and determine whether further steps are required to enhance risk management. Information on existing controls and specifics of planned new controls are kept on file in the risk register. It's crucial that the risk register not turn into a stagnant record. It need to be seen as a dynamic component and as the organization's overall or a unit's risk action strategy [6].

Information on the accountability for certain controls will also need to be kept on file, in addition to risk response strategies. If further controls are needed, it is important to note the timeframe and who will be responsible for putting those new, better controls in place. The possibilities for risk response are more thoroughly discussed in Part Four of this book. The risk register is the place to record specifics of the major threats for hazard risks and control risks. Plans for risk improvement will need to be thoroughly analyzed. Risk improvement strategies often call for capital expenditures, which may need to be authorized via the organization's spending authorization processes. The creation of risk registers for projects, particularly those in software and construction, has become routine procedure. Construction and software project risks may lead to a great deal of uncertainty, and these risks are often control risks. Once again, a dynamic record of the steps done to reduce the uncertainty should be kept, and new steps should be planned.

The fact that risk registers are only completed once or twice a year and provide a static view of the organization's hazards is a typical criticism of them. Risk management must be an active process that produces results that have an influence on the business in order to be efficient and contribute significantly. If this is to take place, the danger register must develop into a record that motivates modifications and advancements. It could be preferable to refer to the risk register as the organization's "risk management action plan."

Reports on occurrences, analysis of those events, and suggestions all have to do with keeping track of the specifics of those events and controlling their effects. This kind of risk management paperwork includes information on incident investigations, performance analyses of company processes, and suggestions for risk reduction. Recommendations for risk improvement target substantial control flaws and seek to reduce the possibility of more material or significant failures. The practice of recording occurrences is crucial, particularly when it comes to danger hazards. Additionally, it will be crucially critical to document and analyze occurrences that occur throughout a project. The risk of danger and control is particularly relevant to event reports. Annual risk performance evaluations will also result in reports that need in-depth study. An essential function of internal audit is the evaluation of risk performance [7].

A well-established subfield of risk management is clinical risk management. It's critical to retain accurate records in order to prove that the proper risk mitigation measures have been taken and to document any clinical errors. An overview of the significance of record keeping in relation to clinical risk management is given in the box below. Preliminary reports of operations' outcomes are taken into account and analysed in risk performance and certification reports, along with more official declarations and certified reports to stakeholders. In certain instances, the company may pursue certification of its operational outcomes as a formal attestation of operational success. In terms of financial reporting, the Sarbanes-Oxley Act mandates this method. Most

often, a third party, such as an external auditor, will do this attestation. A review of the success of the control measures might likewise be the subject of such an attestation [8], [9].

CONCLUSION

Information on risk performance will be of interest to management. This will be crucial when the company is exposed to a variety of hazards that together put the overall risk exposure very near to the organization's tolerance and/or capacity for risk. For instance, a company could have set aside money in its budget for a certain amount of loss in respect to hazard risks. If this budget proves difficult, diligent loss monitoring will be necessary to make sure that the exposure to the particular kind of hazard risk is not exceeded. The company will need to closely manage hazard losses since the hazard tolerance may be restricted. For instance, a transportation business must keep track of the frequency of vehicle breakdowns and the number of accidents involving motor vehicles. Furthermore, the paper discusses the need for regular review and continuous improvement of the risk management policy. It highlights the importance of incorporating feedback from stakeholders, monitoring the effectiveness of risk management activities, and updating the policy to reflect changes in the organization's objectives or external environment. Overall, the paper emphasizes the critical role of a risk management policy in ensuring that the council effectively manages risks and achieves its objectives. It highlights the need for a comprehensive risk management framework, clear roles and responsibilities, effective communication, and regular review to ensure the ongoing effectiveness of the policy.

REFERENCES:

[1] P. J. Schweizer, “Systemic risks–concepts and challenges for risk governance,” *J. Risk Res.*, 2021, doi: 10.1080/13669877.2019.1687574.

[2] A. Dedekorkut-Howes, E. Torabi, and M. Howes, “Planning for a different kind of sea change: lessons from Australia for sea level rise and coastal flooding,” *Clim. Policy*, 2021, doi: 10.1080/14693062.2020.1819766.

[3] K. Yeung, “Recommendation of the Council on Artificial Intelligence (OECD),” *Int. Leg. Mater.*, 2020, doi: 10.1017/ilm.2020.5.

[4] J. K. Kalonda, H. Pupkewitz, and K. Govender, “Factors Affecting Municipal Service Delivery A Case Study of Katima Mulilo Town Council, Namibia,” *African J. Public Aff.*, 2021.

[5] M. Al-mueed *et al.*, “Potential of community volunteers in flood early warning dissemination: A case study of Bangladesh,” *Int. J. Environ. Res. Public Health*, 2021, doi: 10.3390/ijerph182413010.

[6] R. Mouchantaf, D. Auth, Y. Moride, J. Raine, S. Y. Han, and M. Y. Smith, “Risk Management for the 21st Century: Current Status and Future Needs,” *Drug Saf.*, 2021, doi: 10.1007/s40264-020-01033-z.

[7] IRGC, “An introduction to the IRGC risk governance framework,” *Int. Risk Gov. Counc.*, 2005.

[8] M. Woods, "A contingency theory perspective on the risk management control system within Birmingham City Council," *Manag. Account. Res.*, 2009, doi: 10.1016/j.mar.2008.10.003.

[9] M. Al-Saidi and S. Saliba, "Water, energy and food supply security in the Gulf Cooperation Council (GCC) countries-A risk perspective," *Water (Switzerland)*. 2019. doi: 10.3390/w11030455.

CHAPTER 20

DISCUSSION ON RISK MANAGEMENT RESPONSIBILITIES

Vipin Jain, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-vipin555@rediffmail.com

ABSTRACT:

Risk management is a critical process that involves identifying, assessing, and managing potential risks that an organization may face in pursuit of its objectives. It is essential to have a clear understanding of risk management responsibilities to ensure that risks are effectively managed and that the organization achieves its goals. This paper provides an overview of the risk management responsibilities of individuals and organizations. It explores the importance of assigning clear roles and responsibilities in the risk management process to ensure that risks are identified and managed effectively. The identifies the key risk management responsibilities of individuals and organizations, such as identifying potential risks, assessing their likelihood and impact, developing risk mitigation strategies, and monitoring and reviewing risk management activities.

KEYWORDS:

Business, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

Everyone who works for a company, including contractors and suppliers, must be made aware of their roles in risk management. Many professionals in major businesses who are knowledgeable about risk have a considerable impact to make on the effective management of the most important hazards. Regrettably, opinions on risk management and other matters that are significant to the firm are not always shared. It is crucial to take responsibility for core procedures, major dependencies, and hazards because doing so allows the risk management and audit committees (see Part Eight) to keep an eye on performance. Although the audit committee will only keep an eye on the most serious risks, this ownership is crucial for all risks. Any ambiguity about roles and the hierarchy of reporting must be removed[1], [2]. The following elements of the management of each priority substantial risk should have unambiguous declarations of responsibilities:

1. Establishing necessary risk thresholds.
2. Putting in place risk guidelines.
3. Keeping track of risk performance.

The roles of risk owners, process owners, internal audit, risk management functions, employees, contractors, and outsourced operations, as well as all others, will be clearly defined and

understood with the help of a specific list of responsibilities. Another crucial factor to take into account is how duties are distributed across committees as part of the risk architecture. The terms of reference for any committee will typically include the membership, duties, and reporting structure. The risk registry should provide information on who owns each important priority risk. It is crucial that local ownership of substantial risks does not diminish as a result of the work of the risk manager, risk management committee, audit committee, internal auditors, and others. Managers must see the ownership of risks as a component of managing key business processes and activities rather than as a distinct concern that falls within the purview of internal audit and/or specialised professional risk management practitioners. The division of duties among the board and executive, who make up senior management, is the subject of this item. The distribution of tasks to department heads or middle management is the subject of this item. The delegation of staff members' roles in risk management is the subject of this item. Together, these three levels of management serve as the first line of defense in ensuring that risk management and internal control are given the proper amount of attention.

The obligations of the organization's risk management. The duties of specialized risk management roles, such as business continuity or health and safety, are outlined in item. These tasks may be seen as the second line of defense in attaining effective risk management and internal control since they provide specialized assistance to management. The duties of the internal audit manager are outlined in item of. The third line of defense in establishing acceptable standards of risk management and internal control may be called internal audit operations. Externally, insurance brokers, insurance providers, accounting firms, and external auditors may all help their clients' enterprises manage risk more effectively. Collaboration amongst risk management experts is crucial. However, it is also crucial that the advantages of risk management be integrated into the organization's fundamental procedures.

Set goals for the location's risk management performance; consider employee reports on risk management issues; monitor the execution of suggestions for risk reduction; and identify and report altered conditions or hazards. Understanding, accepting, and implementing RM procedures. Reporting ineffective, unneeded, or impractical controls. Reporting loss occurrences and near-miss situations. Work together with management to investigate incidents and make sure that contractors and guests adhere to protocol. The risk manager's primary duties in terms of risk management are to create and maintain the risk management policy and to promote a culture of risk awareness throughout the company. Organize the risk management efforts by creating internal risk policies and frameworks. Gather information on risks and provide reports for the board. Main RM obligations for specialized risk management functions [3].

Help the business create specialized risk policies and create specialized contingency and recovery strategies. Keep abreast of new advances in your field of expertise. Assist with investigations into accidents and near-misses. Write thorough reports on your field's dangers. Internal audit managers' primary roles in risk management are to: Create a risk-based internal audit program; Inspect the organization's risk management procedures; and Provide assurance. Report on the efficacy and efficiency of internal controls. Support and assist in developing the risk management procedures. It is important to make sure that risk management is given enough

attention. The person who promotes risk management awareness at the board and gives risk management reports to the board is often a board member. Risk architecture, strategy, and protocols (RASP) are often the responsibility of the risk manager, who typically reports to that board member. Assigning the role of "risk owner" is one of the most crucial tasks. A risk owner is a "person with authority and accountability to decide whether to treat, or not to treat, a risk," according to the ISO Guide. According to the handbook, whomever is responsible for a goal is also responsible for the risks related to that aim and for putting controls in place to manage those risks.

Management's Statutory Obligations

In many nations, there has been a growing tendency toward guaranteeing more clarity with respect to the duties of corporate directors. In most nations, the common law has evolved over many years to include the basic responsibilities of directors. The duties of directors are significant in terms of risk management, and effective risk management will help directors successfully carry out their duties. In order to succeed as an organization and exercise appropriate care, competence, and effort, risk management is very crucial. Organizational directors must have a solid grasp of risk management in order to fulfill their statutory and other obligations. Board members are typically either executive or non-executive directors of the company. The non-executive directors make up a "board of governors" and meet separately as a "executive committee" in certain organizations, such as charities and the majority of governmental agencies. Executive directors often work for the company full-time and are assigned a particular area of responsibility. Non-executive directors are crucial to the organization's risk management process. However, this position will often be limited to compliance, assurance, and auditing tasks. Since executive directors are in a better position to comprehend and manage the risks that the organization faces, it may not be appropriate for non-executive directors to get involved in the management of the specific risks. This is because doing so would conflict with their non-executive audit responsibilities. An illustration of the function and requirements of non-executive directors may be seen in the box below. Non-executive directors generally shouldn't become engaged in the organization's day-to-day management. They often play a supporting role in the development of strategy and performance monitoring. Executive directors are in charge of carrying out the plan.

The Risk Manager's Function

Table outlines the usual historical responsibilities of the insurance risk manager. .With board approval, the risk manager has historically evaluated the organization's entire risk policies and processes. These past duties have included making decisions on insurance risk management problems and providing statistical analyses of insurance losses. The risk manager for insurance must assess how risk management is doing right now and consider the health of the insurance industry. The quantity of insurance that major businesses acquire has changed as a result of rising insurance premiums and a more sophisticated approach to risk finance. There have often been fewer insurance purchases, which has resulted in lower premium spending and a smaller budget for the department of insurance risk management.

DISCUSSION

The risk manager does not have a single designated reporting role inside a company. Currently, risk managers might report to the secretary of the firm, the director of finance, or human resources. The risk manager sometimes reports to the company treasurer and, in rare occasions, the CEO. Most big firms still need a facilitator and coordinator for risk management. As a result, the business will be able to use risk management tools and strategies to address a larger variety of problems. In the past, risks have been separated into pure (insurable) and speculative (non-insurable) risks. These distinctions between different risk kinds are arbitrary from the standpoint of corporate performance. The corporate learning that must occur so that the company can comprehend the advantages of risk management should be the responsibility of the risk manager. The risk manager will be in charge of creating the strategy, methods, and procedures by which the organization's needed risk management results are attained as the person with responsibility for the risk architecture, strategy, and protocols (RASP).

In the past, it's likely that the insurance risk manager was not engaged in the strategic planning and growth of the company. A risk manager should become more involved in project management, strategy development, and execution as a result of the expanded role that is now expected of them. The position of the risk manager inside the firm will be very difficult for someone who has a wide variety of duties. It will be a position that gives the risk manager the opportunity to comprehend and participate at a deeper level than most other positions or functions. Perhaps the term "risk manager" has too many associations with the past to be utilized to describe what is presently necessary. Finding a new name and redefinition of risk management's function are both necessary. The growing significance of organizational resilience may provide a chance for the risk manager to become the "risk and resilience manager" and take on a much larger responsibility that is intended to be more in line with the performance of the business [4].

The advantages of combining the management of credit, market, and operational risks have been recognized by several companies in the financial and energy industries. In the financial industry, risk management and insurance purchases have always been handled separately. This reality is reflected in the evolution of the chief risk officer (CRO) position, which reports directly to the CEO. It is doubtful that the majority of firms will need to employ someone with the seniority of a CRO given that one of the fundamental tenets of risk management is that the response to risk should be appropriate to the amount of risk posed by the company. However, companies should consider the right scope of duties and degree of seniority for the risk manager while examining their risk architecture. Although the term "chief risk officer" has not yet been widely accepted, it is spreading across the energy and financial industries. An outline of the chief risk officer's evolving function is given in the box below. The impact that a CRO may make to a company will be significant if it is deemed appropriate for one to be hired.

Actual Risk Architecture

The Sarbanes-Oxley Act's standards for the risk architecture of a typical major business organization. The organization's risk management guide should outline this risk architecture. A

calendar of risk management activities or the risk management handbook should include the terms of reference for the different committees as well as a timetable of the activities. This program of events ought to complement the organization's other business initiatives.

Risk management plans for Major Corporations

The audit committee need to be represented in the risk architecture for a large business with non-executive directors. In order for the business to implement its risk management plan, the audit committee's and the head of internal audit's roles are crucial. There will also be an obligation to guarantee that all information released by the corporation is correct for companies subject to the Sarbanes-Oxley Act's standards. This need led to the creation of a disclosures committee in many large companies. The disclosures committee's job is to verify the accuracy and reliability of the information that the organization discloses. The Sarbanes-Oxley Act mandates that financial data be scrutinized more closely. An organization's risk architecture outlines the hierarchy of committees and tasks linked to risk management and internal control. in the arrangement seen in. The corporate risk management committee's attention is given to operational risk management procedures [5], [6].

Divisional management should be given responsibility for risk management for operations at the unit or divisional level. Divisional management is in charge of organizing the identification of important risks at the divisional level, creating the division's risk register, and making sure that the proper controls are found and put in place. The corporate risk management committee should provide advice to the divisional management. The global risk management committee should be obliged to receive reports from any divisional committees in order to build the corporate or group overview of risk management priorities. A public-sector or nonprofit organization will have a somewhat different risk architecture. Describes a charity's typical risk architecture. The governance and risk committee is the primary target of these risk management initiatives. Information flow and risk management operations under control. That risk governance is a considerably more high-profile concern for charities than in many other businesses is evident. According to studies, governance concerns are the main thing on charity trustees' minds. This suggests that many charity trustees prioritize governance above fund raising for the organizations they support. This may be an instance when worries about risk management go out of hand to the point that they change the character of the company.

Risk management reporting lines may be developed in a variety of ways. The organization's complexity and risk tolerance should be reflected in the reporting structure. The risk committee is probably a direct subcommittee of the board for high-risk businesses, notably those in the banking industry. In these circumstances, it is expected that the group finance director would serve as head of the risk committee, and other senior board members will also serve on it. Generally speaking, the risk management committee ought to be an executive committee that is made up only of executive directors and excludes any non-executive directors. This is because non-executive directors are generally in charge of audit and risk assurance, whereas risk management is an executive role. Non-executive directors will have the chance to assess risk performance and get risk assurance when the audit committee receives reports from the risk management committee.

The risk committee may not need to be a direct report to the main board for firms that do not operate in such a high-risk environment. The risk committee in these situations can be a subsidiary of the executive committee or the operations committee. In all circumstances, the corporate structure for risk management should be commensurate with the organization's degree of risk as well as its size, complexity, nature, and risk exposure. However, there are no certain proper frameworks for an organization's risk architecture. The risk committee's membership and terms of reference will be decided by the organization, provided that it produces the needed outputs. However, the overall notion that risk management is an executive role and audit operations should be overseen by non-executive directors is still valid [7].

The Risk Committees

Outlines the usual duties of a risk management committee (RMC). A senior non-executive director serves as the head of the audit committee, which is present in the majority of big corporations. Many firms have proposed expanding the audit committee's responsibilities to include all facets of risk management or creating a separate risk management group led by an executive director. The RMC should be an executive group rather than a member of any existing non-executive audit committee, according to a compelling case. This is essential since managing risks pro-actively is an executive duty. The current audit committee will probably see risk management as a non-executive (reactive) compliance audit. It will also be in line with the fundamentals of sound company governance to separate executive responsibility for risk management from non-executive duty for auditing and reviewing compliance.

Some organizations have created the RMC as an audit committee subsidiary. If this is the case, steps must be made to guarantee that risk management is handled as an executive responsibility rather than being checked during an audit as a matter of compliance or assurance. In reality, making the RMC a subcommittee of the audit committee would add to its administrative burden and place an undesirable focus on compliance and auditing at the expense of proactive risk management. Another issue that has to be addressed is RMC membership. In large organizations, the fundamental choice is whether the risk management committee should consist of a select group of senior executives who set strategy and policy, or whether it should be a knowledge-sharing group with representation from all organizational units and departments. The solution will depend on the organizational structure and the committee's intended mission. There has been much debate over the risk committee's mandate and place within the organization's risk architecture. There is a claim that the risk committee should solely consist of executives since the highest executive management inside the organization is in charge of managing risk [8].

to provide risk management advice to the board and to promote a culture that highlights and exemplifies the advantages of a risk-based approach to risk management. To properly advise the board on all important issues pertaining to the company's risk strategy and procedures. To analyze reports created by relevant parties and keep track of how well the risk management systems are doing. To continuously assess the efficiency of the company's risk management infrastructure, including:

Assessment of risk management practices in light of operational environment changes. To determine the degree of company risk exposure, take into account risk audit reports on the major business sectors. Taking into account any significant conclusions from any risk management evaluations and the management's reaction. Evaluating the risks associated with new endeavors and other operational, project, and strategic activities. To evaluate the company's risk exposure in light of the board's risk appetite and the company's capacity for risk. to take into account the evolution of risk management and provide the board with pertinent advice. To determine if the organization's disclosure of information about its main risk exposures and risk management practices complies with financial reporting requirements. The amount of risk that the firm should assume, however, is a crucial choice in various economic sectors. In banks and other financial institutions, this is unquestionably true.

Selecting a risk appetite and keeping track of actual risk exposure become high-profile board responsibilities in these situations. The risk committee will thus need to be a board-level group with both executive and non-executive membership. The risk committee, however, is unlikely to be a non-executive group, as the audit committee is, even under these conditions. Maintaining the integrity of the three lines of defense model will be crucial for the company if a risk committee is created as a subcommittee of the board. Any business must make crucial choices about the risk committee's terms of reference and place within the risk architecture. The arrangements must always be suitable for the organization and consistent with company operations. Additionally, the risk committee's structure must be suitable for the organization's internal, external, and risk management settings.

CONCLUSION

Simply said, there isn't a single solution that works for all enterprises. A distinct risk management committee may often be out of proportion to the degree of risk that the firm faces. In these situations, the duties that a risk committee would have performed will still need to be delegated to a committee with the appropriate level of seniority. Some businesses give the executive committee or the board's finance committee control over risk management. The organization's risk management standards must be improved in a prioritized, verified, and audited manner. Therefore, the risk management committee and audit committee should function in a manner that supports one another. For most companies, the wisest course of action will not be to merge the two committees into a single body or to elevate one committee over the other. The main worry is that by merging the risk and audit committees, the business would operate on a two-line of defense strategy rather to the three-line strategy that will provide stronger protection. Furthermore, the paper emphasizes the importance of accountability and transparency in risk management. It highlights the need for individuals and organizations to take responsibility for managing identified risks and to communicate the results of risk management activities to stakeholders. Overall, the paper emphasizes the critical role of risk management responsibilities in the success of risk management efforts. It highlights the need for individuals and organizations to work together, assign clear roles and responsibilities, and promote accountability and transparency to ensure that risks are effectively managed and that the organization achieves its goals.

REFERENCES:

[1] K. Oliveira, M. Méxas, M. Meiriño, and G. Drumond, "Critical success factors associated with the implementation of enterprise risk management," *J. Risk Res.*, 2019, doi: 10.1080/13669877.2018.1437061.

[2] M. Urbański, A. U. Haque, and I. Oino, "The moderating role of risk management in project planning and project success: Evidence from construction businesses of Pakistan and the UK," *Eng. Manag. Prod. Serv.*, 2019, doi: 10.2478/emj-2019-0002.

[3] Y. F. Kuo, Y. M. Lin, and H. F. Chien, "Corporate social responsibility, enterprise risk management, and real earnings management: Evidence from managerial confidence," *Financ. Res. Lett.*, 2021, doi: 10.1016/j.frl.2020.101805.

[4] B. W. Husted, "Risk management, real options, corporate social responsibility," *Journal of Business Ethics*. 2005. doi: 10.1007/s10551-005-3777-1.

[5] H. L. Tran, V. H. Bui, T. T. H. Phan, X. C. Dau, M. D. Tran, and D. T. Do, "The impact of corporate social responsibility and risk management on financial performance: the case of vietnamese textile firms," *Manag. Sci. Lett.*, 2019, doi: 10.5267/j.msl.2019.4.003.

[6] D. Henstra, J. Thistlethwaite, C. Brown, and D. Scott, "Flood risk management and shared responsibility: Exploring Canadian public attitudes and expectations," *J. Flood Risk Manag.*, 2019, doi: 10.1111/jfr3.12346.

[7] S. F. Kingma, "Paradoxes of risk management: Social responsibility and self-exclusion in Dutch casinos," *Cult. Organ.*, 2015, doi: 10.1080/14759551.2013.795152.

[8] T. Naseem, F. Shahzad, G. A. Asim, I. U. Rehman, and F. Nawaz, "Corporate social responsibility engagement and firm performance in Asia Pacific: The role of enterprise risk management," *Corp. Soc. Responsib. Environ. Manag.*, 2020, doi: 10.1002/csr.1815.

CHAPTER 21

CONTROL OF SELECTED HAZARD RISKS

Manjula Jain, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-jainmanjula776@gmail.com

ABSTRACT:

Hazard risks are a potential threat to individuals and organizations, and it is essential to identify, assess and control them to prevent harm. Effective hazard risk control measures require a systematic and proactive approach that involves hazard identification, assessment, and implementation of control measures. This paper provides an overview of the importance of controlling selected hazard risks in ensuring safety and preventing harm. It explores the key steps involved in the hazard risk control process, including hazard identification, risk assessment, and implementation of control measures. The identifies the various types of hazard risks that organizations may encounter, such as physical, chemical, biological, and psychological hazards, and the importance of identifying and assessing them to determine the most appropriate control measures.

KEYWORDS:

Business, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

A risk's inherent level is its level when no control measures are in place. The gross amount of the danger is another name for this. The degree of risk that takes into consideration the present control measures is known as the current level of risk. This is often referred to as the residual risk or the net level of risk. The term "current level" rather than "residual level" has been used throughout this book since it suggests a far more dynamic approach to risk management. When controls are implemented, it gives an example of the control effect or control vector. The company should be aware of the cost associated with adopting controls while taking into account the inherent, intermediate (where more than one control is in place), and goal risk levels. The organization's overall cost of risk should be taken into account when calculating the cost of the control measures. The company may then assess the effectiveness of the controls in place.

For Risk A, a succession of lines may be created to show the impact of each distinct risk management method. It is evident that the control's impact increases with line length. In terms of management time, effort, and financial resources, it is also true that the longer the line, the larger the control effort. To reach the goal level of risk for Risk A, three controls (Control A, Control A, and Control A) are necessary. Since just one control is necessary for Risk B (Control B), it is clear that significantly more work is required to keep Risk A at the desired level of risk. This is important to know for management and internal audit to verify that all controls (particularly for Risk A) are running effectively and efficiently. the difference between the risk's intrinsic level

and its present level. Additional control work will be needed to transition the level of risk from the present to the new goal level (not indicated in the picture) if a lower target level of risk is created. This straightforward example of control effort is significant and shows the need of doing a risk assessment at the inherent level of risk (if this is feasible), in order to clearly identify and depict the necessary control effort.

The total benefit of each control may be calculated by first calculating the risk exposure at the original level and then calculating the risk exposure at the new level. The cost of each control may then be taken into account, allowing for the completion of a cost-benefit analysis of each control. This will be a crucial task for the firm to carry out in order to define priorities for cost-effective risk management. The selection and execution of activities to lessen risk probability and risk effect constitutes risk treatment, which is sometimes referred to as risk response or risk management. When determining the kind and scope of risk management actions that should be undertaken, the various control types discussed in Paper should each be taken into account. It goes without saying that preventative measures should be implemented as a first resort whenever reasonably practical. Corrective measures should be used to reduce the probability and effects of an adverse occurrence if prevention is not practicable.

The company should think about directive controls that are intended to lead the activities of those engaged in the management of that specific risk after hazards have been avoided and remedied to the maximum degree possible while still being cost-effective. Finally, the use of investigative controls may be useful in addition to the other three kinds of controls. Detective controls have several uses, including those related to health and safety. The key hazard concerns that are likely to worry an organization are covered in the examples in the sections below. describes the potential consequences of the risk as well as the factors and problems that need to be taken into account. Following assessment of the measures that are essential and suitable, the control choices that are accessible in respect to that specific risk are taken into account. To show how various sorts of controls might be applied to these two threats, the examples of fraud and health and safety are used. The sorts of controls that may be used for various hazards threats that aren't included here might be specified using the framework of preventive, corrective, directive, and detective controls. It's crucial to choose controls that are both affordable and effective when choosing and implementing controls. Plots the decreasing potential loss (vertical-axis) and the decreasing cost of controls (horizontal-axis) versus rising control level (horizontal-axis). It does this by combining the total cost of controls and the comparable potential loss for each level of control.

DISCUSSION

Controls that are Affordable

The implementation of low-cost controls results in a large decrease in potential loss. 'Cost-effective controls' is the label for this area. The central portion of the picture shows how increasing the amount spent on controls may reduce the net cost of risk up to a certain point. Decision-making is needed in this section over whether to use the extra money for controls.

Spending more on controls on the right side of the results in just a little decrease in potential loss. Additional regulations in this section are not economically viable.

Taking notes on Controls

The many instances taken into account in this paper provide a broad overview of the hazards dangers that a company may encounter. This book has covered a lot more risk instances than those included here. Making judgments on the best and most affordable controls to implement is a constant aspect of all different sorts of hazard hazards. The core of risk management is uncertainty in terms of probability, effect, and consequences. Both demonstrate the necessity for judgment when doing risk analysis and risk appraisal as well as when taking into account the effectiveness of current controls and the need for new ones. Decisions must always be made based on the greatest information available. The ability to identify superfluous and unnecessarily complicated controls and take action to delete, modify, or replace them with more cost-effective alternatives is another significant benefit of trying to learn from controls. Because the type and effectiveness of the controls will have an impact on the amount of risk, risk assessment activities should take this into consideration. Internal audit has a well-established field of competence in the responsibility of monitoring controls.

It's possible that the major goal of learning from controls is to make them more effective. To make sure they are appropriate controls and effective, nevertheless, is also required. The review of the efficacy and efficiency of current controls by internal audit will help with learning from controls. The desired degree of reward should be taken into account while evaluating controls. The efficacy and efficiency of hazard and compliance controls must thus be evaluated, together with strategy and tactics. The focus of this paper has been on hazard controls, with information provided on some of the more typical dangers that many businesses would encounter. The concepts and guidelines presented in this paper apply equally to opportunity management and show how the interaction between risk exposure and expected return influences company choices. At first, a bigger payoff will be anticipated as risk exposure rises, and the rise in benefit outweighs the rise in risk exposure. There will ultimately be more exposure but not more projected payoff, therefore there is no advantage to take that additional risk. In the middle of these two scenarios, increasing risk exposure will only slightly boost expected benefit [1].

In this middle ground, management must decide if the organization's appetite for risk is being met by the rise in risk exposure. Although it may not seem reasonable to raise risk exposure in exchange for a little increase in expected profit, doing so could be required to meet the needs of current customers or to further a longer-term company goal. It is possible to do a similar analysis in regard to hazard hazards, where the expense of additional controls must be weighed against the decreased risk exposure that would follow. The company must assess its risk appetite and decide what risks it is ready to accept in order to achieve its strategic goals before determining whether to install additional controls.

Limiting Financial Risks

Fraud

Fraud is a major source of financial risk for all firms and may be perpetrated by suppliers, customers, or staff. By reporting fraudulent operational outcomes, a company itself may also commit fraud. The Sarbanes-Oxley Act's regulations are largely designed to prevent corporations from reporting false information. Fraud happens when there is a desire to do it, the company has valuable assets, there is a chance to commit the theft or fraud, and there is insufficient control. Measures meant to deter theft should also be included in concerns about fraud. These will involve installing security fences and gates, hiring security guards, upgrading lighting, and providing safe building access.

The efficacy of an organization's fraud controls has to be evaluated. Internal audit often gets engaged in this area. This study should look for financial or material losses and determine where there are inadequate controls. The study should be a proactive evaluation that looks at susceptible assets, who is in charge, potential fraud methods, and the efficiency of the current measures. Organizations should assess situations where fraud has been identified on an annual basis and analyze the efficacy of the safeguards in place. The audit committee should get these reports. A corporate fraud policy that outlines the company's stance on fraud, the procedures for detecting and investigating it, who is responsible for managing it, and the resources allotted to it should be implemented by the business in order to avoid fraud. Additionally, procedures for reporting fraud suspicions and a strategy for handling them should be devised. Preventive, corrective, directive, and detective risk management measures fall under the aforementioned categories. Organizations have access to the following techniques for reducing fraud.

Historical Obligations

Organizations' exposure to past obligations is one of the most challenging financial risk sectors. These obligations result from an organization's prior operations or from newly acquired components of the company that were acquired together with their prior obligations. The prior exposure to substances that may result in delayed industrial illnesses is an area that is particularly challenging to measure for industrial enterprises. The most notable example is asbestos exposure and the risk for mesothelioma, a deadly cancer of the pleura or lining of the lungs. For many businesses, mesothelioma claims start to surface years after the claimed exposure. Exposure will have happened at a period when it may be difficult to validate insurance agreements and there won't be any more documentation of the precise working circumstances.

Pension funds are another source of past liability risk. In the past, a lot of pension funds provided pension plans based on the employee's last pay. Common names for them include defined benefit pension plans. In a defined benefits pension plan, the employer is solely responsible for the risks relating to the value of the pension fund and the amount of pension that the available money will buy. Recently, there has been a growing trend toward pension plans that accumulate funds that may be used by the workers to buy a pension when they retire. This model, which is sometimes referred to as a defined contribution pension plan, requires the employee to make financial contributions to his or her pension fund. In this arrangement, the risks related to the value of the

fund have been significantly reduced, and the employee now bears the risk related to the value of the pension that the fund will acquire.

The defined benefit pension plan and the responsibility to individuals who are no longer employed by the firm but have pension rights under the defined benefit pension plan are the specific risk management problem that companies are worried about. Deferred benefits are the name given to them often. For managing these delayed benefits, the firm will need to consider its risk management choices. Deferred benefit ex-employees can be persuaded to leave the program by being paid a certain amount, their deferred benefits can be transferred to an insurance company in exchange for payment of an annuity premium, or they can be attempted to be transferred into a captive insurance company. By definition, historical liabilities of this kind are a bigger problem for firms that have been around for a while. This implies that the company will be well-established and that other parties will be able to pursue liabilities that first surfaced a long time ago. If the organization has evolved over time, particularly if it is substantially smaller than it was in the past, these historical liabilities may be more severe. Additionally, firms that have had a lot of merger and acquisition activity will be more vulnerable.

Risk Management for Infrastructure

Workplace Health and Safety

Health and safety at work are one of the main areas of worry when it comes to infrastructure hazards for enterprises. All organizations should have a top priority for this highly regulated subject. Although it is often handled as a standalone function, it is a well-established discipline within risk management. An organization's health and safety risks include being investigated by a regulatory body, facing legal action from a hurt worker, and experiencing interruption due to mishaps and hazardous situations. There is no question that the complete involvement of health and safety experts is essential to the success of any risk management endeavor. Many health and safety methods and approaches are used in wider risk management operations.

It has long been acknowledged that conducting risk analyses in regard to health and safety is important. When the hazards are minimal, these risk evaluations might be general. Specific documented, in-depth risk assessments will often be needed for high-risk operations. Identification of the risk, identification of potential victims, and evaluation of the severity of any injuries are all characteristics of a risk assessment. The risk assessment should also contain information on the controls and measures that are in place as well as any further steps that are necessary. The main goal of doing a risk assessment is to make sure that the controls are sufficient and that no one is put at unnecessary danger. In connection to the threats to one's health and safety and this hierarchy, there is a set of controls. When compared to the recognized nomenclature for the hierarchy of controls for workplace health and safety, the general generic control categories of preventative, corrective, directive, and detective controls also apply to fraud threats. After conducting a risk assessment of the health and safety risks, organizations must implement controls, which will include preventive controls, corrective controls, and directive controls. Preventive controls aim to reduce risks, while corrective controls aim to control hazards. Lastly, in some situations, health and safety controls that are designed to catch the first

indications of illness may also be necessary (detective controls). When it comes to managing employee stress at work, investigative measures may be necessary to spot early warning signals that staff members are suffering from stress. Depending on the precise nature of the company, there are a variety of workplace dangers that should be taken into account while conducting risk assessments [2].

Fire Protection for Property

Fire is one of the most frequent sources of damage and downtime for enterprises engaged in manufacturing, warehousing, leisure, and retail. More than half of businesses that experience a catastrophic fire don't completely recover. For industries including manufacturing, transportation/distribution, and retail and especially for places of residence, hospitality, and recreation fire is a very dangerous occurrence. The degree of building security in place and the avoidance of arson assaults are also strongly correlated. The company must assess the fire risks in connection to the typical workplace fire causes while developing a fire risk plan. Protecting the safety of anyone who could be impacted by the fire is the main goal of fire safety measures. The availability of emergency evacuation signals and the sufficiency of fire exits should both get careful consideration. Additionally, structures should be well-built, and if required, sprinklers should be used to appropriately cover fire escape routes. Organizations should assess the possibility for the disruption that might follow from a fire, even though human safety is the most crucial factor in fire safety. It is widely documented that loss-control strategies may be used to avoid fires. Loss prevention, damage control, and cost reduction should all get adequate consideration[3]–[5].

Application of preventative controls to the prevention of a fire is property loss prevention. These preventative measures will include keeping up with electrical installations, avoiding ignition sources, and storing flammable and combustible products properly. Sprinkler system installation and the implementation of fire separation plans are examples of corrective controls. The effect of a fire and the amount of damage it produces will be lessened by the employment of directive controls. Controls with directives provide personnel instructions and information on what to do in the case of a fire. These will involve notifying the fire department in advance and, if possible and safe, having staff members utilize the profile extinguishers. To prevent fires from spreading, detective measures can include the installation of heat and fire detectors and regular patrols by security and fire authorities.

IT Protection

The information technology (IT) infrastructure is one of the main dependencies for the majority of enterprises. For many firms, the breakdown of a computer system may be an extremely disruptive occurrence. The IT infrastructure is one of the best-known applications of disaster recovery planning (DRP). Loss of computer data may have major ramifications for a company, and hardware faults are more likely to be to blame than other problems like software glitches, electrical problems, or human mistake. Organizations must anticipate potential losses and take steps to control the corresponding risks as their reliance on computer systems grows.

The majority of firms will need to put up an IT policy that is intended to guarantee proper data usage while also safeguarding the organization's IT infrastructure. Information on who is responsible for maintaining IT systems, specifics on backup methods, anti-virus and spyware procedures, use of personal data, personal internet use, and limitations on personal e-mail use should all be included in the policy. Most businesses let their staff to use computers for personal purposes up to a certain point. This shouldn't, however, be allowed to go too far, and there should be clear limitations on internet access to improper websites. Data protection and the use or disclosure of personal information by the organization are two more areas of concern for organizations. The security of personal data stored on computers is subject to stringent legal standards in the majority of nations [6].

There may sometimes be computer and IT failures, therefore the firm should make sure there are suitable backup plans in place to guarantee that only a small amount of data is lost. Organizations that rely heavily on their IT infrastructure need to have comprehensive DRPs in place. These will often include plans for an emergency duplicate back-up computer facility, which will be accessible either on a mobile trailer driven to the organization's current office site or at a different location. A cold-start facility is an alternate computer system without any data preloaded, whereas a complete duplicate facility with completely updated information (commonly referred to as a hot-start facility) is also a kind of emergency backup facility. These two techniques may be combined to provide a variety of backup system possibilities, which are sometimes referred to as warm-start facilities.

HR Hazard

Every company needs a workforce made up of paid employees, independent contractors, and/or volunteers. Because of this, no matter an organization's size, kind, or range of operations, there will always be human resources risks associated with its operation. There are many risk factors connected to hiring employees and using human resources inside the company, including:

1. The hiring of new employees and dismissals;
2. Adherence to laws and regulations;
3. Skill availability, retention, and recruitment;
4. Plans for pensions;
5. Management of performance and absences;
6. Safety and health.

Large firms often have an HR department with available staff and/or human resources experience. Large firms are seen to be more vulnerable to HR issues than smaller ones. This concept has been supported by the idea that since there are fewer people engaged and people know one other better in small companies, there are deeper working ties across the whole company. It has been thought that because of these deeper working connections, the company is less susceptible to litigation or other disruptions brought on by employee problems. However, it has recently become clear that smaller businesses are also subject to severe HR hazards. Due to this awareness, the majority of small businesses now create a staff handbook that outlines the

terms and conditions of employment, including plans for sick leave, maternity leave, and yearly leave, as well as policies for evaluations, workplace behavior, and roles and duties.

Organizations must establish policies that will assure complete compliance with the applicable employment laws, including diversity policies, to prevent discrimination based on physical characteristics or ethnic origins. Organizations should consider the opportunities that will result from having helpful, understandable, and advantageous hiring, retaining, and employment procedures while expanding on these fundamental legal needs. Any company's brand name is one of its most precious assets, therefore it's critical to protect it and all of its brands from harm. Brand damage may happen for a variety of causes, such as:

1. Alterations in governmental policies;
2. Alterations in the economy;
3. New competitors entering the market;
4. Rivalry for specifications and pricing;
5. False and counterfeit items;
6. Unsuitable franchisee conduct;
7. Failure of the joint venture partner or the sponsor.

Recently, it has been popular to offer products or services that have no visible connection to well-known brands by using those companies' existing reputations. As an example, supermarkets now provide insurance, other financial goods, and gasoline from front-court garages. For many firms, extending or expanding the brand in this manner gives a significant potential, but brand extensions need to be suitable, believable, and effective as well. The majority of businesses cherish their brands and have processes in place to spot chances for brand expansion. But in many big firms, brand ownership isn't always clearly established. It is only possible to successfully utilize a brand to expand into new product categories and industry verticals when there is a defined organizational role for managing the brand.

Along with brand extensions, there has been a recent tendency to permit the establishment of branded concessions inside other enterprises. High-profile catering companies now often oversee the cafeteria and restaurant operations at major department shops. Along with the rise of high-profile sponsorship agreements, this tendency has emerged. For instance, a lot of sports teams have a brand-new stadium that goes by the name of their primary sponsor. Many businesses run on a franchise model, where the brand is licensed to a person or another company. These advancements in branding allow for the most profit to be made from a well-known brand. These benefits come with a lot of hazards too, and trademark usage and expansion is still a problem that has to be handled carefully. There are several obstacles to successful franchise brand management. Although some franchise organizations have been around for a while and the original franchisees may not have had the same strict contract terms, in most situations the expectations and criteria of the franchise or brand owner would be spelled out in a formal contract. The majority of franchise owners provide thorough training to franchisees, sometimes including instruction on product quality. The arrangements for supply acquisition represent a substantial problem for many franchise owners. In order to ensure that the franchisee constantly

delivers the same product, the franchise owner may often forbid the franchisee from buying materials locally [7].

Environment

Global warming and the potential effects of people's and organizations' actions are among the social issues that are advancing the fastest. Environmental concerns may vary from problems with previous soil pollution and water supply contamination to difficulties with industrial emissions into the atmosphere and companies' wish to be seen as environmentally friendly. All organizations are concerned about garbage disposal. The law is quite specific about how industrial waste must be handled and how preparations must be made for its disposal for companies that produce it. There are still concerns for business companies even if they don't create industrial waste or byproducts. Commercial garbage disposal may be expensive, and most nations mandate or (at least) strongly promote recycling.

Therefore, reducing the volume of commercial trash that they generate and implementing other environmentally friendly practices are major considerations for many firms. Due to increased monitoring of public bodies' performance, recycling arrangements are intricate and recycling goals are significant for many public sector organizations. The acquisition of raw materials or supplies with a reduced environmental effect and/or that are simpler to recycle will be one of the arrangements that may be looked at. Additionally, businesses may want to establish a recycling strategy and set up particular procedures for the collecting of recyclable garbage. There may be room for certain firms to examine employee travel plans, encourage them to utilize public transportation when possible, and limit the quantity of travel they do. There are comprehensive standards, norms, and regulations in place for industrial activities, and the enforcement authorities are given significant authority [8].

Keeping up with client expectations and demands is one of the biggest difficulties confronting companies. The ongoing advancement of technology makes this problem more challenging. Companies that provide technology-based consumer products confront a constant struggle, which may also be a constant set of possibilities. In recent years, there have been significant changes in the technology utilized to deliver home and mobile communications and entertainment. Home entertainment and mobile entertainment were formerly reliant on CDs. The emergence of MP technology presented a choice for the organizations functioning in this field over which technology to pursue. The costs associated with changing technology were high, and there were major market risks. The benefits have proven to be significant for the firms who properly detected (and impacted) the advances. Technology benefits in a market that is changing quickly might be considerable, but it can be difficult to choose the technology that will likely succeed, and doing so requires a large investment.

Convenience, quality, affordability, and fashion are the main factors that influence consumer judgments about new technology. The fact that important technological advances of this kind take place on a global scale also has an impact on consumer choices and the accessibility of new technologies. As a result, relatively few companies have the funding to do the research necessary

to create goods based on the new technology. Additionally, they are the same companies who create, produce, and provide products that make use of the new technology.

Numerous firms must form joint ventures, pool their resources, and split the expense of developing the new technologies in order to benefit from them. Selecting joint venture partners may be challenging, and making the right choices is crucial. Competitors sometimes make an effort to agree on the technology that will be chosen while producing a new entertainment technology that will be launched around the globe. The benefit of this strategic strategy is that it prevents technological wars and splits the expense of research. The drawback is that there is less potential for a significant future competitive advantage.

Legal Dangers

Regulatory risk is one of the most challenging risk problems for many firms. The attainment of compliance by the organization is a crucial part of the COSO framework. Although compliance may seem like a fairly simple problem, there are often complications brought on by the possibility of regulatory changes, shifts in the regulatory environment, and variations in regulatory standards across various jurisdictions. Various civilizations have varying and shifting perspectives on certain business sectors. As an example, various regions of the globe have varied standards and regulatory frameworks for the sex business. Additionally, gaming is subject to diverse public perceptions, legislative frameworks, and activity limits depending on the country. It may be challenging to ensure regulatory compliance and maintain positive working relationships with regulators, particularly when public opinion is shifting and/or new or altered regulatory frameworks are being constructed.

The challenges of guaranteeing compliance in the acquisition and implementation of multinational or global insurance programs have received a significant deal of attention lately. Two significant topics have gotten a lot of attention. These include the payment of insurance premium taxes in various jurisdictions and the legitimacy of insurance coverage offered in a nation by an insurance provider without a physical presence there. In relation to global insurance policies, issues arise when a global policy is issued by a large company based in one particular country, but with the insurance coverage applying across all of the organization's operations and in several different countries (insurance written by an insurance company without a presence in a territory is referred to as non-admitted insurance). The payment of insurance premium tax on the portion of the insurance premium that is related to the organization's activities in each nation is governed by local laws. Additionally, non-admitted insurance products are prohibited in many international jurisdictions.

CONCLUSION

Naturally, there are only a limited number of risk control alternatives accessible to firms looking to attain compliance. Compliance is a fundamental need for all commercial and economic activity. Cooperation with outside parties and in-depth guidance from subject-matter experts in that region of the globe may be necessary to ensure compliance. For instance, in the case of insurance, it could be essential for a local insurance business to participate in the insurance program in areas where non-admitted insurance is not permitted, which would increase the cost

of the insurance programs. Additionally, it may be necessary to make arrangements for the payment of insurance premium tax via third-party fiscal agents inside the jurisdiction where the taxes are due. Overall, the paper emphasizes the critical role of hazard risk control measures in ensuring safety and preventing harm. It highlights the need for organizations to adopt a systematic and proactive approach to hazard risk control and to implement effective and appropriate control measures to minimize the impact of identified hazards on individuals and organizations.

REFERENCES:

[1] M. Z. Zakaria, E. Z. Abidin, and N. A. Ya'acob, "Hazard identification, risks assessment and risk controls of work tasks in selected tea and cocoa plantations in Malaysia," *Malaysian J. Med. Heal. Sci.*, 2019.

[2] G. Leonenko *et al.*, "Polygenic risk and hazard scores for Alzheimer's disease prediction," *Ann. Clin. Transl. Neurol.*, 2019, doi: 10.1002/acn3.716.

[3] P. Willumsen, J. Oehmen, V. Stingl, and J. Geraldi, "Value creation through project risk management," *Int. J. Proj. Manag.*, 2019, doi: 10.1016/j.ijproman.2019.01.007.

[4] G. O. Danisman and P. Demirel, "Corporate risk management practices and firm value in an emerging market: a mixed methods approach," *Risk Manag.*, 2019, doi: 10.1057/s41283-018-0040-5.

[5] F. Kabuye, N. Bugambiro, I. Akugizibwe, S. Nuwasiima, and S. Naigaga, "The influence of tone at the top management level and internal audit quality on the effectiveness of risk management practices in the financial services sector," *Cogent Bus. Manag.*, 2019, doi: 10.1080/23311975.2019.1704609.

[6] N. Sattar *et al.*, "Age at Diagnosis of Type 2 Diabetes Mellitus and Associations With Cardiovascular and Mortality Risks: Findings From the Swedish National Diabetes Registry," *Circulation*, 2019, doi: 10.1161/CIRCULATIONAHA.118.037885.

[7] M. Tancredi *et al.*, "Excess Mortality among Persons with Type 2 Diabetes," *N. Engl. J. Med.*, 2015, doi: 10.1056/nejmoa1504347.

[8] N. S. Tzeng *et al.*, "Anti-herpetic Medications and Reduced Risk of Dementia in Patients with Herpes Simplex Virus Infections—a Nationwide, Population-Based Cohort Study in Taiwan," *Neurotherapeutics*, 2018, doi: 10.1007/s13311-018-0611-x.

CHAPTER 22

AN OVERVIEW ON RISK-AWARE CULTURE

Chanchal Chawla, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-chanchalchawla0@gmail.com

ABSTRACT:

Employees who understand their duties in risk management and who are aware of the dangers connected to their occupations operate in an atmosphere where there is a risk-conscious culture. It is crucial to efficient risk management since it aids in identifying and reducing possible hazards before they become an issue for businesses. An overview of the significance of a risk-aware culture in risk management is given in this paper. It looks at the advantages of encouraging a risk-awareness culture, such as enhanced risk detection, higher responsibility, and improved decision-making. The paper lists the essential components of a risk-aware culture, including support from the leadership, clear communication, and continual training and growth. It also looks at how workers may encourage a risk-aware culture and the need for businesses to promote a culture of ongoing learning and development in this area.

KEYWORDS:

Business, Mitigation, Magnitude, Risk Probability, Risk Management, Organizations.

INTRODUCTION

We have previously seen that there are three (complementary) risk management approaches depending on the kind of risk being taken into account. The methods used by an organization to manage risk at a given moment are defined and described by the three terms: hazard management, control management, and opportunity management. There will always be a bad result when taking a risk like a hazard. The hazard tolerance is the greatest exposure to danger that the organization will tolerate. Risks that can be controlled will come at a cost, which is referred to as the control acceptance cost. Opportunities risks may result in a variety of results, from very good to extremely bad. Of course, the desired and anticipated result is favorable. The opportunity investment is one where the company is ready to risk resources in search of opportunity risks. The kind of risk being taken into account influences the approach to risk management that will be used. However, depending on where a risk is in its lifecycle, it could be necessary to manage it utilizing all three risk management approaches. The four risk management approaches may be summarized as follows:

1. Compliance management: based on upholding legal responsibilities, such as those related to health and safety.
2. Hazard management: 'total cost of risk' strategy created by the insurance industry (s).

3. Control management is based on the internal auditors' approach to control.
4. The intersection of risk management and strategic planning is opportunity management (s).

The principles that the organization is willing to jeopardize include hazard tolerance, control acceptance, and opportunity investment. These three elements when combined indicate the organization's overall acceptable risk exposure and its risk appetite. The aggregate of the individual risk exposures creates the overall risk exposure, which may or may not align with the board's risk appetite or the organization's risk capacity. In most cases, the insurance risk manager will handle motor vehicle hazards as a matter of loss minimization or "total cost of risk." The internal audit department will typically monitor and assess the prevention of internal fraud as a matter of internal control. The CEO or another top executive should handle the risks involved in a merger or acquisition as an opportunity problem.

A risk management effort will be necessary in order to enhance an organization's risk management performance. The scope of this endeavor will depend on the organization's size, complexity, and character. When it comes to adopting risk management in a company, there is no one right way to do it. The motivations for risk management initiatives, as well as the anticipated results and effects, will differ amongst enterprises. Despite the fact that there is no one perfect strategy, this paper outlines some of the essential elements for effective risk management. An technique that is fully compatible with the problems is presented in Appendix C. A list of the numerous risk management tools and strategies connected with each step in the execution of a successful enterprise risk management program is also provided in the appendix, which includes compiles the acronyms used throughout the book [1].

Making sure that the risk management project is supported by a board member or a senior member of the executive committee of the business is the first and maybe most crucial stage. The numerous risk management frameworks and standards that are described throughout this book also provide information on how to successfully introduce a risk management program. The actions that different businesses will take will alter as risk management evolves and changes. The governance, risk, and compliance (GRC) movement has modified and advanced the setting for risk management. Professionals in risk management need to be aware of these developments and changes in order to make sure that their operations are always perfectly coordinated with those of the rest of the company. Or, to put it another way, risk management efforts need to always be completely in line with the internal environment. Although having a general strategy for the execution of the risk management initiative is crucial, it is equally crucial that the risk manager specifically pinpoints any obstacles to the initiative's implementation. The possible roadblocks and facilitators to a risk management initiative's effective implementation. The following are only a few of the numerous variables that will affect the strategy's effectiveness:

1. Top management's influence over departments;
2. Outside factors, such as company governance;
3. The nature of the company, its offerings, and its culture;
4. Business philosophies, especially prior RM encounters;
5. The beginnings of the risk management division.

By recognizing obstacles, one may put strategies in place to go around them. These include the need of everyone's commitment to effective risk management and the idea that implementation is only as good as the department's least dedicated employee. The best choices to guarantee that risk management offers the most advantages will be identified via analysis of these obstacles within the context of the particular firm.

No one course of action will guarantee proper implementation, and there is no single deadline by which implementation will be completely realized. Many businesses have found that it might take between two and five years to fully adopt the method at all levels. The documentation process will be one of the crucial factors to take into account while determining the implementation schedule. The timeframe for effective and thorough deployment may be increased if a comprehensive risk management information system (RMIS) is deployed [2].

How to define risk culture

It might be challenging to describe an organization's culture. It is widely acknowledged, nevertheless, that it reflects the mentality of the whole management team as a whole. How people behave inside an organization is influenced by its culture. It will specify how a person feels compelled to act in every situation.

A healthy risk culture will result from attitudes and behavioral patterns, as well as from individual and community ideals. This will result in a dedication to the organization's risk management goals. Communication that is based on mutual trust and a common understanding of the significance of risk management are characteristics of organizations with a risk-aware culture. Along with shared trust in the chosen control mechanisms, there also has to be a dedication to following the defined risk management protocols. The potential elements of a risk-aware culture. Recent UK Health and Safety Executive (HSE) study suggests that these elements include leadership, engagement, learning, accountability, and communication. So, LILAC becomes the acronym. Most businesses have a long-term goal of developing a culture where efficient risk management is fundamental to how employees do their jobs.

An organization may opt to start a campaign to highlight the dangers and relevant controls if it intends to increase public awareness of security concerns. If the campaign is to be effective, it must use several forms of communication. The LILAC components might all be a part of the awareness campaign, which could also include:

1. Risk awareness instruction;
2. Poster campaigns promoting awareness;
3. Inspections of the site;
4. Arrangements for defect reporting;
5. Pamphlets and booklets.

Without the organization's culture being open to it, a risk management effort will fail. A risk-aware culture is necessary in the company for it to be responsive. Senior management must actively encourage a risk-aware culture in order for the organization to demonstrate a high degree of leadership maturity. This will include establishing goals for risk management

performance and ensuring that top management's commitment to the risk-aware culture is evident. Both oral and written communication will be needed for this. Achieving a risk-aware culture requires top management's involvement and engagement. Adequate training may foster involvement by ensuring that everyone fully understands their responsibility for hazards. Expert risk functions should serve in an advising or consulting capacity. Any actions that are likely to have an impact on the employees should be made known to them via feedback channels.

A risk-aware culture must have a learning culture in order to succeed. Organizations with a learning culture are better equipped to recognize and alter inappropriate risk behavior. A learning culture may emerge with the help of thorough study of situations and effective feedback transmission. Risk management workshops are yet another essential element of a learning culture. The effectiveness of the risk-aware culture depends heavily on accountability. It differs from a blaming culture, however. The company must see to it that it transitions from a blame-driven culture to a fair one based on responsibility. Management should show concern and care for workers while looking into situations. Employees should feel comfortable raising difficulties and concerns without worrying about being singled out for criticism or disciplinary action. A risk-aware culture requires effective risk information communication from top management. those from any employee, as well as those from outside the company, must be accepted and welcomed in order for communication to be effective. The communication efforts should include information on risk performance.

DISCUSSION

Measuring risk culture within a business may be challenging. But since the organization's risk culture is so crucial, measures must be made. How seriously a department or location approaches risk management is a question audit committee often ask. In general, it will be simple to provide a qualitative response to this topic. However, quantifiable assessments are necessary in order to pinpoint problem areas and develop corrective measures. The Canadian Criteria of Control (CoCo) framework serves as a tool for assessing the organization's risk culture. The audit committee's efforts to assess the amount of risk assurance offered by the specific unit or division under review serve as another indicator of the risk culture [3].

Examining the organization's degree of risk maturity is another way to gauge risk culture. Risk maturity models are more thoroughly discussed in a subsequent part of this paper. The degree of risk maturity may be determined quantitatively, and opportunities for improvement can then be found. An illustration of risk awareness and how risk management is ingrained in an organization's culture can be found in the box below. The effectiveness of a risk management policy and the specifics of the rules and procedures in the risk protocols or guidelines will offer a clue as to the organization's risk culture. Increasing the risk culture is a legitimate strategic risk aim for many firms. This will be particularly true if areas of risk awareness that need improvement have been found. Recognizing that bettering risk management procedures must result in bettering risk management outputs is crucial when taking steps to enhance risk culture within an organization. This should therefore have a favorable effect that increases the advantages of risk management. If the total efficacy of the risk management effort is not increased, there is no sense in upgrading the risk management procedures as a method of

changing the risk culture of the firm. There is a risk that upgrading and improving the risk management process will immediately be seen as increasing the risk culture in a company.

It is feasible to improve the risk management procedure without also improving the organization's risk culture. For instance, a more active internal audit program may raise compliance requirements, but it does not always mean that the organization's risk culture has improved. While enhancements to the risk culture should be anticipated to give a higher degree of risk assurance, improvements to the risk management process may not provide any further advantages. The standard contains information on the significance of the internal, external, and risk management contexts for the company. The advantages that will result from improved risk management inside the enterprise and context are closely tied. The control environment inside an organization is the focus of the Canadian Criteria of Control (CoCo) framework of internal control. In contrast to the control environment that is defined in the COSO Internal Control framework, the COSO ERM framework relates to the internal environment of the organization. The internal and control environments are indicators of the organization's risk culture and degree of risk awareness [4].

Through enhancements to the internal context, risk management context, control environment, or internal environment, risk performance will be improved overall. The degree of risk maturity, the development of a risk-aware culture, and the fulfillment of the established LILAC criteria are all ways to enhance the internal environment under management. The balanced scorecard method rose to prominence as a management tool in the s. Organizations may use this management approach to make their vision and strategy clear and put them into practice. Balanced scorecards are used by many major businesses to provide context for the many efforts that are carried out inside the firm. the federal agency that served as the model for a balanced scorecard-using enterprise. It makes sense to utilize the same framework for risk management activities if a firm implements the balanced scorecard. The likelihood that risk management requirements will be accepted and met increases when risk management techniques and procedures are consistent with ongoing operations. In order to integrate risk management within the business and foster a culture that is more risk-aware, these efforts constitute an alignment with current standards.

Coordination of Activities

The organization's primary business operations should be in line with the risk management activities, risk architecture, strategy, and procedures. Risk information circulates through the risk management system, producing a number of outputs if it is effective. The accomplishment of required requirements, provision of assurance, improvement of decision-making, and achievement of effective and efficient core processes have previously been mentioned as these outcomes. The majority of risk management guidelines mention the positive aspects of risk or cover how to handle opportunity risks. Within the field of risk management, project risk management also known as the management of control risks has grown into a distinct profession with its own set of guidelines.

Decide if the contribution will be related to strategy, projects, or operations when thinking about the contribution risk management may make to the company. This choice will make it possible

for the organization's risk management initiatives to be in line with other business objectives, activities, and imperatives. In order for the risk management processes to be completely integrated into the current management processes and activities inside the company, it is crucial that risk management activities be coordinated with other operations. This will also make sure that risk management operations are carried out effectively and are integrated into the management of the business, rather than being perceived as a distinct activity.

The internal auditing operations have to be in line with the organizational setting or culture. When selecting to create a risk-based audit program, internal audit takes a two-pronged strategy. Internal audit will first examine the high-risk activities and concentrate the audit program on them. Second, the risk-based audit program will consider the organization-wide maturity of risk management. Internal audit may elect to do a greater level of audit activities in that section of the business if it has a less risk-mature attitude [5].

The fragmented-organized-influential-leading (FOIL) method might serve as a further indicator of an organization's level of enterprise risk management integration. As the four levels of risk maturity are applied, it is clear from the features of the FOIL method and the four stages of risk maturity that enterprise risk management has a greater impact. When various risks are handled by professionals who don't always collaborate in separate departments and by different types of threats, there is a fragmented approach to enterprise risk management. For instance, a company could have outstanding standards for health and safety, security, and business continuity, but it might not have proven the advantages of collaboration. The next step is to coordinate these operations so that the corporate risk management strategy is more structured. When all hazards are taken into account, a thorough risk register is likely to be the end outcome. Enterprise risk management, however, offers additional advantages. These extra advantages accrue to organizations that set up ERM activities that influence decision-making. The impact of risk management and the risk manager

Decisions concerning strategy are driven by ERM considerations, which guarantee that risk-related concerns are thoroughly considered while strategy and tactics are formed. The consideration of risk is a significant component in corporate decision-making. The creation of strategy and tactics inside the firm is led by risk management in the final stage. In order to prevent the risk implications from being taken into account after the strategy and tactics have been established, this will need the risk manager being a member of a senior management team [6].

Models of Risk Maturity

Risk maturity models may also be used to gauge improvements in risk management efficiency. The advantages that may be obtained from risk management are indicated by the degree of risk management sophistication. A measurement of the effectiveness of risk management initiatives and the degree to which they are ingrained in the company is the level of risk maturity. Models of risk maturity may be used to gauge the organization's present risk culture. Risk management efforts will be incorporated more deeply into the organization's everyday business operations as

risk maturity levels rise. Later in this paper, the characteristics of an effective embedded risk management system are discussed.

Consideration of an organization's degree of risk management sophistication is not the same as risk maturity. While a company may have modest expectations for risk management, its approach to pursuing the rewards available to it is highly mature. An organization's degree of risk maturity provides insight into how risk procedures and skills are established and used. Informal risk management procedures will be used in a young company. But when things go wrong, there is probably a blaming culture in place, and there may be a lack of responsibility for risk. Additionally, resources allotted to risk management may not be suitable for the degree of risk involved.

The procedures will be kept active, relevant, and helpful when explicit risk management is in place. Open communication and learning are likely to occur, allowing for the utilization of information to support risk assessments and choices. There will be faith in the ability to manage innovation and risk-taking, with assistance when things go wrong. An company may struggle to manage risk effectively if it becomes too dependent on processes as a result of being risk-obsessed. Over-reliance on information at the cost of sound judgment and reliance on procedure to explain decision-making will both occur. People could become risk-averse because of a fear of being judged, and they might follow processes only to satisfy the law rather than for their own sake.

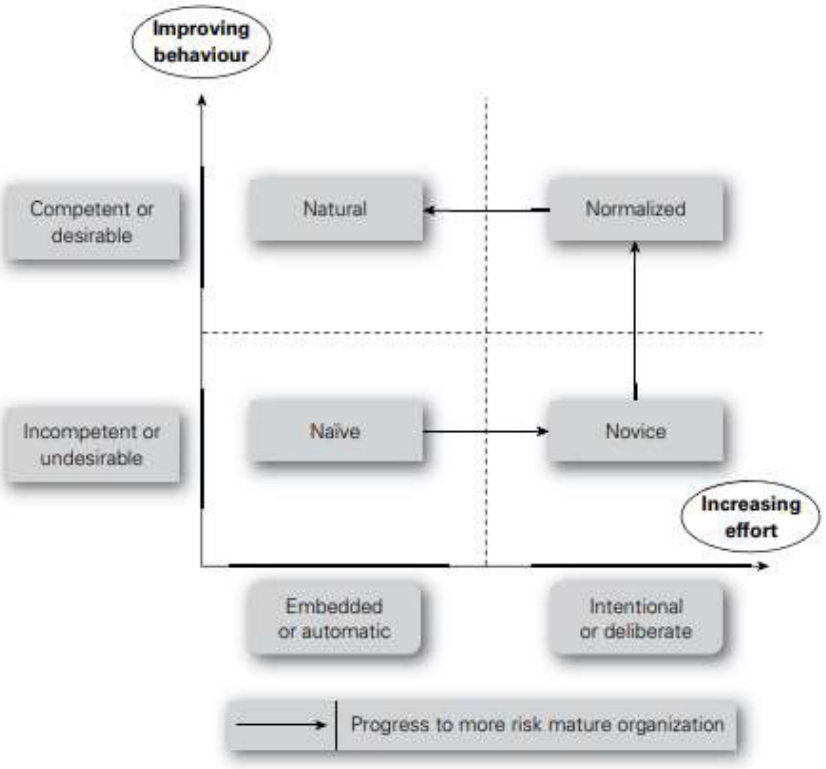

Figure 1: Illustrate the Risk maturity demonstrated on a matrix.

A method for assessing the organization's degree of risk maturity in relation to its risk management procedures. Here, risk maturity is divided into four categories: naive, novice, normalized, and natural (Ns). The Ns model is in line with the FOIL technique for characterizing the degree of risk maturity in an organization since each of these levels' attributes is specified. Undoubtedly, it is preferable for a company to aim for a greater risk maturity level. The method used by the company to achieve risk maturity should, however, be commensurate to the degree of risk it confronts. The degree of sophistication an organization has in its risk management operations will be determined in part by the amount of risk maturity that exists within the company. The degree of complexity that risk management may provide to business operations. The advantages increase when a company achieves a higher degree of risk management competence. Even while risk management procedures are becoming more mature, this does not imply that they will get more sophisticated or that they will provide more advantages [7].

However, one of the strategic goals for risk management inside the business may be to achieve a higher degree of risk maturity. If so, a recognized methodology for assessing risk maturity is necessary. The company must employ a risk maturity model that supports its goals for risk management maturity and offers a workable strategy that can be ingrained across the organization. Based on the Ns model, Figure 1 offers an assessment of the degree of risk maturity of a company. The graph implies a connection between competence or desired behavior on the one hand and ingrained or automatic behavior on the other. Unwanted or inept behavior will be automatically accepted in a naive company. An inexperienced company will recognize that the behaviors are unprofessional or unwanted and will begin to try to modify the behavior, but change will not yet have occurred. However, when change occurs, it will lead to better, more typical behavior.

A Matrix Showing the Risk Maturity

An organization that has reached the natural state of risk maturity has attained the level where competent or desired behaviors will take place without much managerial effort or enforcement. At this stage, the accomplishment is to guarantee that behaviors are likewise constant. Making risk management rules and procedures is done mostly to make sure that acceptable behavior is regularly shown. One of the main goals of a risk management strategy is to ensure continuous desired behaviors. Although competent or desired behaviors are successfully attained in the normalized organization, they have not yet become automatic. The competent or desired behaviors will become unconscious or automatic when the company reaches the point where risk management comes naturally. The four levels of risk maturity (Ns) are represented by this model, which also shows that for businesses that do not make enough effort to maintain their level of risk maturity, the drop from natural behavior back to naive may be a little step [8].

CONCLUSION

There are several techniques to measuring risk maturity, such as the Criteria of Control (CoCo) framework. The CoCo framework's strategy places a strong emphasis on the value of risk maturity. This internal control framework takes the stance that excellent levels of risk management and internal control may be attained if the risk culture, risk architecture, strategy,

and procedures are proper. The European Foundation for Quality Management (EFQM) model is another often used risk maturity framework. Overall, the paper emphasizes the critical role of a risk-aware culture in the success of risk management efforts. It highlights the need for organizations to invest in promoting a culture of risk awareness and to foster a workplace environment where employees are empowered to identify and manage potential risks effectively.

REFERENCES:

[1] B. Minguez Garcia, "Resilient cultural heritage: from global to national levels – the case of Bhutan," *Disaster Prev. Manag. An Int. J.*, 2020, doi: 10.1108/DPM-08-2018-0285.

[2] J. K. C. Chen and D. Zorigt, "Managing occupational health and safety in the mining industry," *J. Bus. Res.*, 2013, doi: 10.1016/j.jbusres.2012.04.013.

[3] R. Köhler, C. Lambert, and H. K. Biesalski, "Animal-based food taboos during pregnancy and the postpartum period of Southeast Asian women – A review of literature," *Food Research International*. 2019. doi: 10.1016/j.foodres.2018.10.026.

[4] R. L. Jenkins, "Ensuring access to education and services on infertility for the underserved.," *Journal of the National Cancer Institute. Monographs*. 2005. doi: 10.1093/jncimonographs/lgi016.

[5] R. Ramphal, "Overview of the new ISO 9001:2015 standard and challenges ahead," *African J. Hosp. Tour. Leis.*, 2015.

[6] T. El-Toukhy, Y. Khalaf, and P. Braude, "IVF results: Optimize not maximize," *American Journal of Obstetrics and Gynecology*. 2006. doi: 10.1016/j.ajog.2005.05.018.

[7] A. Alaszewski and K. Coxon, "The everyday experience of living with risk and uncertainty," *Health, Risk and Society*. 2008. doi: 10.1080/13698570802383952.

[8] P. M. Davidson, J. Daly, K. Hancock, and D. Jackson, "Australian women and heart disease: trends, epidemiological perspectives and the need for a culturally competent research agenda.," *Contemporary nurse : a journal for the Australian nursing profession*. 2004. doi: 10.5172/conu.16.1-2.62.

CHAPTER 23

IMPORTANCE OF RISK APPETITE IN RISK MANAGEMENT

Manjula Jain, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-jainmanjula776@gmail.com

ABSTRACT:

Risk appetite is the level of risk that an organization is willing to accept in pursuit of its objectives. It is an essential concept in risk management because it helps organizations make informed decisions about the level of risk they are willing to take on to achieve their goals. This paper provides an overview of the importance of risk appetite in risk management. It explores how risk appetite helps organizations set boundaries for risk-taking and make informed decisions about risk management strategies. The paper identifies the key benefits of having a clear risk appetite, including improved decision-making, better risk management, and increased stakeholder confidence. It also explores the factors that influence risk appetite, such as the organization's culture, values, and risk tolerance.

KEYWORDS:

Business, Mitigation, Magnitude, Risk Appetite, Risk Management, Organizations.

INTRODUCTION

In the practice of risk management, the idea of risk appetite is very significant. It is, nevertheless, incredibly difficult to accurately describe and execute in reality. Some people believe that a person's risk tolerance is determined by the risk standards set by the organization. In the risk ranking stage of the risk management process, the risk appetite or risk criteria are crucial elements. This comes after the risks have been appraised according to probability and impact in the risk management process. Risk appetite is the organization's willingness to engage in a risky activity now or in the near future. Similar to how a person would have an instant hunger for food and a longer-term attitude towards food, risk attitude and the risk criteria imply a longer-term perception of risk.

One of the key issues with the idea of risk appetite is that companies often have an appetite to go on with a certain operation, start a project, or adopt a strategy rather than an appetite for the risk directly. In other words, rather than being a factor in driving business choices, risk exposure and appetite should be seen as a consequence of those actions. The choice about risk appetite is often made in conjunction with other business decisions rather than on its own. Risk management guidelines generally advise against managing risk in isolation, therefore inquiries regarding risk

appetite may only be addressed in the context of the strategy, tactics, operations, and compliance activities under consideration. While many businesses are profitable enough, they often take on too much risk or improperly use their risk capacity. The ability of an organization to accept risks, or its risk capacity, differs from the sum of all the individual values at risk connected to the hazards to which it is exposed. The organization's risk exposure is represented by this cumulative amount.

Risk appetite, in contrast, is the entire amount of corporate resources that the organization's board is prepared to put at risk. Most businesses have not assessed their risk appetite (the amount of value they should be willing to take on), their risk exposure (the amount of value really at risk), or their risk capacity (the amount of risk they are willing to take on). a variety of risk appetite definitions. It is evident that the definitions of risk appetite given by various professional organisations are quite similar. Based on its attitude toward risk, a business should be able to select how much it wants to put at risk. By deciding on a risk tolerance, the business may avoid putting too much (or too little) value at risk. To guarantee that risk taking is at the ideal level and yields the most profit, the organization's risk capacity must be properly used. Similarly, given the industry in which it works and the current state of the market, the organization shouldn't put more value at risk than is necessary.

The organization's willingness to invest in opportunities may be determined by the share of risk appetite that is connected with such prospects. Resources will be invested by organizations on opportunities that they feel will result in a profit. The company should be aware that risking assets in this manner could not result in a benefit, however. Losses might occur if strategic choices are put into action. In fact, poor strategy choices have a greater potential to reduce value than hazards, controls, or even compliance concerns. The business may be eager to spend a certain amount of money in a potential opportunity, but it must be certain that it is able to withstand any potential losses. Additionally, it must ensure that the overall amount spent, or value at risk, does not exceed the organization's capabilities. It is important to carefully identify the types of hazards and calculate the real risk exposure related to the opportunity.

The risk matrix and risk appetite

The ideas of risk exposure, risk capacity, and risk appetite. The risk matrix uses colored squares to represent risk appetite, and a curving line represents the organization's overall exposure to risk. For a risk-averse firm, this picture shows risk appetite, exposure, and capability. An instance when the organization is okay with taking a risk is represented by the medium-shaded region. The lighter regions stand for the reserved and wary zones, where management discretion is needed before accepting the risk. The serious risks indicated by the darkest area are the only ones that will be acknowledged when a business requirement exists [1].

Optimal Risk Tolerance, Exposure, and Capability

This is the ideal point, where the entire exposure cuts through the lighter region, for the organization's overall risk exposure. The organization's risk capacity is well-integrated inside the darker area and is proven to be greater than both risk appetite and risk exposure. This is the ideal situation to be in. This guarantees that the company is not taking on more risk than its maximum

risk tolerance and that the risks it is taking are within the board's appetite. In the s, total cost of risk estimates were routine, and the goal was to determine the overall risk exposure. Organizations or their insurance agents often carried out these computations. They made it possible for an organization to calculate the overall cost of risk from hazards. The three key factors in the computation were the cost of uninsured claims, the cost of loss-control measures, and the insurance premium.

The total cost of risk in different organizations was published in tables, and it was feasible to compare an organization's performance to that of other businesses operating in the same industry. This kind of total cost of risk analysis was helpful and often used to support the creation of an internal or captive insurance firm. This sort of computation presented a challenge since it was heavily reliant on past data. Historical loss information is not always a reliable indicator of future loss performance. This strategy was designed to encourage businesses to handle hazard risks at the lowest possible cost overall. Unfortunately, when a significant event happened, this lowest-cost method often proved to be a mistake. Organizations should be mindful that the lowest cost for managing hazard risks may be represented by the total cost of risk calculation, but it might be at the expense of a high overall risk position. It is important to keep in mind that buying too much insurance could put an organization in the lowest risk situation, but at a high total cost.

Organizations currently use a somewhat different method for calculating the overall cost of risk. The idea of risk appetite is often used by organizations to do calculations that determine the degree of risk that the company is prepared to bear. The board's risk appetite may then be compared to the actual risk exposure the firm is exposed to. An updated version of the total cost of risk calculation, the real risk exposure in this calculation should take into account all forms of hazards, not only those that can be insured. In general, the organization will have to raise its risk exposure as the market gets more unstable. This calls for a board-room debate that results in an agreement to raise the overall value that the business is prepared to put at risk and/or identify strategies to lower overall risk exposure. As a result, risk management is especially crucial during periods of fast change and elevated market volatility. A company's decision to pursue a merger or acquisition will also expose it to more risk. All acquisition prospects must be analyzed by organizations, and this analysis must take into account at least the following characteristics of the acquisition opportunity:

1. The acquisition's reputation and financial standing.
2. Possibility of generating more income or profit from the purchase.
3. Risks related to the terms and circumstances of the recommended purchase contract.
4. The proposed acquisition's expected profitability and durability.
5. Investment necessary to carry out the acquisitions expected future ambitions.
6. The effect on current investment and corporate expansion plans.

The real cumulative amount at risk is known as risk exposure, however it is often determined risk per risk without taking into account whether the risks are interrelated. A company must take into consideration the possibility of the risks materializing by allowing for the correlation of hazards. It is crucial to alter the cumulative total of the values at risk in order to account for

whether or not hazards are connected when determining the organization's overall real risk exposure.

Risk and Ambiguity

The variety of results for various risk exposures. With regard to opportunity investment, a variety of results are conceivable, from a total loss of the resources invested to a sizable return. If the overall negative risk exposure connected with the investment is not accurately evaluated, the losses sometimes may be more than the original investment. how risk and uncertainty are related. It shows the normal range of outcomes for opportunity, control, and hazard risks. It is feasible to show how the three forms of risk are connected, interdependent, and create a continuum by presenting all three in a single graphic. The entire amount of risk that the organization is willing to take will be represented by the sum of all of its hazard exposures, control acceptances, and opportunity investments.

The range of potential outcomes for each risk position, with a probability of occurring outside that range or with a certainty of 1%. An organization may determine that it has the risk tolerance to accept the hazard risk shown at point A. The risk appetite for that particular form of hazard risk is shown by the risk appetite point A. When deciding on a risk appetite, the company will be aware that a variety of outcomes are conceivable. The lines representing the percent certainty represent that range of possibilities [2].

Similar to point A, the organization will have a hunger to seize an opportunity. Again, there are a variety of outcomes that might occur with this potential investment. The desired result is a positive return, but if the investment is unsuccessful, a loss might result. The percent confidence lines illustrate the range of potential outcomes. is used to show how putting a value at risk may result in a variety of consequences. A variety of dangers that may destabilize organizations exist. These are the risk factors for hazards that have been covered in this book that result in a risk exposure for the organization. In other words, as part of routine business activities, the company will be prepared to tolerate exposure to certain hazard risks. The quantity and kind of risk that a business is willing to seek or maintain is described as risk appetite by Guide.

Hazard risks will be expensive, both in terms of the cost of occurrences that do happen as well as the cost of loss-prevention, damage-limitation, and cost-containment measures, such as insurance premiums. There will be a variety of potential outcomes, all of which are adverse, for each risk of danger. The company will need to estimate the costs and hazards connected with any potential hazards. It should be able to determine the level of hazard risk it is willing to accept; this is a component of its overall risk tolerance. The company may choose the level of risk that it is willing to accept, but the real exposure to risk may be more than expected. Many hazard risks are controlled by law, and as a result, enterprises must deal with the compliance risks connected to those regulated hazards. The majority of corporations often have a zero-risk tolerance for breaking the law.

All companies must also deal with uncertainty and the control risks that cause them. These are dangers associated with potential occurrences whose results are undetermined. An example of a control risk is the fact that removing all fraud measures from a company would result in a net

savings equal to the cost of the controls. However, it would be unclear how much fraud would really arise from the absence of all safeguards, even while it was possible that fraudulent behavior would occur and significant losses may be incurred. The initiatives that the company is now working on will include control hazards. The price of essential controls could be covered by the project's total budget. It would be foolish to leave the cost of required controls out of the project budget when designing a big project. The project budget's allocation for the cost of the controls reflects the organization's adoption of controls.

DISCUSSION

Risk Capacity and Exposure

The zones of caution and worry are more condensed, and the darkest zone makes up even less of the total matrix. One way to define this circumstance is as an extremely constrained risk universe approach. The darkest squares indicate the company's whole risk universe, and it is only in this region that the board of the organization will deem the risks to be considerable. Simply because it takes risk more aggressively, it has a higher risk appetite. The company will have less risks in the crucial zone if it takes a more active stance toward risk. In this scenario, the board of the organization's "universe of risk" will be highly constrained. The hazards that will be taken into account at the board level are represented by the universe of risk. Before a risk attracts boardroom attention, its probability and effect must be very high.

The lighter-shaded zones represent the organization's maximum risk-bearing capability. This is a scenario in which the organization can be incurring risks that are greater than its maximum risk tolerance. To make matters worse, the organization's real risk exposure is also shown inside the darkest region. As a result, the company is exposed to risk to a far greater extent than its maximum level of risk-taking capability. It takes discretion to determine the organization's risk appetite, and this discretion may be used at various organizational levels. At the board level, taking one's risk tolerance into account will be a strategic driver. Since line managers are expected to work within the board-established risk appetite policy, risk appetite is likely to constitute a limitation on operations at the level of line managers [3].

Consideration of risk appetite will probably be a behavior regulation at the individual level. This is so that each employee may only work within the framework for evaluating risk that has been defined at the board level and put into place by line managers. For risk management professionals, it is still quite difficult to define and use the idea of risk appetite. Organizations should identify their risk appetite early on, according to a number of existing risk management standards and those that are being developed. Although ISO does not use the term "risk appetite" specifically, it does recommend that an organization create the risk criteria as soon as possible.

This seems to go against a fundamental principle of risk management, according to which hazards shouldn't be addressed out of context. Just as risks shouldn't be handled outside of context, it makes no sense and is probably impossible to identify risk appetite outside of context. The organization's strategy, tactics, regular operations, and fundamental compliance procedures must all be taken into consideration when determining the organization's risk appetite. Without a doubt, the subject of risk appetite will get greater attention in the future, and risk management

professionals need to comprehend this idea and its applications better. The study's riskiness index follows a somewhat different methodology[4], [5].

Like people, organizations do not purposefully seek danger. Although someone may be labeled as a risk-taker, the truth is that they really like engaging in high-risk activities. In the beginning, the action itself, not the danger itself, is what draws the person. People who engage in high-risk hobbies or pastimes may be labeled as risk takers. This does not imply that the person will continue to take risks, such as crossing a busy street without looking. To put it another way, taking risks must be understood in the context of the activity and the desired benefits. Organizations are similar in that the strategy, initiative, or activity not the actual risk is what appeals to the board. A company could choose a risky strategy, authorize a dangerous project, or carry out hazardous operations or basic procedures. Board members, however, are more concerned with the business imperatives and drives than the degree of risk involved. Instead of the risk appetite determining the strategy, it is more common for the amount of risk to come together with the established plan.

Risk Appetite Declarations

The idea that an appetite will often connect to a variety of potential outcomes is one of the additional characteristics linked to the risk appetite. As a result, there will be a certain zone of risk exposure or degree of risk that falls within appetite surrounding the risk appetite. The risk tolerance range for exposure to that specific danger may be referred to as this. The permissible degree of variance in relation to achieving a certain goal, which is often best assessed using the same units as the goal-related goal. Management balances risk appetite with risk tolerance by taking into account the proportional relevance of the relevant aim. Operating under risk tolerances makes it more likely that the entity will stay within its risk appetite and, as a result, accomplish its goals.

It should be highlighted that three main factors contribute to the form of risk appetite. The strategy of certain firms may be influenced by their risk appetite. Organizations like banks and other financial entities would fall under this category. The desire of an organization to, for example, lend money to certain firms or groups of individuals will be a reflection of its risk appetite and will be the primary engine of its business. Risk is at the core of the banking industry. The firm will want to take on risk if risk appetite is a driving force behind the business in order to reap the rewards. Risk is not a business driver for many firms; rather, it results from the strategy, tactics, operations, and compliance fundamental procedures that the company uses. In this situation, risk appetite is unlikely to be the driving force behind the company; rather, it will serve as a planning tool for the organization to choose if it wants to embrace certain strategies in light of the risks associated with such strategies, initiatives, or changes. An company will want to operate within certain tolerance levels and manage the uncertainty associated with risk when utilizing risk appetite as a planning tool [6].

In other cases, risk appetite may simply be a reflection of the restrictions imposed on employees by the firm. Within an organization, a Delegation of Authority is often used to create authorization thresholds, spending caps, and other restrictions. The organization's risk appetite

may clearly be seen in the levels of authority. Due to the magnitude, complexity, and exposure to risk in these situations, the company will want to establish limitations that define its risk appetite before mitigating or minimizing the risk exposure, as well as any potential effect and repercussions. Simply put, if risk management is about eliminating uncertainty and attaining the best possible result, then risk appetite is about determining the ideal degree of risk that will provide the best possible result. The organization's risk attitude, risk criteria, and willingness to accept risks are all reflected in the organization's risk appetite. Risk appetite may be a strategy-determining factor, a planning tool for tactics, or a set of operational restrictions. Without being clear on whether risk is a driver, planning guide, or set of operating limits, many businesses have tried to create risk appetite statements. The intricacy of each strategy will be reflected in the risk appetite statement if all three are used. A collection of risk tolerance declarations that could be in force at a university or other educational institution. The institution takes opportunities that come with a high risk of failure that might harm its reputation, expose it to financial loss or exposure, cause serious IT system failure, result in substantial instances of regulatory non-compliance, or place employees and students at serious danger of harm [7].

The organization's risk categorization system should logically be in line with the structure of the risk appetite declarations. Risk sources, organizational parts that might be impacted by a risk event, and/or impact or consequence categories, such as the FIRM risk scorecard, or the organization's strategy, tactics, operations, and compliance (STOC), are all possible structures for risk appetite statements. The Network Rail risk appetite statement is organized similarly to the FIRM risk scorecard, as seen in the summary below. A manufacturing organization's risk appetite statement is an example of how risk appetite statements may be designed to represent the bow-tie approach to risk management.

Risk Tolerance and Lifestyle Choices

An individual's risk appetite and lifestyle choices are related. Determinations will be made on, for instance, long-term health problems based on personal lifestyle choices and family history. Additionally, decisions on short- and long-term health will be made depending on medical care, diets, and weight growth. Short-term choices will also need to be made about matters of health, such as those pertaining to exercise, alcohol, recent sickness or accidents, and recent health difficulties. Based on their risk attitude, appetite for risk, exposure to risk, and capacity for risk, people will need to make lifestyle choices. Decisions on the amount of exercise a person is prepared to do in the near term to keep their weight within a healthy range must be made in relation to health problems. A person may have a specific appetite for risk factors related to their health and well-being, but the exposure that they actually experience may be more than their hunger. People are eager to use cigarettes, for instance, but they also want to live better lifestyles. In this case, the risk appetite may not match the level of real risk exposure.

When the consequence is immediate, favorable, and definite, individuals have a predisposition to respond in a specific way. The quick, favorable, and definite effects of nicotine will make a smoker desire to smoke. Contrarily, quitting smoking will likely have long-term benefits, albeit they may take time to manifest and are unpredictable. Additionally, there will be unpleasant withdrawal symptoms. Depending on the sort of risk being examined, people's attitudes about

taking risks might differ greatly. For instance, people could drive their automobiles with extreme caution yet take substantial risks when it comes to their health. It's possible that risk appetite statements for people are just as challenging to create as those for corporations in terms of the risks they are prepared to face. A properly defined risk attitude would in both situations serve to define the appetite for a variety of risk elements[8], [9].

CONCLUSION

The kind of risk involved and the capacity to implement efficient controls will both affect people's willingness to accept risks. Describes some of the cost-effective controls that can be put in place to minimize risks, manage uncertainties, and seize opportunities; the particular compliance requirements, risks, and opportunities related to these things. In general, a person's risk attitude and risk appetite will be shown by the amount of money they are ready to spend on financing a control. In terms of strategy, tactics, operations, and compliance (STOC), this real-world example illustrates a portion of the embrace, manage, mitigate, and minimize (EM) approach. Moreover, the paper emphasizes the need for organizations to establish a risk appetite framework that is aligned with their overall strategy and objectives. It highlights the importance of involving key stakeholders in the development of the risk appetite framework and regularly reviewing and updating it to ensure it remains relevant and effective. Overall, the paper emphasizes the critical role of risk appetite in the success of risk management efforts. It highlights the need for organizations to establish a clear and effective risk appetite framework that guides their risk-taking decisions and helps them achieve their objectives while minimizing the impact of potential risks.

REFERENCES:

[1] W. Gontarek, “Risk governance of financial institutions : The growing importance of risk appetite and culture,” *J. Risk Manag. Financ. Institutions*, 2016.

[2] S. Takehara *et al.*, “Appetite, oral health and weight loss in community-dwelling older men: an observational study from the Concord Health and Ageing in Men Project (CHAMP),” *BMC Geriatr.*, 2021, doi: 10.1186/s12877-021-02169-y.

[3] H. Dincer and S. Yuksel, “IT2-Based Fuzzy Hybrid Decision Making Approach to Soft Computing,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2895359.

[4] P. Willumsen, J. Oehmen, V. Stingl, and J. Geraldi, “Value creation through project risk management,” *Int. J. Proj. Manag.*, 2019, doi: 10.1016/j.ijproman.2019.01.007.

[5] G. O. Danisman and P. Demirel, “Corporate risk management practices and firm value in an emerging market: a mixed methods approach,” *Risk Manag.*, 2019, doi: 10.1057/s41283-018-0040-5.

[6] M. E. J. Lean and D. Malkova, “Altered gut and adipose tissue hormones in overweight and obese individuals: Cause or consequence,” *International Journal of Obesity*. 2016. doi: 10.1038/ijo.2015.220.

[7] S. Steinsbekk, D. Belsky, I. C. Guzey, J. Wardle, and L. Wichstrom, "Polygenic risk, appetite traits, andweight gain in middle childhood a longitudinal study," *JAMA Pediatr.*, 2016, doi: 10.1001/jamapediatrics.2015.4472.

[8] K. Buganová and J. Šimíčková, "Risk management in traditional and agile project management," in *Transportation Research Procedia*, 2019. doi: 10.1016/j.trpro.2019.07.138.

[9] R. L. Kumar and S. Park, "A Portfolio Approach to Supply Chain Risk Management," *Decis. Sci.*, 2019, doi: 10.1111/deci.12332.

CHAPTER 24

A FUNDAMENTAL OF RISK TRAINING AND COMMUNICATION

Mohit Rastogi, Associate Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-rtmohit@yahoo.co.in

ABSTRACT:

Effective risk management requires a comprehensive approach that includes training and communication. Training ensures that employees understand the organization's risk management framework and their role in mitigating risks. Communication, on the other hand, ensures that employees are aware of new risks and changes in the risk environment. This paper provides an overview of the fundamental principles of risk training and communication. It highlights the importance of effective training in building a culture of risk management and promoting accountability across the organization. The paper also explores the role of communication in ensuring that employees are aware of new risks and changes in the risk environment.

KEYWORDS:

Business, Environment, Mitigation, Magnitude, Risk Appetite, Risk Management.

INTRODUCTION

To guarantee that a consistent reaction to comparable risk occurrences is always accomplished, risk information dissemination and risk training are important. The only way to guarantee this is to share knowledge and expertise. Concerning the hazards of danger, control, and opportunity, a consistent approach is necessary. When a business has an intranet, this is the best strategy to ensure that the right information is accessible and to achieve a consistent reaction to risk. Consistent risk processes must also be created and communicated, in addition to a consistent reaction to specific risks. Identifying risks in advance and confirming the controls that will be in place for them are important steps in maintaining a consistent response. This strategy is applicable to operational, project, and strategic risks, and training and communication procedures should be put in place to improve consistency in how the company responds to risk.

Each request for capital expenditures should be accompanied with a risk assessment, which should be a requirement for every business. The risks that the project is attempting to manage as well as internal project hazards should both be included in this risk assessment. The project's hazards might make it more difficult to complete it on schedule, within budget, and according to specifications. Strategic analysis's integration of risk assessment is a crucial component of establishing a consistent approach to risk. It may also be beneficial to create a "issues manual" to communicate risk across the firm and guarantee a uniform reaction to hazards. The hazards, situations, and other occurrences that call for a reaction will be included in the problems handbook. Consistent and suitable risk management processes will be more likely to be followed if enough information, supervision, and training are provided.

When a new risk arises or an old risk significantly changes, it is crucial to examine the requirement for consistent responses to risk. In these situations, risk escalation may be necessary so that top management may assess the altered conditions. It is necessary to create and implement reliable risk escalation processes and to offer the necessary training for these procedures. In a crisis, a consistent approach to risk management is crucial. Training for directors, managers, and employees is crucial once an organization has created a disaster recovery strategy. Additionally, all those who could be impacted by the business continuity plan's obligations must be informed of them. Once again, training is crucial to ensuring a consistent reaction to challenging conditions.

DISCUSSION

LILAC stands for leadership, engagement, learning, accountability, and communication, and it may be used to describe the risk culture of a business. The LILAC categories also provide an idea of what makes an effort to integrate risk management within the company effective. The risk-aware culture's engagement, learning, account-ability, and communication elements are all very pertinent to risk training and risk communication. Managers and employees will have access to accurate risk management documents that will outline the degree of participation and responsibility that the business expects. Adequate risk training may provide a high level of learning and communication, which will improve the organization's risk-aware culture [1].

Take a publisher who is exposed to libel and slander risks as an example. The business should draft risk policies, protocols, and procedures that mention training for all employees on risk awareness. Libel and slander risk management plans should be comprehensive and take into account the degree of exposure to risk. Each magazine title will determine how much attention is given to such dangers, but the following structure could be suitable: The introduction of specific review processes for political titles; the fundamental libel and slander training for all journalists; and the legal assessment of each issue of a satirical magazine.

The updated processes must be trained on for the workforce, and information should be posted on the corporate intranet. It is important to encourage managers and employees to provide feedback on the new processes so that they may be further enhanced as part of the company's learning culture. For managers, employees, and other stakeholders to be engaged, risk training is a critical component of learning and communication. In addition to giving information on the control mechanisms that are in place and the crucial role played by employees in the effective application of these controls, it should cover a broad variety of subjects and obtain a deeper awareness of all the risk-related concerns. Ongoing training in risk management is necessary. Gives some instances in which risk management training could be especially pertinent or required.

A excellent example of a training program with clearly stated training goals is the following excerpt from the risk management handbook of the United Nations Educational, Scientific, and Cultural Organization (UNESCO): The goal of risk management training is to increase participants' fundamental understanding of risk management ideas and methods, to empower them to recognize and manage risks in their own units, and to improve project management via

sufficient risk planning in advance. The half-day risk management training module presents the concept of risk, explains its goal, and goes through the procedures that may be taken to effectively manage risks. The training covers topics including corporate culture, decision-making, and situational awareness in addition to providing general skills.

Information And Communication About Risks

The necessity of risk communication and information is taken into account by a US COSO ERM framework component. The first step in risk communication is identifying the parties having an interest in the specific risk being discussed. After the stakeholders have been identified, a decision must be made about the kind of risk information that has to be shared. Finally, it is important to evaluate the motivation for sharing risk information with each set of stakeholders. Risk communication should be given against the backdrop of stakeholders' preexisting perceptions of hazards as they will already have such perceptions. the regulations pertaining to risk communication. These recommendations aim to set norms for informing various stakeholders about risk problems. These guidelines undoubtedly become more significant when risk is discussed with other entities. Nevertheless, they provide a helpful set of recommendations for communicating risks to internal and external stakeholders. There are further justifications for sharing risk information with internal stakeholders. The company will typically anticipate that managers and employees will contribute to the management of the risk in the future, although this may not always be the case for external stakeholders [2].

The organization's other training initiatives should be in line with the delivery of risk training. The training's content must be in line with the demands of the profession, just as it is with all other sorts of training. In a variety of situations, such as when new risks have emerged or current risks have drastically altered, training on risk topics will be necessary. A new job or more responsibility will also need training for the person. After an event and the implementation of new or improved processes, risk training will be even more crucial. Making sure there are adequate arrangements for "whistleblowers" is a crucial part of risk information and communication; despite the fact that employees and other parties may gather information about a company that is normally kept private, there needs to be a system in place that allows staff and other stakeholders to voice concerns if they have good reason to believe serious malpractice has occurred. An excerpt from the University of Cambridge's whistleblower policy is provided in the text box below.

The creation of a unified language of risk is essential to effective risk communication. The terminology used in this book's vocabulary and the meanings used in the ISO Guide, which lists terms linked to risk management that are globally recognized, are both included in Appendix B. To account for elements that could be special and exclusive to an organization, it is sometimes essential for it to create its own risk lexicon. Arguments regarding the exact meaning of a phrase to various risk management practitioners are less significant than a shared concept of risk based on terminology usage inside the company. In fact, it could be acceptable for the risk manager to adopt the language currently in use in an organization as part of coordinating risk management efforts and incorporating risk concerns into everyday operations. Even if the organization's

terminology clashes with rigid risk management requirements, using the established terminology will improve communication [3].

A common language has been used in this work to help with the introduction and clarification of topics related to risk management. This language sometimes deviates from the ISO Guide, however it has been utilized to improve comprehension and communication. Compromise is often necessary when discussing the creation of a risk vocabulary and agreeing upon terminology. To ensure that everyone participating in a debate has a shared knowledge of the terminology being used, it is crucial to establish a common vocabulary and agreed-upon definitions. The synopsis in the box below serves as an example of this.

On An Intranet, Risk Data

Stakeholders may get risk information in a number of ways. To explain the current risk risks and concerns to stakeholders, several organizations create concise guides and booklets. Depending on the kind of stakeholder, as well as the nature and complexity of the message to be delivered, a different method of communication will be most effective. There are formal channels for communicating risks if the company is required to update financial stakeholders. A variety of communication approaches may be employed when risk communication is necessary. An casual video, PowerPoint presentation, and/or telephone conference call may support a formal report to the stock market or to other financial stakeholders, as necessary.

Organizations often have access to extra risk communication tools. A lot of firms have created an intranet for employee usage, and this may be utilized to include information on risk and risk management. It is typical for the intranet to be used by many major firms to disseminate business continuity plans and information on health and safety. The general risk assessments that have been conducted and the control measures that have been established may both be disclosed on the intranet. As well as giving updates on risk assessments, management strategies, and the current severity of any given risk, the intranet may be used to transmit important risk information. The alignment of risk information with other management information systems inside the firm is a crucial factor to take into account when it comes to its collection, storage, and delivery. Risk management efforts may fail to be aligned with or integrated into other activities if risk information is provided as a distinct management information stream. When an organization has a specialized risk management information system (RMIS), there is a larger risk that risk information may lose its relevance to managers [4], [5].

Risk management information systems (RMIs) A risk management information system (RMIS) software package may be used to disseminate risk management guidelines, protocols, and processes. The organization's intranet might house the RMIS. The RMIS will make it easier to gather and share risk data, as well as enable local management to report occurrences as they happen. The RMIS often contains a broad variety of data. RMIS have been used for a while to keep track of insurance claim information. The utilization of an RMIS has evolved during the last several years. Using such a software package, it is now able to keep track of specifics about risk exposure, risk management, and risk action plans. Details of insurance policies, insurance claims processes, and insurance claims history may all be recorded and made accessible to

authorized personnel for RMIS that are utilized in conjunction with insurance. A system like this may also be used to gather data on risk exposure and record accidents or other occurrences that can result in an insurance claim. A variety of software solutions, in addition to RMIS systems that record information, enable risk management. These include systems that can do risk analysis and dependency-modeling evaluations as well as software programs that can carry out a variety of analytical tasks [6], [7].

The paper identifies the key elements of an effective risk training program, including clear objectives, relevant content, and interactive delivery methods. It also explores the importance of ongoing training and the need to tailor training programs to the specific needs of different employee groups. Moreover, the paper emphasizes the importance of clear and timely communication in risk management. It highlights the need for organizations to establish effective communication channels and to ensure that employees receive regular updates on new risks and changes in the risk environment [8].

CONCLUSION

It is well acknowledged that using an RMIS software package in conjunction with an enterprise risk management (ERM) program may be highly beneficial. The drawback, however, is that it might take a lot of time to input a significant quantity of risk data into a computer database. The advantages of having the data accessible for thorough examination, however, may make the effort worthwhile. In order to increase risk awareness and assure enhanced risk performance, risk information has to be communicated throughout the business. People that work for an organization nearly usually have the finest grasp of the risks and the most in-depth practical knowledge of the steps that need be done to minimize risk occurrences. Sharing information regarding events that have happened, including the lessons that have been learned and the steps that have been taken to ensure that the occurrence is not repeated, requires communication. The box below contains an examination of RMIS's benefits and drawbacks. Generally speaking, when risks are complicated or there is a significant quantity of data that has to be captured, an RMIS becomes more beneficial. Overall, the paper emphasizes the critical role of risk training and communication in the success of risk management efforts. It highlights the need for organizations to invest in developing effective training programs and communication channels and to foster a culture of continuous learning and improvement in this field.

REFERENCES:

[1] C. J. Gidlow *et al.*, “Cardiovascular disease risk communication in NHS Health Checks: A qualitative video-stimulated recall interview study with practitioners,” *BJGP Open*, 2021, doi: 10.3399/BJGPO.2021.0049.

[2] B. Momand and A. Dubrowski, “Addressing Social Context in Health Provider and Senior Communication Training: What Can We Learn From Communication Accommodation Theory?,” *Cureus*, 2020, doi: 10.7759/cureus.12247.

[3] L. Birch *et al.*, “Obstetric skills drills: Evaluation of teaching methods,” *Nurse Educ. Today*, 2007, doi: 10.1016/j.nedt.2007.01.006.

[4] A. Al Thobaity, V. Plummer, and B. Williams, "What are the most common domains of the core competencies of disaster nursing? A scoping review," *International Emergency Nursing*. 2017. doi: 10.1016/j.ienj.2016.10.003.

[5] R. Mangifesta, F. Marino, and L. Di Giampaolo, "Risk perception in construction sites in the Covid-era," *J. Biol. Regul. Homeost. Agents*, 2021.

[6] J. A. Pattinson, H. Chen, and S. Basu, "Legal issues in automated vehicles: critically considering the potential role of consent and interactive digital interfaces," *Humanit. Soc. Sci. Commun.*, 2020, doi: 10.1057/s41599-020-00644-2.

[7] Y. Leung, J. Oates, and S. P. Chan, "Voice, articulation, and prosody contribute to listener perceptions of speaker gender: A systematic review and meta-analysis," *Journal of Speech, Language, and Hearing Research*. 2018. doi: 10.1044/2017_JSLHR-S-17-0067.

[8] C. J. Gidlow *et al.*, "Cardiovascular disease risk communication in nhs health checks using qrisk® 2 and jbs3 risk calculators: The rico qualitative and quantitative study," *Health Technol. Assess. (Rockv).*, 2021, doi: 10.3310/hta25500.

CHAPTER 25

A DISCUSSION ON RISK PRACTITIONER COMPETENCIES

Vibhor Jain, Associate Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-vibhorjain7@gmail.com

ABSTRACT:

Risk management is an essential function for any organization, and it requires a skilled workforce to identify, assess, and mitigate risks effectively. Risk practitioners play a crucial role in this process, and their competencies are critical to the success of risk management efforts. This paper provides an overview of risk practitioner competencies, highlighting the key skills, knowledge, and abilities required to excel in this field. It explores the various competencies needed at different levels of risk management, from entry-level positions to senior leadership roles.

KEYWORDS:

Business, Environment, Mitigation, Practitioner Competencies, Risk Appetite, Risk Management.

INTRODUCTION

More and more, risk management is seen as a profession rather than a collection of tasks. A set of skills must be defined for every profession in order to specify the behaviors that practitioners in that area must exhibit. Although competence frameworks come in a variety of forms and formats, the most are based on the phases that are engaged in the practice of the profession. The degrees of proficiency necessary at various levels of seniority are then outlined after identifying the steps involved in the profession. It is widely acknowledged that persons working in any profession must possess a combination of a variety of interpersonal or soft skills in addition to the technical or hard abilities needed to succeed in the field. In other words, in order to effectively help an organization with the design and implementation of a risk management framework, the risk practitioner requires more than just technical expertise.

A risk practitioner has to be proficient in two technical areas. The practitioner must first and foremost be competent in a variety of risk management concerns and actions. Additionally, in order to comprehend the external and internal contexts in which the firm functions, he or she will require a variety of business abilities. If the risk management practitioner is to effectively establish an adequate risk management process and supporting risk management framework or internal context, they must have a solid grasp of business and the development of relevant business skills. The development of business skills is not the emphasis of this textbook, thus the technical risk management abilities that the risk practitioner will need are given more attention. According to an overview of the risk management technical skills that will be necessary for a

successful risk management practitioner, these risk management technical skills will be closely connected with the phases in the execution of a risk management project.

Array of Abilities

A good risk management practitioner must possess both people, interpersonal, or soft skills as well as technical or hard abilities. Technical skills may be further broken down into business and risk management technical abilities. A competence framework for risk management technical abilities may be established. Depending on the sort of company, different business abilities will be needed. They will typically consist of knowledge in the areas of information technology, operations, marketing, human resources, finance, and accounting [1].

With the evolution of organizational communication, the value of people skills has grown significantly. Soft skills are another name for people skills. Technical expertise is often seen to be connected to intellectual intelligence, while soft expertise, or people skills, is connected to emotional intelligence. The risk practitioner requires both forms of intelligence and both sets of skills in order to be effective. The effective risk manager will need the abilities related to self-management and self-development in addition to technical and interpersonal capabilities. These are often the abilities that are required of all technical workers, and they are frequently supported by adherence to a code of ethics or behavior. Activities that improve abilities and potential are included in self-development, as are those that improve work satisfaction and future employability. Self-development also include helping others, which may entail serving as a teacher, mentor, trainer, or professional coach, among other things. The variety of interpersonal skills needed in a corporate setting. These abilities fall under the CRAM skill category (communication, relational, analytical, and management). Technical skills may be learned via a mix of instruction and experience, while interpersonal skills depend a great deal more on the personality of the person. Therefore, it presents a bigger challenge for risk practitioners to develop the variety of interpersonal skills necessary for success.

Talents in Communication

It is crucial to communicate risk problems accurately. Through the risk architecture, internal communication inside the company will be carried out. This is the official framework for communicating risks connected to risk management operations and data gathering for external risk reporting. For instance, a road haulage firm could want to emphasize the organization's effective operation and make sure risk management gets the proper attention. In these situations, the business could choose to use a variety of quantifiable loss-control programs. Every board meeting, the company's board has asked for a report on the number of traffic accidents, the frequency of vehicle breakdowns, the amount of gasoline used, and any reported issues during deliveries. With the use of these reports, the board will be able to measure the company's performance against both its rivals and its own past performance data. In this instance, the board is in charge of performance evaluation, although line management is still in charge of managing the enhanced risk performance. Risk communication may also be more casual inside other businesses. There will be communication throughout risk assessment workshops and risk training sessions. The risk culture includes the ways that communication is conducted. External

stakeholders, such as the media, the general public, and pressure organizations, will need to be informed about external risks.

For instance, if a road haulage business wants to expand its vehicle storage facility, it will need to consult with stakeholders and the planning offices of local governments. The business must present reasons that assess any hazards to the neighborhood that could rise as a result of the depot's extension. It's possible that the public's assessment of the proposal's effects on the neighborhood is not entirely true. As a result, the organization will need to produce truthful, transparent, and thorough justifications that reassure all parties involved that sufficient risk management measures are in place. An example of risk communication in connection to the nuclear and chemical sectors in the US is given in the box below. The takeaway from this is that the general public's sense of danger could not match the available scientific facts. An organization's information should do more than just provide knowledge. Emotional issues should be included in the dialogue as well. The capacity to lead a training course is a crucial factor in regard to communication abilities. Risk practitioners in particular will need to provide training on risk assessment. A successful workshop must have a lot of fundamental abilities, but setting up its structure and format is the first step. In general, it will be important to make sure that the conversation is organized effectively and that each participant has an equal chance to speak. Sticky notes are one method that is used during workshops to record suggestions from participants. The relationship between these remarks and the particular questions posed is then compiled. It takes ability on the part of the facilitator to combine disparate ideas into a manageable number of problems, or more particularly, recognized risks. The facilitator will need to see patterns in the ideas and combine compatible concepts into a smaller number of concerns [2].

Running training sessions needs a distinct set of abilities, but maintaining participant engagement is always a major goal. It is often recommended that training sessions follow a three-stage structure: inform the participants of what you will say, what you will say, and what you will say after you have said it. Although this strategy seems laborious and simplistic, it is often the most effective method to make sure that the messages are sent and received. Perhaps thinking of a training course as having three sections is more organized. Speaking and writing presentation abilities are related to other communication skills. The capacity to produce reports for both internal and external dissemination will be one of them. The writing style of written reports will vary substantially depending on the company. The majority of businesses want quick summaries of reports for the board, with extensive supporting documentation readily accessible. It is crucial that the risk practitioner establish a communication style that blends in with the organization's culture.

The display of risk information may be done in this way if reports often include visuals. The risk practitioner will find it difficult to provide risk reports in an interesting manner using simply words if all reports inside the business are narrative. The presentation manner must also be consistent with previous board presentations if the risk practitioner is asked to address the board. It is crucial to prepare well and be knowledgeable about pertinent background material. The risk practitioner must determine what should be learned from the presentation before presenting it to

the board. A report to the board that requests a decision or permission to pursue a particular course of action is presented differently from one in which the risk practitioner is only delivering facts. When the audience is the organization's board, the adage "know your audience and their expectations" is crucial. The "Cs" of communication are helpful to keep in mind while conveying a message. The message must be thorough, convincing, succinct, cohesive, and clear.

A clear message will guarantee that the receiver knows the reason for your communication. Because you kept it succinct and to the point, your message is more likely to be understood. A communication is logically coherent if all of its points are related to the primary subject and make sense together. A trustworthy message will persuade the audience that you are aware of their needs and priorities. The audience receives a complete message that has all the information they need to take the appropriate action.

Relations Abilities

There are many different connection skills needed, but as was already said, persuading and negotiation abilities are the most crucial. Relationship skills are crucial, as are political and motivational abilities. Relationship skills must be used within the organization's culture and in a manner that fully considers its internal context, much like other people skills. Listening abilities are a part of interpersonal abilities. It is crucial to pay attention to the viewpoint of the person you are negotiating with or trying to persuade. Generally speaking, influence is attained by bringing passion and good energy to the problems that need to be resolved.

Those with the capacity to garner support, motivate others, forge connections, and capture their audience's imaginations are most effective influencers. Improvements in risk management guidelines sometimes need ongoing dialogue. Risk practitioners should be aware of and embrace negotiating strategies since they are well-established ways of establishing effective agreements. Politics may be challenging and the topic seems pretty ominous. However, a successful risk practitioner has to be aware of the value of political acumen in order to have a constructive influence. There are difficult people in every workplace who act inappropriately. The risk practitioner will need to comprehend group dynamics, be able to diffuse disagreement, and be flexible while negotiating solutions. Understanding cultural impacts and varying stakeholder needs are among the political talents. The risk practitioner's role as meeting chair is often when their political acumen is most crucial. Everyone present at the meeting has the right to speak out in full as long as their point of view is credible, succinct, and unambiguous. The chairman's job is to steer the meeting toward a suitable consensus while remaining impartial, particularly while serving in a non-executive capacity [3].

Building connections with many stakeholders is the core of relationship skills. As was covered in Paper, a risk practitioner must interact with stakeholders who will be many and diverse. Customers, employees, financiers, suppliers, regulators, and society are only a few of the stakeholders that make up an organization (CSFSRS). It is clear that the risk practitioner requires great interaction and communication skills given the vast spectrum of stakeholders, not all of whom will be engaged in risk and risk management. Risk practitioners will need to have highly well-developed people skills to deal with certain stakeholders' viewpoints. The current state of

health and safety makes it almost difficult for me to do my duties. The BBC health and safety staff are referred to as Prohibition Officers from the PPD, or the Program Prevention Department, in Top Gear.

DISCUSSION

Diverse analytical abilities are needed, along with logical and strategic thinking. Sometimes, when issue resolution is involved, the risk practitioner also has to be creatively lateral thinking. The quantification of risks involves a large number of risk practitioners, either as part of the Basel II capital requirement calculation or as part of an analysis to identify the proper amount of insurance that is necessary. However, analytical abilities are not usually grounded on mathematics, and a normal risk practitioner will profit greatly from well-developed problem-solving abilities. Many risk practitioners often need research abilities in addition to analytical abilities. A risk practitioner will greatly benefit from having the capacity to discover and analyze information quickly and effectively. Risk practitioners often need to examine a lot of data on a particular subject, identify the themes within that data, and convey the conclusions succinctly and logically. When the risk practitioner is creating a written report, a training session, or a presentation, this will nearly always be necessary. When a risk practitioner is attempting to lead a risk assessment workshop, the advantage of having analytical skills is at its highest [4].

In risk assessment workshops, it often happens that the participants will have varying opinions on the degree of risk provided by a particular circumstance. A skilled facilitator is able to take in these opposing points of view and pinpoint the underlying assumptions that led to the various findings. The professional facilitator will then be able to question the various participants with the grounds for their divergent perspectives after identifying the presumptions and assumptions. This will be the most effective method of reaching a consensus. The capacity to comprehend, question, and express issues and ideas allows one to make judgments based on the facts at hand. These abilities include the capacity to exhibit and use logical thinking while collecting and analyzing information, as well as when creating and putting to test problem-solving ideas. The capacity to construct adequate alternative solutions and question the alternatives in order to produce the most logical plan of action is the result of analytical abilities.

Making decisions and addressing problems are crucial abilities for the workplace. Making decisions is a crucial part of problem resolution, particularly when it comes to risk management. There are exercises and methods to enhance decision-making and decision quality. Some personalities are better at making choices than others, thus these individuals should concentrate more on doing so. Although they may need to be more resolute in carrying out their judgments, people who are less natural decision-makers often have the ability to produce high-quality evaluations. Both problem solving and decision-making involve creativity in order to uncover and create possibilities. Techniques for brainstorming, like as SWOT and PESTLE analytical frameworks, are very helpful. A variety of abilities, including imaginative invention and identification of choices, clarity of judgment, firmness of conclusion and effectiveness of execution, are needed to make good decisions[5].

Managing Abilities

Risk management departments are often fairly small, however this is not always the case. In any case, it is necessary for the risk practitioner to comprehend management abilities even if they do not directly oversee management. These abilities could be useful in getting other managers to follow a different path. This understanding of management abilities need to include team management and power delegation. Many of the soft skills discussed in this section that relate to people also apply to management. The ability to motivate others may be the most crucial of these interpersonal abilities for a manager. For risk practitioners, motivational skills are crucial, particularly when a change in behavior or the emergence of a risk-aware culture is called for. The risk practitioner will have to persuade others to act differently, including managers and directors. Self-management abilities are quite important as well. These will include the capacity to establish sensible priorities, fulfill pressing deadlines, and keep one's drive. Throughout their career, risk practitioners need to have strong time management, organizational, and self-motivational abilities. Maybe it's worthwhile to consider the distinction between management and leadership. A person may be able to oversee a department by exerting strict control over each employee's actions. This differs from a team leader who assigns team members responsibility for managing their own activities in order to achieve the team's priorities. The leader should have made sure that the people in charge of carrying out the priorities were fully involved in the development of the priorities.

Sustainability and accountability at Tim Hortons

At Tim Hortons, sustainability and responsibility are incorporated via a structure with three main pillars: people, communities, and the environment. A variety of critical topics that have been identified as being significant to our stakeholders are included in each pillar, such as nutrition, food safety, staff, kids, animal welfare, community giving, environmental stewardship, climate change, and sustainable supply-chain methods. Regarding each of these areas of concentration, we have established a number of commitments and objectives. Our annual sustainability and responsibility report details how we performed in relation to these goals. Our sustainability and responsibility policy is continuously evaluated and contains a framework and auxiliary procedures for efficient governance and accountability of sustainability and responsibility. The board's nominating and corporate governance committee oversees sustainability and responsibility. Review of policy formulation, plans for sustainability and responsibility, risk mitigation, organizational sustainability and responsibility pledges, objectives, and external reporting are all examples of oversight activities. The Tim Hortons executive group has managerial responsibility for sustainability and responsibility. Our governance system incorporates the evaluation and management of sustainability-related risks and opportunities, as well as our sustainability and responsibility plan and its

Risk Management

The development of internal performance scorecards, keeping track of our relationships with our stakeholders, assessing sustainability and responsibility trends, and taking into account public policy, consumer, corporate, and general public are some of the key components of our approach. Risk is actively handled inside the core department, and risk management is ingrained throughout all departmental procedures. The board, the executive board, and its subcommittees

all play a crucial role in risk management, according to the department's risk framework. Staff members have access to policy and direction through the intranet, and risk management masterclasses have been offered. The corporate committee is in charge of the framework for risk management generally [6].

There are three management levels in the risk management framework where risks are managed: Risk is handled locally, and risk registers are kept up to date by project and program teams from throughout the department, together with operational and policy teams. The corporate committee oversees risk management at the committee level. The committee controls operational risks with a red rating in the corporate sector and keeps a separate risk registry. The executive board oversees department-wide operational, delivery, and strategic risks as well as those elevated by the corporate committee, investment committee, and governance board. The department's risk management systems gave a fair level of confidence, according to an internal audit evaluation. It came to the conclusion that the department was aware of and managing the main business risks related to routine business operations and program activities. Although there is not universal adherence to the agreed-upon risk management framework or single-risk severity scoring method, different approaches to risk management methodology revealed this. It was therefore necessary to develop a more structured and uniform approach to monitoring and comparing risks in these areas [7], [8].

CONCLUSION

The paper identifies the core competencies that all risk practitioners should possess, such as risk identification, analysis, and evaluation. It also examines specialized competencies that may be required in specific industries or sectors, such as financial risk management or cybersecurity risk management. Moreover, the paper emphasizes the importance of soft skills, such as communication, collaboration, and leadership, in the success of risk management efforts. It highlights the need for risk practitioners to be able to work effectively with stakeholders across the organization and to communicate complex risk concepts clearly and persuasively. Overall, the paper emphasizes the critical role of risk practitioner competencies in the success of risk management efforts. It emphasizes the need for organizations to invest in developing the skills and knowledge of their risk management teams and to foster a culture of continuous learning and improvement in this field.

REFERENCES:

[1] B. Kubheka, “Risk Management Competencies for Medical Practitioners Working in South African Hospitals,” *ProQuest Diss. Theses*, 2014.

[2] A. Rashid and M. S. Ghazi, “Factors affecting Sharīʿah audit quality in Islamic banking institutions of Pakistan: a theoretical framework,” *Islam. Econ. Stud.*, 2021, doi: 10.1108/ies-07-2020-0025.

[3] N. Muthomi, L. J. Wachira, and W. S. Ooko, “Knowledge in pre-hospital emergency and risk management among outdoor adventure practitioners in East Africa afro-alpine mountains,” *African J. Emerg. Med.*, 2021, doi: 10.1016/j.afjem.2020.08.006.

[4] N. J. Harper and P. Obee, "Articulating outdoor risky play in early childhood education: voices of forest and nature school practitioners," *J. Adventure Educ. Outdoor Learn.*, 2021, doi: 10.1080/14729679.2020.1784766.

[5] P. Willumsen, J. Oehmen, V. Stingl, and J. Geraldi, "Value creation through project risk management," *Int. J. Proj. Manag.*, 2019, doi: 10.1016/j.ijproman.2019.01.007.

[6] A. Zerfass, J. Hagelstein, and R. Tench, "Artificial intelligence in communication management: a cross-national study on adoption and knowledge, impact, challenges and risks," *J. Commun. Manag.*, 2020, doi: 10.1108/JCOM-10-2019-0137.

[7] C. J. Gidlow *et al.*, "Cardiovascular disease risk communication in NHS Health Checks: A qualitative video-stimulated recall interview study with practitioners," *BJGP Open*, 2021, doi: 10.3399/BJGPO.2021.0049.

[8] K. Wheeler and K. E. Phillips, "The Development of Trauma and Resilience Competencies for Nursing Education," *J. Am. Psychiatr. Nurses Assoc.*, 2021, doi: 10.1177/1078390319878779.

CHAPTER 26

AN OVERVIEW ON CORPORATE GOVERNANCE MODEL

Aditya Sharma, Professor
Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id-adityahr2018@gmail.com

ABSTRACT:

Corporate governance is the system of rules, practices, and processes by which a company is directed and controlled. It encompasses the mechanisms through which companies, boards of directors, and senior management operate and are held accountable to stakeholders. Effective corporate governance is essential for sustainable growth, investor confidence, and the long-term success of a company. This study provides an overview of the corporate governance model, highlighting the main principles and best practices that guide the functioning of boards of directors, executive management, and other stakeholders. It explores the role of the board of directors in setting the company's strategic direction, overseeing management's performance, and ensuring accountability to shareholders.

KEYWORDS:

Business, Environment, Mitigation, Practitioner Competencies, Risk Appetite, Risk Management.

INTRODUCTION

Risk management is a crucial component of effective corporate governance in any firm, and the issue of corporate governance is quite broad. Organizations must comply with corporate governance laws in the majority of nations. In regard to publicly traded enterprises, registered charities, and government departments, agencies, and authorities, these standards are more stringent. For instance, the UK Corporate Governance Code () issued by the Financial Reporting Council must be followed by businesses that are listed on the London Stock Exchange. Corporate governance exists to support accountability, responsibility, and ethical behavior as well as effective and efficient performance. Executives and staff should be protected while doing the tasks that are demanded of them. Finally, it should guarantee stakeholder trust in the organization's capability to recognize and deliver results that matter to its stakeholders.

The enforcement of corporate governance rules may be done in two ways. Some nations have a "comply or explain" policy on corporate governance rules. Alternatively, the organization must provide a justification for why it was not suitable, essential, or practical to comply with the standards. An organization may, if appropriate, describe how a different strategy was used to arrive at the same outcome. The criteria may be seen as one way to promote best practices in these nations, but equally effective other systems are also acceptable. Other nations demand

complete adherence to certain rules, even if these requirements may give limited possibilities for obtaining adherence. Detailed compliance is anticipated in these nations, and deviations won't be tolerated.

Corporate governance standards should be seen as duties put on an organization's board of directors. Legislation and numerous rules of practice impose these obligations on board members. These corporate governance rules are sometimes laid out as comprehensive codes of conduct. An organization may create an acceptable "delegation of authority document" and a code of ethics for company directors as a starting point for improving corporate governance standards. Directors should be obliged to submit an annual declaration of any possible "conflicts of interest," and the board should get corporate governance training. Additionally, the organization should form the proper committees (as indicated below), which may be constituted as subcommittees of the board. Each of these committees should have clear terms of reference and membership. Every board meeting should hear reports on corporate governance norms, issues, and actions. The company secretary will often provide these documents. These committees might be:

1. Committee for risk management;
2. Committee for auditing;
3. Committee for disclosures;
4. Committee on Nominations;
5. The compensation committee.

'The method by which corporations are directed and managed' is a fundamental definition of corporate governance. As a result, corporate governance is concerned with the systems, practices, checks, and balances, as well as the accountability and decision-making processes at the highest levels of a company. Every organization's entire corporate governance structure includes a significant portion of risk management since corporate governance is concerned with how senior management fulfills their duties and exercise their power. Regardless of size or whether they are in the public or private sector, all organizations, regardless of size, need to make decisions with transparency, honesty, and accountability [1], [2].

An international body called the body for Economic Cooperation and Development (OECD) assists nations in addressing the economic, social, and governance issues brought on by a globalized economy. The list of corporate governance standards has been revised by the OECD. These guidelines concentrate on creating a framework for corporate governance that is efficient and respectful of stakeholders' rights.

DISCUSSION

Promote open and equitable markets, effective resource allocation, adherence to the rule of law, and encourage efficient oversight and enforcement. Protect and make it easier for shareholders to exercise their rights, and make sure that all shareholders, particularly minority and foreign owners, are treated fairly. Good corporate governance is facilitated by stock markets that operate in a manner that is consistent with sound incentives across the investment chain. The principles of corporate governance demand that all stakeholders be treated fairly and have a voice in how

the firm is governed. The principles also call for effective board oversight of management and board responsibility to the company and its shareholders. The principles also call for openness and dis- closing. Since the board of the organization is responsible for delivering all of these principles, the principles include extensive references to the duties of the board [3].

Recently, British Standards and other organizations produced a number of standards on corporate governance. Code of conduct for ensuring efficient organizational governance. 'It is becoming evident that society's expectations of organizational behaviors and performance, and thus: "governance," are growing,' British Standards said when it released the standard. The scope of the code thus extends beyond the prevention or mitigation of issues, in part because of a continual stream of big occurrences and apparent abuses of power. It establishes various responsibilities to various stakeholders and serves as a basic check list to make sure that all the components of a sound governance system are in place. Additionally, it is stressed that although having a corporate governance framework in place doesn't ensure successful governance, it does promote and foster admirable organizational ideals and conduct.

The efficacy of the board is the main emphasis of corporate governance recommendations from the London Stock Exchange (LSE). According to LSE, corporate governance is concerned with the efficient running of the business as well as the roles and duties assigned to top managers and board members inside the company. a concise illustration of the governing structure of the London Stock Exchange. The LSE advice refers to these boards as supervisory and management boards since they are the focus of the organization's governance efforts. The two fundamental parts of the corporate governance framework are:

The general standards and structure within which corporate governance must be delivered are provided by the OECD principles and the LSE corporate governance framework. However, different strategies will be used to meet each of the five stakeholder expectations. Activities related to risk management should be regarded in the context of corporate governance as a whole. The LSE framework presents risk management as a distinct aspect of corporate governance, although risk problems also support strategy, corporate social responsibility, audit, and transparency. The function of non-executive directors in company governance is crucial. The audit committee, as previously said, will often be a non-executive body and serve as the third line of defense.

Corporate responsibility for a Bank

Activities related to corporate governance and risk management are carefully supervised and regulated inside financial organizations. Banks and the majority of other financial institutions create their own internal corporate governance policies. These regulations often address the requirements for directors, their duties, and the obligations and powers granted to board committees. The recommendations should also take into account the procedures for the board's yearly performance review and the plans for senior management succession. A collection of guiding guidelines for the behavior of the board of directors will often comprise the corporate governance framework. These governing principles will provide board members with guidance on how to handle conflicts of interest, maintain confidentiality, and adhere to laws, rules, and

regulations. Proper training and induction for board members will play a significant role in providing proper corporate governance for a financial institution. Banks and other financial organizations are now examining their own corporate governance rules as a consequence of the global financial crisis. An overview of a large national bank is given in the evaluation in the box below, along with complaints of the bank's corporate governance shortcomings [4].

Corporate responsibility for a Government Organization

Corporate governance policies that are strong are often required for government organizations. Additionally, many government organizations focus on risk management primarily to make sure that sufficient corporate governance procedures are in place. In other words, a typical government agency's primary driving force for maintaining high standards of risk management would be its need to support its corporate governance structures. Demonstrates the elements of corporate governance for a typical government organization. Corporate governance and risk management are intended to help commercial companies accomplish their goals, especially market- or commercial-related goals. Government agencies are more often driven by accountability and have a more limited incentive to implement high corporate governance standards.

Corporate responsibility in a government organization

The avoidance of improper behavior and getting the most value for your money are the guiding principles of government organizations. Governmental organizations often see corporate governance as building a framework of control that fosters innovation, integrity, and accountability and promotes effective management across the board. Individual staff member roles are usually outlined in the corporate governance structure. Also described is the method for reporting risk-related concerns. Specific risk areas that need extra attention may be recognized when risk management initiatives are linked to corporate governance. Value for money, business continuity, fraud prevention, and guarantee of IT security are usually included. The Nolan principles, also known as the principles of public life, will serve as the foundation for corporate governance operations inside a government department, agency, or authority. The Welsh Assembly Government's (WAG) risk policy outlines its approach to identifying and managing risks that might prevent it from achieving its goals. Its objectives are to make sure that risk is considered at all stages of developing and implementing WAG activities, including risk analysis and the creation of risk management measures, as well as to monitor, assess, and evaluate such activity[5], [6].

In order to establish the conditions and frameworks for the implementation of the WAG plans, the Accounting Officer and Strategic Delivery & Performance Board of the Welsh Assembly Government have adopted the following risk management policy. Its purpose is to: Ensure that the goals of the Welsh Assembly Government are not adversely impacted by significant risks that have not been anticipated. Ensure that outputs and outcomes are met, and make sure you have solid contingency plans in place to handle any unforeseen circumstances that can endanger the delivery of services. Encourage a more inventive and risk-tolerant culture where taking calculated chances in search of possibilities that will benefit the WAG is rewarded. Establish a

solid foundation on which to incorporate risk management into decision-making. a part of top-notch business governance and management techniques.

Review Of the Board's Performance

The board is in charge of determining the organization's overarching strategy and maintaining effective governance. Executive management is in charge of the company's management, and top management often consists of board members in the form of the executive directors of the organization. The term "unitary board" refers to a board that includes both executive and non-executive directors. In many businesses, the board is known as the supervisory board and exclusively includes non-executive directors. The executive directors will convene as the executive committee in jurisdictions without a supervisory board. Sometimes referred to as a two-tier board structure, this arrangement separates executive and non-executive directors into different committees [7].

The two-tier board arrangement is more typical in certain nations. Additionally, it is typical for nonprofits and public-sector organizations to have a two-tier board structure in place. The board will be responsible for a variety of tasks whether the organization is unitary or two tiers. The board will typically list the matters over which it will continue to have final say and accountability. These concerns are often referred to as board-reserved topics. Setting the organization's risk appetite is a crucial duty for the board that is often not assigned. After deciding which problems are to be left up to the board, it will be required to determine how power and responsibility will be assigned with regard to other concerns. A declaration of the delegation of power, which will be a key document in relation to the governance structure in the company, is often produced by big enterprises.

The three layers of management within a company, executive directors, managers, and employees, serve as the first line of defense in maintaining appropriate standards of governance, including risk management and internal control. The board should be informed about the existence of specialized risk management departments inside the company, as well as the operations of these departments and their duty as the second line of defense. The audit committee would consist of non-executive board members, and they should be aware of their responsibilities as the third line of defense in ensuring sufficient risk governance. Any organization's corporate governance practices must include an evaluation of the board's performance. A list of issues that need to be examined while determining if a board is successful. The following are the areas to be evaluated:

1. Membership and organization.
2. Intention and purpose.
3. Participation and responsibility.
4. Monitoring and evaluation.
5. Impact and performance.

Focuses on the effectiveness of corporate governance and the board's performance. The board must make sure that sufficient processes are in place for making judgments when making decisions on strategy, tactics, operations, and compliance. These choices will lead to a course of

action, and it is important to keep an eye on how that course of action is being carried out. There will be some outputs from the course of action, and they must be assessed in terms of the effect made. The outcomes of the board's choices serve as the ultimate barometer of its performance. The amount of influence may then be assessed in relation to the organization's vision, purpose, and goals [8].

CONCLUSION

In conclusion, a well-designed corporate governance model is crucial for the success and sustainability of any organization. Corporate governance refers to the system of rules, policies, and procedures that govern an organization's operations and behavior. It provides a framework for decision-making, accountability, and transparency, and helps to ensure that an organization operates in an ethical and responsible manner.

An effective corporate governance model should include several key components, including a clear definition of the roles and responsibilities of the board of directors, senior management, and shareholders. It should also include mechanisms for monitoring and evaluating organizational performance, as well as policies and procedures for managing risk and ensuring compliance with legal and regulatory requirements. However, it is important to recognize that there is no one-size-fits-all approach to corporate governance, and that different organizations may require different models depending on their size, structure, and industry. Furthermore, the effectiveness of a corporate governance model depends on its implementation and the commitment of the organization's leaders to promoting a culture of ethical and responsible behavior. Overall, an effective corporate governance model is critical for the success and sustainability of any organization. By providing a framework for decision-making, accountability, and transparency, it can help to promote organizational integrity, enhance stakeholder confidence, and support long-term sustainability.

REFERENCES:

[1] M. Kausar Alam, S. Ab Rahman, H. Mustafa, S. Mohammed Shah, And M. Mizanur Rahman, “An Overview Of Corporate Governance Models In Financial Institutions,” *Int. J. Manag. Sustain.*, 2019, Doi: 10.18488/Journal.11.2019.84.181.195.

[2] A. Jamaludin, “The Islamic Models Of Corporate Governance Turkish Journal Of Computer And Mathematics Education Research Article,” *Turkish J. Comput. Math. Educ.*, 2021.

[3] M. K. Alam, S. A. Rahman, H. Mustafa, S. M. Shah, And M. M. Rahman, “An Overview Of Corporate Governance Models In Financial Institutions,” *Int. J. Manag. Sustain.*, 2019, Doi: 10.18488/Journal.11.2019.84.181.195.

[4] A. C. Fernando, K. P. Muraleedharan, And E. K. Satheesh, *Corporate Governance Principles, Policies And Practices*. 2017.

[5] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama, And J. Shah, “Iot Security Risk Management Model For Healthcare Industry,” *Malaysian J. Comput. Sci.*, 2019, Doi: 10.22452/Mjcs.Sp2019no3.9.

[6] W. Boonyanusith And P. Jittamai, "Blood Supply Chain Risk Management Using House Of Risk Model," *Walailak J. Sci. Technol.*, 2019, Doi: 10.48048/Wjst.2019.3472.

[7] C. Doyle, D. Murphy, And D. Watson, "Corporate Governance: An Organisational Attribute Or An Academic Exercise?," *Mark. Int. J. Bus.*, 2021.

[8] P. Howard, C. O'brien, B. Kay, And K. O'rourke, "Leading Educational Change In The 21st Century: Creating Living Schools Through Shared Vision And Transformative Governance," *Sustain.*, 2019, Doi: 10.3390/Su11154109.