iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6372

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Risk Management Associated in Organization

Prabhu Prasad
University of Mysore, Karnataka, India

Abstract: ***The present paper aims to highlight the risk management strategies associated in any organization. The risk management strategy can be of different kinds which plays important roles in gaining the profit ratio and avoid the risk for smooth running of organization. Hence in the present study, each components of the risk management is briefly discussed along with the role of emerging techniques of information science to keep updated the risk management process.***
Keywords: Risk management, Organization, Information tools, management techniques

I. INTRODUCTION

Various experts had expressed numerous outcomes for the Risk, and some revolve around a selected business condition, even when others have a continually non-selective meaning of Risk [1-4]. The sufficiently well-known importance of risks in the context of the state of the organization can be described as a phenomenon in which the likelihood of a merger may create a risk, which may be unique due to the likelihood of a threat occurring [2]. Additionally, Oxford's English expression of reference defines Risk as "A condition that encapsulates the preface to the threat" or "The for something bad or unpleasant to happen." [2,4]. According to Poudyal Chhetri (2003),[2] offers a condition of imminent Risk, which is "risk = deficiency + damage". There is no longer critical in terms of conditions and that an equivalent state of affairs can typically be used to visualize and recognize the Risk. In any case, the Risk must now be resolved backwards with the membership peak that influences a lot. For example, a slight obsession can be described as "the scattering cluster of the solid secondary results of the flexible chain, its and its excited qualities". Others continually summarize the consequences of the threat. Before we can select a management installation, we must understand the occasion. An affiliate must go through three steps before selecting the excellent risk control method to use. Since hazard management can use many sources, explanations, and rules must be established before guiding hazard management. The three fragments are

A. Recognizable probability test: enrollment must begin by analyzing all activities susceptible to the skill. Also, they can use a risk assessment device to find out the possible threat that could occur
B. Evaluation of possible fortuitous occasions: although the membership perceived the Risk, predicts it should no longer neglect the damage of ability that they should cause. Ultimately, randomness is vital for an association not to be forgotten because it will help shape and train any important case management method.
C. Develop a well-informed response to the occasion of Risk
D. After the Risk has been practiced and disaggregated, membership can begin to choose which resources must conquer what many would consider possible or ruin the occasion of Risk.

II. ADDRESSING THE SOURCES OF RISK:

Once an associate has identified unexpected opportunities that may occur, they must be aware of all their sources to choose the Risk that will be addressed first [2,4]. Most associations can also have a limited level of resources and can cope with each of the two activities. If many dangerous activities occur, this includes figuring out what to limit. It advises the institutions not to forget the impact that the possibility of a liquidity-related affiliation can have and expose the benefits, concentrating all their activities to postpone the risks first.

The intention is risk management, and its negative result can have real effects for an affiliation. However, nobody will guarantee the execution of the movement. It gives the importance of an affiliate who manages threat manipulation [4-6].

There are some unique structures and considerations that allow forming an occasion that we need to be aware of while limiting the organization. One of the maximum complete systems for the company at Risk is the photo of opportunities and effects. This module tracks risks, changes and unanswered questions and measures the likelihood of such opportunities occurring and the severity they face [2,7].

III. TECHNIQUES

Furthermore, there are some specific techniques to explain which threatening event should be assessed. Risk properties can also be distinguished using excellent income frameworks. For companies that want to acquire a versatile approach to the threat that gradually take what they want, they may need a broad and varied approach. It is due to the data that we can choose exciting qualities depending on the activities and the importance of the desires of the relationship and curious partners. It has several similarities to an accounting option; however, it offers a slow, dynamic and creative approach to controlling the representation of the parties in an attempt to use Risk. There are some corrections to this method, along with a pocket diagram, a choice scheme, a significant employer for infertility and an excessive risk model [8]. The final framework to make sure the case is prepared is the use of quantitative trends and techniques. The fundamental clarification that a commercial company will use a quantitative risk method is that it is an extraordinarily cautious technique that expects almost nothing, nothing, changes and alterations (Hopkinson et al., 2008). It recommends maintaining a quantitative threat approach for organizations that wish to organize hazards competently, with reduced charges and the use of an inconsistent percentage of activities that can be moderately ordinary. The process of risk management cannot be under estimated in any organization which is considered to be the basic entity for functioning of organization [9,10].

When the Risk is sufficiently organized, it should also be studied thoroughly. There are some risk assessment techniques, and simple threat assessment strategies are quantitative hazard assessment and comparative hazard assessment.

IV. COMPETITIVE RISK ANALYSIS

Also, comparative risk analysis is becoming the preferred risk assessment technique for some groups around the world [2,8]. It is due to the truth that a comparative risk assessment has become effective and complete and offers the subtleties and reality of a casual. Also, a comparative probability assessment incorporates recognition of the maximum legitimate Risk before verifying other threatening events [11-13].

Furthermore, there may be another approach to perceived threats. It takes advantage of the Inventive Adaptive Threat Assessment (CORE) structure. It is a tool created through Microsoft and Arthur Anderson to allow a business company to detect, examine and prevent any risky possibilities [2].

The tool recognizes a total of nineteen random elements and describes them in 4 distinctive subgroups; foundation, organizational checks, checks and business associations. It offers participants the excellent chance, as each company can increase the importance of each topic considering its importance for the daily physical games of the complicit groups.

Most risk assessment strategies and methods share a standard theme, in particular by comparing the possibility and impact of imaginable risk activities that could arise and have an impact on the daily activities of an affiliation. It provides the importance of threat assessment and why it is a basic set that a risk manager should be able to use [2,8,13]

Additionally, there may be another element to consider when developing a threat management method, which is the person and individual of the principal. Some managers will follow the usual techniques and will not perceive the warnings of others, which also suggests that they will no longer follow a neglected risk management strategy, regardless of whether it is fruitful step by step.

After an affiliation has completed the 3 phases mentioned above, to perceive the test, compare and improve a reaction, they will have to keep with the fourth step. The final segment is choosing and updating the accepted hazard method, which has changed to chosen in the three phases mentioned above, beyond what many might think of conceiving or ruining the potential threat event.

V. RISK MANAGEMENT STRATEGY

A Risk Management Strategy "specializes in perceiving and analyzing the possibilities and outcomes of hazards and in choosing appropriate strategies to reduce the likelihood of episodes associated with hostile events. Risk reduction focuses on reducing the effects of if a risky event is observed. Although there are many threat management strategies, some of which generally depend on conditions, there are three critical techniques for controlling capabilities.

VI. THE AVOIDANCE STRATEGY

The fundamental type is the point at which an affiliation will attempt to reduce the possibility of an identical or near zero chance of a risk occurring, which may be regular due to conditions. The second type of evasion strategy is the point where an association tries to deal with the risk event.

VII. PROTECTION STRATEGY

A risk control security method that aims to limit the threat of events that occur. It is essentially the same as the circumvention strategy, despite the data that everyone sees how a risk event will occur and is more effective in stabilizing the association since any effect that can cause the threat occasion can be incredibly standard. Updating a security strategy should be feasible in various ways, by consolidating personal frameworks with neighboring governments, proactively maintaining suggestions or ensuring the security and internal benefits of joining.

VIII. VERIFY / SHARE / MOVE

This strategy can appear as a vertical commitment. It increases the potential of a pioneer within an association to control various procedures, auxiliary strategies and choices. Having an apparent logical authority over an affiliate's daily activities can help limit the likelihood and effect of the threat. It can help spread the Risk through various activities and, in this sense, reduce the severity of the threatening event. However, the crucial elements for gradual dazzling manipulation can also cause the need for a visible union which can be difficult for associations to achieve.

IX. DISCUSSION AND INTERPRETATION

If the threat occasion dramatically ruins an association and is considered a "high threat", a company should plan to use an intelligent approach suggests that it would be better as it would limit or completely exhaust such possibility to occur. In any case, this could be very expensive for the part and many resources for the buyer. On the other hand, if the fortuitous event affects the experience of an organization to a limited extent and is visible as a "particularly guaranteed" event, an approach to security could be consistently valid as it will guarantee sources and associative activities organization of the hazard event. The development of new models based on advanced management tools can help in providing additional safety and security to gain more protection.

Developing the right method of managing the maximum opportunities to be used can be quite an activity for any manager. The supervisor chooses a missing risk management technique. One of the most crucial parts that can influence the selection of which threat technique to look for is the severity of the possibility [14-16]. The use of management information system is reported to benefit the organization to forecast the risk management hence the multi-national organization and companies are setting up management information system to predict and overcome the financial loses [17]. Further, the disaster recovery planning can also associate with organization to plan the protocols which can help to prevent financial losses at larger extend as per the recent report published by Dineskumar, 2020 [18].

X. CONCLUSION

There are some steps that a supervisor wants to take to perform a risk management method properly. One of the crucial maximum snapshots of this system is to give enough centrality to look at and examine the Risk so that we can choose a quick and reasonable strategy.

Similarly, the threat officer should attempt to use a guided technique to get the most out of models, undertake any risky activities that may arise and expand a vital crisis development path to address those opportunities. However, due to some parts, which consist of limited sources, it is generally not possible for a company to perform the task. In this situation, they should focus on a management approach that limits the effects of the risks. Most of the random activities can be considered with a weighted connection and an evaluation. In any case, it is possible to make a passage to limit the consequences of the occasion that will occur.

REFERNCE

[1] S. A. Weil, S. A. Brandt, E. L. Miller, D. D. Long, and C. Maltzahn “Ceph: A scalable, high-performance distributed file system,” Operating systems design and implementation. USENIX Association, 2010, pp. 307– 320.

[2] M. B. Poudyal Chhetri. Risk management in Nepal: organisations and programmes. Managerial Finance, 29(5/6), 20–35. https://doi.org/10.1108/03074350310768733(2003)

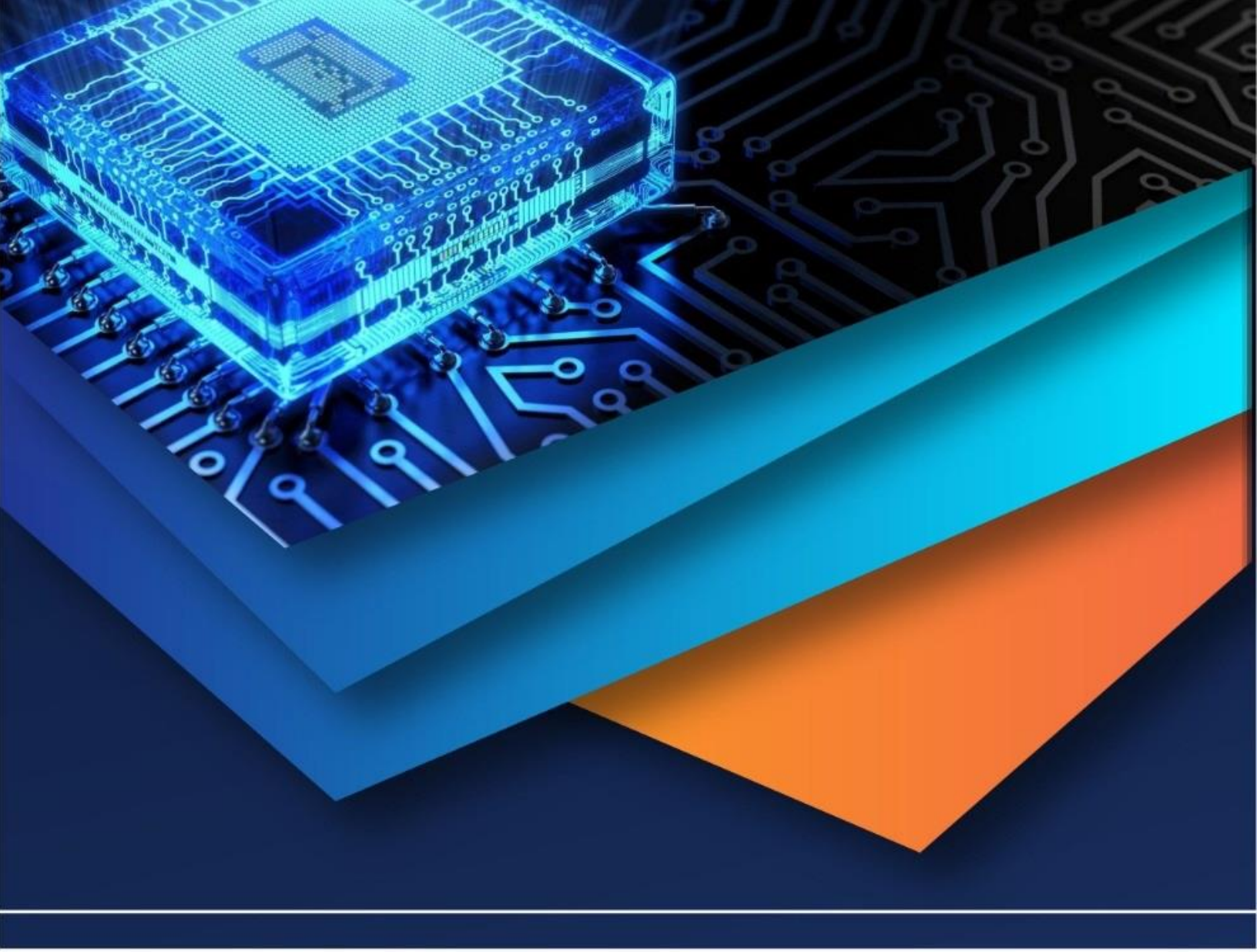
[3] F. Bin Shawiah, Risk management strategies for dealing with unpredictable risk in saudi arabian organisations [ProQuest Dissertations Publishing] http://search.proquest.com/docview/1947636990/(2016).

[4] B .Boland and S.Bremner, (2013). Squaring the circle: developing clinical risk management strategies in mental healthcare organisations. Advances in Psychiatric Treatment, 19(2), 153–159. https://doi.org/10.1192/apt.bp.111.010009(2013).

[5] S. Falkiner, OHS risk management for an ageing workforce: where does it fit within your organisation? Journal of Occupational Health and Safety : Australia and New Zealand, 25(6), 483–493. http://search.proquest.com/docview/211506753/(2009).

[6] D.Giarratano , L.Guise and Y.J Bodin, Does cyber security moving towards risk management leads to new grid organisation? CIRED - Open Access Proceedings Journal, 2017(1), 2700–2702. https://doi.org/10.1049/oap-cired.2017.0799(2017).

[7] J .Maxted, Risk management in the outdoors: A whole-of-organisation approach. Journal of Outdoor and Environmental Education, 16(2), 44–45. https://doi.org/10.1007/BF03400945(2013).
[8] C. Wendling, Incorporating Social Sciences in Public Risk Assessment and Risk Management Organisations. European Journal of Risk Regulation : EJRR, 5(1), 7–13. http://search.proquest.com/docview/1519054035/ (2014). http://search.proquest.com/docview/212682942/(2004).
[9] R.R.Nadikattu, Risk Management in the IT Department (May 21, 2020). Risk Management in the IT Department, International Journal Of Advance Research And Innovative Ideas In Education, Volume 6, Issue 3, 2020. Available at SSRN: https://ssrn.com/abstract=3620047.
[10] R.R. Nadikattu, "Effective Innovation Management in Strategic Planning", international Journal of Engineering, Science and Mathematics. 9, 5, 106-116. 2020.
[11] James G.March and Zur Shapira. Managerial Perspective on risk and risk taking1 Nov 1987https://doi.org/10.1287/mnsc.33.11.1404
[12] M.Moyo, H. Abdullah and R.C. Nienaber. Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems. 2013 Information Security for South Africa, 1–6. https://doi.org/10.1109/ISSA.2013.6641062(2013).
[13] J. Price, S .L. Man, S. Bartlett, K. Taylor, M. Dinwoodie and P. Bowie Repeat prescribing of medications: A system-centred risk management model for primary care organisations. Journal of Evaluation in Clinical Practice, 23(4), 779–796. https://doi.org/10.1111/jep.12718(2017).
[14] T. Rhodes and A. Quirk. Drug users' sexual relationships and the social organisation of risk: The sexual relationship as a site of risk management. Social Science & Medicine, 46(2), 157–169. https://doi.org/10.1016/S0277-9536(97)00156-1(1998).
[15] I.Veljkovi and A. Budree. Development of Bring-Your-Own-Device Risk Management Model: A Case Study From a South African Organisation. Electronic Journal of Information Systems Evaluation, 22(1), 1–14. http://search.proquest.com/docview/2272758573/(2019).
[16] M.S. Mohsienuddin, Risk Management in Information Technology (June 9, 2020). Available at SSRN: https://ssrn.com/abstract=3625242 or http://dx.doi.org/10.2139/ssrn.3625242
[17] S.V. Dineshkumar, Management Information Systems: Mastering the Discreet Planning (June 23, 2020). International Journal for Research in Applied Science & Engineering Technology (IJRASET); ISSN: 2321-9653;Volume 8 Issue VI June 2020; http://doi.org/10.22214/ijraset.2020.6258. Available at SSRN: https://ssrn.com/abstract=
[18] Soni, Vishal Dineshkumar, Disaster Recovery Planning: Untapped Success Factor in an Organization (June 16, 2020). Available at SSRN: https://ssrn.com/abstract=3628630 or http://dx.doi.org/10.2139/ssrn.3628630



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY