IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 12, December 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

RISK MANAGEMENT

Dr. Krishna Kumar Verma

Assistant Professor, Faculty of Commerce, Swami Shukdevanand PG College, Shahjahanpur, MJP Rohilkhand University, Bareilly, Uttar Pradesh, India

ABSTRACT: Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events[1] or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in international markets, threats from project failures (at any phase in design, development, production, or sustaining of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.

There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities. Risk management standards have been developed by various institutions, including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards.[2][3][4] Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety. Certain risk management standards have been criticized for having no measurable improvement on risk, whereas the confidence in estimates and decisions seems to increase.[1]

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat. The opposite of these strategies can be used to respond to opportunities (uncertain future states with benefits).

I. INTRODUCTION

As a professional role, a Risk Manager[5] will "oversee the organization's comprehensive insurance and risk management program, assessing and identifying risks that could impede the reputation, safety, security, or financial success of the organization", and then develop plans to minimize and / or mitigate any negative (financial) outcomes. Risk Analysts [6] support the technical side of the organization's risk management approach: once risk data has been compiled and evaluated, analysts share their findings with their managers, who use those insights to decide among possible solutions. Risk management appears in scientific and management literature since the 1920s. It became a formal science in the 1950s, when articles and books with “risk management” in the title also appear in library searches.[7] Most of research was initially related to finance and insurance.

A widely used vocabulary for risk management is defined by ISO Guide 73:2009, "Risk management. Vocabulary."[2]

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first. Risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss, versus a risk with high loss but lower probability of occurrence can often be mishandled.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost-effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Opportunity cost represents a unique challenge for risk managers. It can be difficult to determine when to put resources toward risk management and when to use those resources elsewhere. Again, ideal risk management minimizes spending (or manpower or other resources) and also minimizes the negative effects of risks.

Risk is defined as the possibility that an event will occur that adversely affects the achievement of an objective. Uncertainty, therefore, is a key aspect of risk. Systems like the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM), can assist managers in mitigating risk factors. Each company may have different internal control components, which leads to different outcomes. For example, the framework for ERM components includes Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring.

Opportunities first appear in academic research or management books in the 1990s. The first PMBoK Project Management Body of Knowledge draft of 1987 doesn't mention opportunities at all.

Modern project management school does recognize the importance of opportunities. Opportunities have been included in project management literature since the 1990s, e.g. in PMBoK, and became a significant part of project risk management in the years 2000s,[8] when articles titled “opportunity management” also begin to appear in library searches. Opportunity management thus became an important part of risk management.

Modern risk management theory deals with any type of external events, positive and negative. Positive risks are called opportunities. Similarly to risks, opportunities have specific mitigation strategies: exploit, share, enhance, ignore.

In practice, risks are considered “usually negative”. Risk-related research and practice focus significantly more on threats than on opportunities. This can lead to negative phenomena such as target fixation[9]

II. DISCUSSION

For the most part, these methods consist of the following elements, performed, more or less, in the following order:

1. Identify the threats
2. Assess the vulnerability of critical assets to specific threats
3. Determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. Identify ways to reduce those risks
5. Prioritize risk reduction measures

The Risk management knowledge area, as defined by the Project Management Body of Knowledge PMBoK, consists of the following processes:

1. Plan Risk Management - defining how to conduct risk management activities.
2. Identify Risks - identifying individual project risks as well as sources.
3. Perform Qualitative Risk Analysis - prioritizing individual project risks by assessing probability and impact.
4. Perform Quantitative Risk Analysis - numerical analysis of the effects.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

5. Plan Risk Responses - developing options, selecting strategies and actions.
6. Implement Risk Responses - implementing agreed-upon risk response plans. In the 4th Ed. of PMBoK, this process was included as an activity in the Monitor and Control process, but was later separated as a distinct process in PMBoK 6th Ed.[10]
7. Monitor Risks - monitoring the implementation. This process was known as Monitor and Control in the previous PMBoK 4th Ed., when it also included the "Implement Risk Responses" process.

The International Organization for Standardization (ISO) identifies the following principles of risk management:[11]

Risk management should:

- Create value – resources expended to mitigate risk should be less than the consequence of inaction
- Be an integral part of organizational processes
- Be part of decision-making process
- Explicitly address uncertainty and assumptions
- Be a systematic and structured process
- Be based on the best available information
- Be tailorable
- Take human factors into account
- Be transparent and inclusive
- Be dynamic, iterative and responsive to change
- Be capable of continual improvement and enhancement
- Be continually or periodically re-assessed

Benoit Mandelbrot distinguished between "mild" and "wild" risk and argued that risk assessment and management must be fundamentally different for the two types of risk.[12] Mild risk follows normal or near-normal probability distributions, is subject to regression to the mean and the law of large numbers, and is therefore relatively predictable. Wild risk follows fat-tailed distributions, e.g., Pareto or power-law distributions, is subject to regression to the tail (infinite mean or variance, rendering the law of large numbers invalid or ineffective), and is therefore difficult or impossible to predict. A common error in risk assessment and management is to underestimate the wildness of risk, assuming risk to be mild when in fact it is wild, which must be avoided if risk assessment and management are to be valid and reliable, according to Mandelbrot.

III. RESULTS

According to the standard ISO 31000 - "Risk management – Principles and guidelines on implementation,"[3] the process of risk management consists of several steps as follows:

Establishing the context

This involves:

1. observing the context
   - the social scope of risk management
   - the identity and objectives of stakeholders
   - the basis upon which risks will be evaluated, constraints.
2. defining a framework for the activity and an agenda for identification
3. developing an analysis of risks involved in the process
4. mitigation or solution of risks using available technological, human and organizational resources

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of problems and those of competitors (benefit), or with the problem's consequences.

- Source analysis[13] – Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed).

- Some examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport. Problem analysis– Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; lightning striking an aircraft during takeoff may make all people on board immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

- Objectives-based risk identification– Organizations and project teams have objectives. Any event that may prevent an objective from being achieved is identified as risk.
- Scenario-based risk identification – In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk – see Futures Studies for methodology used by Futurists.
- Taxonomy-based risk identification – The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.[14]
- Common-risk checking[15] – In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.[16]
- Risk charting[17] – This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about.

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of an unlikely event, the probability of occurrence of which is unknown. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the risk management plan.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

Even a short-term positive improvement can have long-term negative impacts. Take the "turnpike" example. A highway is widened to allow more traffic. More traffic capacity leads to greater development in the areas surrounding the improved traffic capacity. Over time, traffic thereby increases to fill available capacity. Turnpikes thereby need to be expanded in a seemingly endless cycles. There are many other engineering examples where expanded capacity (to do any function) is soon filled by increased demand. Since expansion comes at a cost, the resulting growth could become unsustainable without forecasting and management.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents and is particularly scanty in the case of catastrophic events, simply because of their infrequency. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for senior executives of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized within overall company goals. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is: "Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude."

IV. CONCLUSIONS

Select appropriate controls or countermeasures to mitigate each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions. There are four basic steps of risk management plan, which are threat assessment, vulnerability assessment, impact assessment and risk mitigation strategy development. [24]

According to ISO/IEC 27001, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why.

For medical devices, risk management is a process for identifying, evaluating and mitigating risks associated with harm to people and damage to property or the environment. Risk management is an integral part of medical device design and development, production processes and evaluation of field experience, and is applicable to all types of medical devices. The evidence of its application is required by most regulatory bodies such as the US FDA. The management of risks for medical devices is described by the International Organization for Standardization (ISO) in ISO 14971:2019, Medical Devices—The application of risk management to medical devices, a product safety standard. The standard provides a process framework and associated requirements for management responsibilities, risk analysis and evaluation, risk controls and lifecycle risk management. Guidance on the application of the standard is available via ISO/TR 24971:2020.

The European version of the risk management standard was updated in 2009 and again in 2012 to refer to the Medical Devices Directive (MDD) and Active Implantable Medical Device Directive (AIMDD) revision in 2007, as well as the In Vitro Medical Device Directive (IVDD). The requirements of EN 14971:2012 are nearly identical to ISO 14971:2007. The differences include three "(informative)" Z Annexes that refer to the new MDD, AIMDD, and IVDD. These annexes indicate content deviations that include the requirement for risks to be reduced as far as possible, and the requirement that risks be mitigated by design and not by labeling on the medical device (i.e., labeling can no longer be used to mitigate risk).

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

Typical risk analysis and evaluation techniques adopted by the medical device industry include hazard analysis, fault tree analysis (FTA), failure mode and effects analysis (FMEA), hazard and operability study (HAZOP), and risk traceability analysis for ensuring risk controls are implemented and effective (i.e. tracking risks identified to product requirements, design specifications, verification and validation results etc.). FTA analysis requires diagramming software. FMEA analysis can be done using a spreadsheet program. There are also integrated medical device risk management solutions.

Through a draft guidance, the FDA has introduced another method named "Safety Assurance Case" for medical device safety assurance analysis. The safety assurance case is structured argument reasoning about systems appropriate for scientists and engineers, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment. With the guidance, a safety assurance case is expected for safety critical devices (e.g. infusion devices) as part of the pre-market clearance submission, e.g. 510(k). In 2013, the FDA introduced another draft guidance expecting medical device manufacturers to submit cybersecurity risk analysis information.

REFERENCES

1. Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46.
2. ^ ISO/IEC Guide 73:2009 (2009). Risk management — Vocabulary. International Organization for Standardization.
3. ^ ISO/DIS 31000 (2018). Risk management — Principles and guidelines on implementation. International Organization for Standardization.
4. ^ ISO 31000:2018 - Risk management - A Practical Guide (1 ed.). ISO, UNIDO. 2021. ISBN 978-92-67-11233-6. Retrieved 17 December 2021.
5. ^ "Risk Manager" Society for Human Resource Management
6. ^ "What Are Risk Analysts & Risk Managers?", CFA Institute
7. ^ Dionne, Georges (2013). "Risk Management: History, Definition, and Critique: Risk Management". Risk Management and Insurance Review. 16 (2): 147–166. doi:10.1111/rmir.12016. S2CID 154679294.
8. ^ "The ascent of risk". www.pmi.org. Retrieved 2021-12-13.
9. ^ "Target fixation in risk management. Arguments for the bright side of risk". Stefan Morcov. 2021. Retrieved 2021-12-13.
10. ^ Morcov, Stefan (2021). Managing Positive and Negative Complexity: Design and Validation of an IT Project Complexity Management Framework. KU Leuven University. Available at https://lirias.kuleuven.be/retrieve/637007
11. ^ "Committee Draft of ISO 31000 Risk management" (PDF). International Organization for Standardization. 2007-06-15. Archived from the original (PDF) on 2009-03-25.
12. ^ Mandelbrot, Benoit and Richard L. Hudson (2008). The (mis)Behaviour of Markets: A Fractal View of Risk, Ruin and Reward. London: Profile Books. ISBN 9781846682629.
13. ^ "Risk Identification" (PDF). Comunidad de Madrid. p. 3.
14. ^ CMU/SEI-93-TR-6 Taxonomy-based risk identification in software industry. Sei.cmu.edu. Retrieved on 2012-04-17.
15. ^ "Risk Management Systems Checklist (Common Items)" (PDF). www.fsa.go.jpn.
16. ^ Common Vulnerability and Exposures list. Cve.mitre.org. Retrieved on 2012-04-17.
17. ^ Crockford, Neil (1986). An Introduction to Risk Management (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2.
18. ^ "CRISC Exam Questions". Retrieved 23 Feb 2018.
19. ^ Dorfman, Mark S. (2007). Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 978-0-13-224227-1.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 12, December 2022||

| DOI:10.15680/IJIRSET.2022.1112010 |

20. ^ McGivern, Gerry; Fischer, Michael D. (1 February 2012). "Reactivity and reactions to regulatory transparency in medicine, psychotherapy and counseling" (PDF). Social Science & Medicine. 74 (3): 289–296. doi:10.1016/j.socscimed.2011.09.035. PMID 22104085. Archived from the original (PDF) on 21 April 2018. Retrieved 20 April 2018.
21. ^ IADC HSE Case Guidelines for Mobile Offshore Drilling Units 3.2, section 4.7
22. ^ Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk". Business Trends Quarterly.
23. ^ Shashi; Centobelli, Piera; Cerchione, Roberto; Ertz, Myriam (2020). "Managing supply chain resilience to pursue business and environmental strategies". Business Strategy and the Environment. 29 (3): 1215–1246. doi:10.1002/bse.2428. ISSN 0964-4733. S2CID 213432044.
24. ^ Snedaker, Susan (2014). Business continuity and disaster recovery planning for IT professionals. Chris Rima (2nd ed.). Waltham, MA: Syngress. ISBN 1-299-85332-3. OCLC 858657442.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details