International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-10, Special Issue-12, December-2022
Innovative Projects 2022
Organized by Presidency University, Bangalore, India

A Brief Discussion on Risk Management

Mr. Ashok Bhat
Assistant Professor, Masters In Business Administration, Presidency University, Bangalore, India,
Email Id-ashokbhat@presidencyuniversity.in

ABSTRACT:

System engineering relies heavily on risk management to ensure the effective design, implementation, and operation of complex systems. The relevance, fundamental ideas, and practical tactics of risk management in system engineering are highlighted in this abstract. It presents the fundamental ideas behind system engineering risk management. It focuses on the significance of early stakeholder involvement, distinct risk goals, and the development of an iterative risk management approach. In order to achieve a comprehensive and organised approach, it also emphasises the integration of risk management with other system engineering activities. It emphasises the importance of risk documentation and communication throughout the system engineering process. It emphasises the need of informing stakeholders on risks, possible effects, and mitigation strategies in order to facilitate informed decision-making and uphold openness. It gives a general review of risk management in system engineering and emphasises its significance, fundamental ideas, and successful tactics. It acts as a starting point for further study and the effective use of risk management procedures to enable the successful creation and operation of complex systems.

KEYWORDS:

Mitigation, Risk Hierarchy, Risk Management, Risk Planning.

I. INTRODUCTION

Identifying, evaluating, and managing risks related to the creation, adoption, and usage of complex systems is the subject of risk management, a crucial part of system engineering. It is a methodical procedure that aids stakeholders and project managers in proactively addressing possible risks and uncertainties that may affect a system's performance. Risks in system engineering may come from a variety of places, including technological difficulties, resource shortages, time restraints, shifting requirements, outside causes, and human factors. If these risks are not appropriately managed, they might result in project failure as a whole, as well as delays, cost overruns, performance problems, safety concerns, and other problems [1], [2].

By putting in place suitable methods and mitigation mechanisms, risk management in system engineering aims to reduce the probability and effect of hazards. Risk identification, risk assessment, risk prioritisation, risk mitigation planning, and risk monitoring and control are some of the phases involved in this process. Systematically identifying and recording any hazards that could have an impact on the system is known as risk identification. The system's needs, design, interfaces, dependencies, and external influences are examined to achieve this. Risks are ranked and categorised according to their seriousness, chance of happening, and possible consequences.

In order to evaluate risks, they must be thoroughly examined, along with any possible repercussions and chance of occurrence. Understanding the system's entire risk exposure and prioritising hazards for mitigation are made easier as a result. Planning for risk reduction entails creating strategies and activities to minimise or eliminate recognised hazards. This can include making design modifications, carrying out more testing and validation, creating backup plans, or obtaining more resources. The objective is to manage risks proactively to minimise any possible negative effects [3], [4].

Continuous monitoring and evaluation of the efficacy of risk mitigation measures are part of risk monitoring and control. To make sure risks are adequately handled and that new risks are found and managed as they materialise, regular assessments are carried out. Overall, risk management in system engineering is essential to the efficient design, implementation, and operation of complex systems. System engineers may prevent problems, reduce interruptions, and enhance project results by methodically identifying, evaluating, and managing risks. Throughout the system's lifespan, effective risk management adds to the system's overall dependability, safety, and success.

II. DISCUSSION

Risk as Reality

There is risk involved with any activity. It is a typical state of affairs. Risk is the possibility of a bad future reality, which may or may not occur. The terms "risk" and "consequences of occurrence" describe two aspects of a potential adverse future event: likelihood of occurrence (if something will occur) and "how catastrophic if it occurs." If the likelihood of an event is unknown, there is ambiguity and no clear danger. Risk itself is not an issue. It is an awareness of the gravity of the danger posed by possible issues. A consequence that has already happened is a problem [5], [6].

In reality, being aware of a danger gives you the chance to take preventative measures. Risk exists whether or not efforts are made to control it. Risk exists whether or not you admit it, accept it as true, believe it, have it in writing, or comprehend it. Because you expect it to, dismiss it, or your boss's expectations don't take it into account, risk does not alter. It also won't alter just because it runs counter to a rule, method, or policy. There is no good or bad risk. It's just the way things are. Risk goes hand in hand with advancement and opportunity. Risks must be comprehended, controlled, and decreased to acceptable levels in order to advance [7], [8].

Types of Risk in a Systems Engineering Environment

Risks associated with systems engineering management may be connected to the system's end products or to the system's development process. Figure 1 depicts how system development risks are broken down. Risks connected to the system development may often be traced back to meeting client needs throughout the life cycle. Product risks encompass both end product risks, which pertain to the system's fundamental functionality and cost, and enabling product risks, which relate to the items used in the system's manufacture, upkeep, maintenance, testing, training, and disposal.

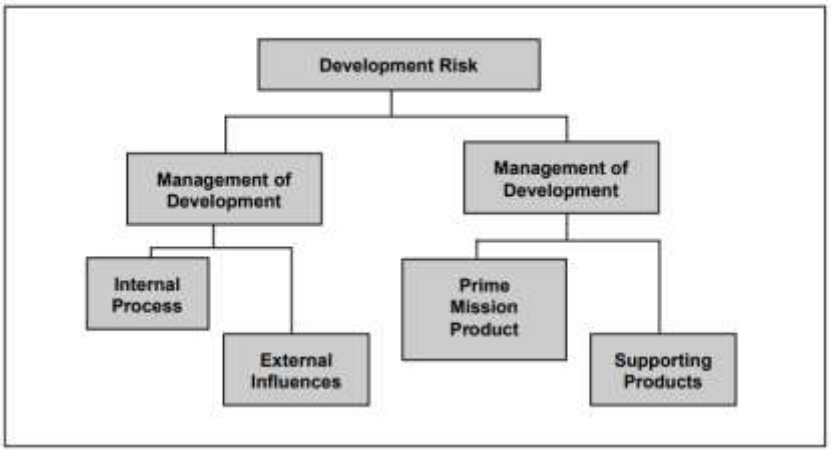

Figure 1: Risk Hierarchy [ocw.mit.edu].

Figure 2: Four Elements of Risk Management [ocw.mit.edu].

Technical management risks and risks brought on by outside forces are both risks related to managing the development effort. Schedules, resources, work flow, on-time deliveries, the availability of qualified staff, possible bottlenecks, critical path activities, and similar risks include those relating to internal technical management. Risks associated with external influences include those related to resource availability, greater delegation of responsibility, programme visibility, regulatory requirements, and similar factors. An organised approach to recognising and evaluating risk as well as choosing, creating, and putting into practice solutions for risk handling is risk management. It is a procedure, not a succession of things. Planning for risk management is essential, as are early risk detection and analysis, ongoing risk monitoring and reevaluation, prompt execution of remedial measures, communication, documentation, and collaboration [9], [10].

Although there are other methods to organise risk management, the four sections of planning, assessment, handling, and monitoring will be used in this book. As shown in Figure 2, all of the components are interlocked to show that after initial planning, the components start to rely on one another. Figure 3 depicts the crucial control and feedback links in the process to exemplify this.

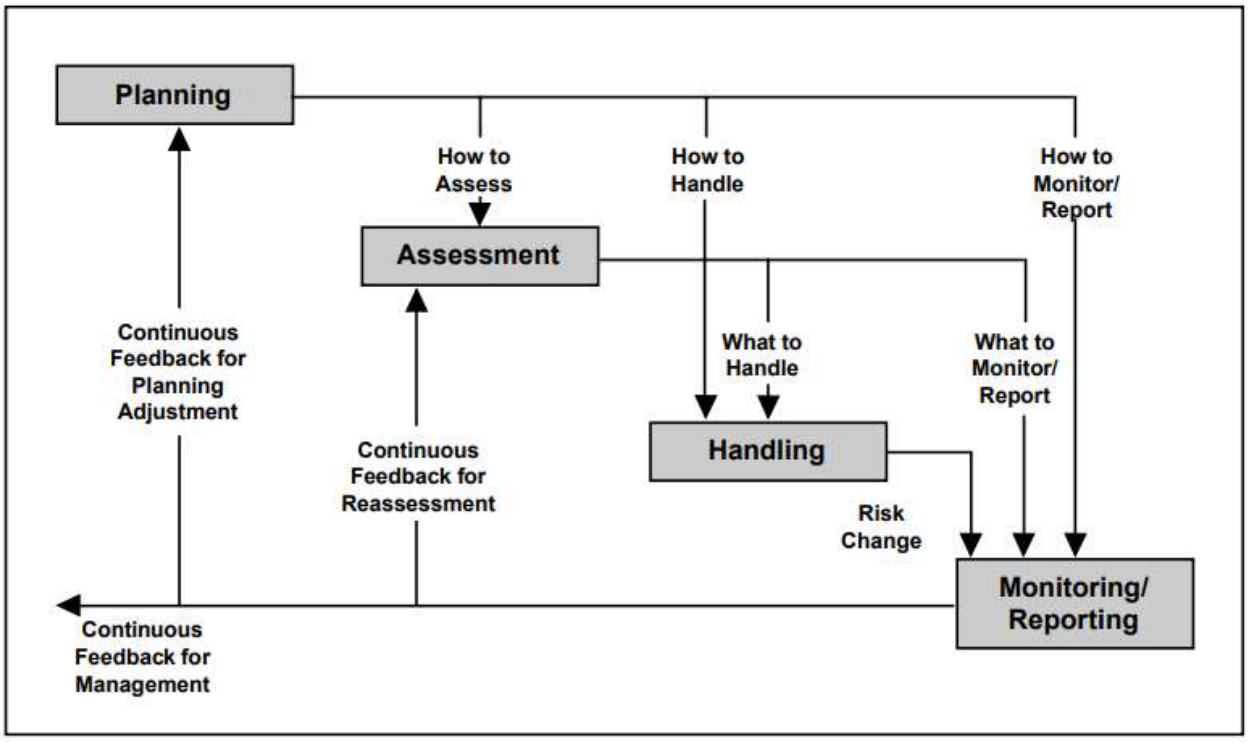

Figure 3: Risk Management Control and Feedback [ocw.mit.edu].

Risk Planning

The ongoing process of creating a structured, all-inclusive approach to risk management is known as risk planning. A strategy, goals, and objectives, planning assessment, handling, and monitoring activities, identifying resources, tasks, and responsibilities, organising and training risk management IPT members, establishing a method to track risk items, and establishing a method to continuously document and disseminate information are all included in the initial planning.

Risk Assessment

The process of risk assessment includes locating and evaluating the hazards connected to the system's life cycle.

Risk Identification Activities

Activities for identifying hazards determine whether dangers are of concern. These actions consist of:

1. Determining the causes and drivers of risk and uncertainty,
2. Turning risk from uncertainty,
3. Calculating risk,
4. Determining likelihood, and
5. Setting the risk items' priority.

The first identification procedure begins with the identification of prospective risk items in each of the four risk categories, as indicated by Figure 4. Risks connected to the functionality of the system and its auxiliary products are often categorised by WBS and originally identified via professional evaluation of the teams and people working on the project. These dangers often call for a further quantitative evaluation. Risks related to internal processes and external influences are likewise evaluated by enterprise-wide experts and identified using risk area templates similar to those described in DoD 4245.7-M. The DoD 4245.7-M templates outline the potential risks involved in system acquisition management procedures and provide strategies for lowering conventional hazards in each one. Based on advice from experts, these templates should be modified for usage with certain programmes.

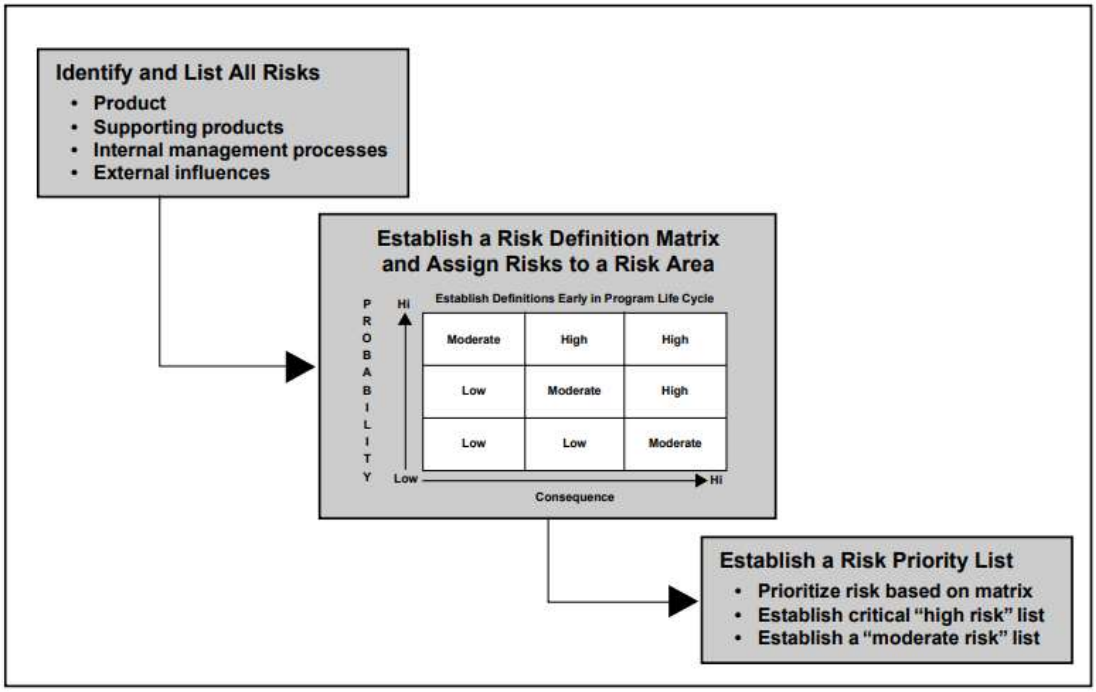

Figure 4: Illustrate the Initial Risk Identification.

The risk level should be set when the risk items have been identified. Use of a matrix, like the one in Figure 5, is one typical technique. To determine the relative risk between each item and each block in the matrix, an association is made. Risk grows diagonally on such a graph, offering a mechanism for determining relative risk. A priority list may be created and risk analysis can start after the relative risk has been determined.

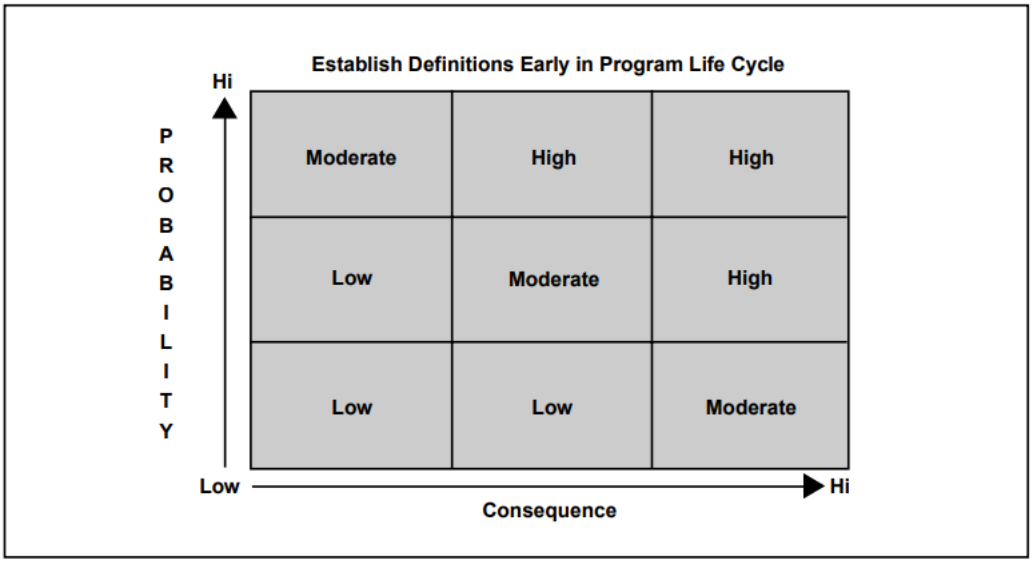

Figure 5: Illustrate the Simple Risk Matrix.

Activities that assist identify the likelihood or effects of a risk item may also be included in risk identification efforts. For example:

1. Tests and analysis to remove uncertainty,
2. Conducting tests to determine consequences and likelihood, and
3. Activities that quantify risk when high, moderate, and low estimates' qualitative character is inadequate for a proper comprehension.

III. CONCLUSION

In conclusion, proactive risk identification, evaluation, mitigation, and monitoring throughout the lifespan of the system are made possible by risk management, a crucial component of system engineering. The goals, performance, schedule, and budget of the system are among the things that risk management seeks to reduce the possible negative effects of uncertainties and threats on. System engineers can efficiently identify and analyse possible risks, prioritise them based on their impact and probability, and create effective risk mitigation methods by using a systematic and organised approach to risk management. This proactive method enables early risk assessment and mitigation, decreasing the possibility of expensive interruptions or breakdowns.

By giving a thorough awareness of the possible risks and their consequences, risk management also makes it easier to make well-informed decisions. It enables project managers and stakeholders to make well-informed choices and prioritise risk mitigation efforts by assisting them in assessing the trade-offs between risk, cost, schedule, and performance. In conclusion, risk management is a crucial step in the design of systems that permits the detection, evaluation, reduction, and monitoring of risks during the course of the system's lifespan. System engineers may reduce the potential negative effects of uncertainties and threats, encourage informed decision-making, improve cooperation, and raise the system's overall resilience and success by putting good risk management practices into practice.

REFERENCES

[1] R. V. Dandage, S. S. Mantha, S. B. Rane, and V. Bhoola, “Analysis of interactions among barriers in project risk management,” J. Ind. Eng. Int., 2018, doi: 10.1007/s40092-017-0215-9.

[2] A. Susanto and Meiryani, “The importance of risk management in an organizations,” Int. J. Sci. Technol. Res., 2018.

[3] G. Behzadi, M. J. O’Sullivan, T. L. Olsen, and A. Zhang, “Agribusiness supply chain risk management: A review of quantitative decision models,” Omega (United Kingdom). 2018. doi: 10.1016/j.omega.2017.07.005.

[4] B. P. Weeserik and M. Spruit, “Improving Operational Risk Management using Business Performance Management technologies,” Sustain., 2018, doi: 10.3390/su10030640.

[5] D. Friday, S. Ryan, R. Sridharan, and D. Collins, “Collaborative risk management: a systematic literature review,” International Journal of Physical Distribution and Logistics Management. 2018. doi: 10.1108/IJPDLM-01-2017-0035.

[6] J. Schulte and S. I. Hallstedt, “Company risk management in light of the sustainability transition,” Sustain., 2018, doi: 10.3390/su10114137.

[7] Z. Hong, C. K. M. Lee, and L. Zhang, “Procurement risk management under uncertainty: a review,” Industrial Management and Data Systems. 2018. doi: 10.1108/IMDS-10-2017-0469.

[8] B. Baharuddin and M. M. Yusof, “Evaluation of risk management practices in information systems project in the public sector,” J. Pengur., 2018, doi: 10.17576/pengurusan-2018-52-03.

[9] K. Eyvindson and A. Kangas, “Guidelines for risk management in forest planning — What is risk and when is risk management useful?,” Canadian Journal of Forest Research. 2018. doi: 10.1139/cjfr-2017-0251.

[10] S. Annamalah, M. Raman, G. Marthandan, and A. K. Logeswaran, “Implementation of Enterprise Risk Management (ERM) framework in enhancing business performances in oil and gas sector,” Economies, 2018, doi: 10.3390/economies6010004.