Comprehensive Framework Of Project Risk Management Based On ISO 31000

Arief Rahmana

Universitas Widyatama, Bandung, Indonesia
Jl. Cikutra No. 204 A, Bandung, Indonesia
arief.rahmana@widyatama.ac.id

Abstract. This paper provides a comprehensive framework of project risk management as guidance for managing a project risk – to know, evaluate, control, minimize a project risk. We proposed a framework project risk management based on International Standardization Organization (ISO) 31000. Project risk management has been implemented in various project over the world, including Indonesia. We believed that project risk management is comprehensive approach for project to get better performances in predicting unintended event in the future. Comprehensive project risk management involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing context and assessing, treating, monitoring, reviewing, recording and reporting risk. Finally, this framework will ensure that project risk management is a part of all activities in the organization for designing, monitoring, reviewing, and continually improving project risk.

Keywords: Comprehensive Framework, Project Risk, ISO 31000

1 Introduction

Project Management (PM) is described as the use of knowledge, skills, tools, and techniques to project activities in order to meet project requirements. Since a project is defined as "a temporary endeavor undertaken to create a unique product, service, or result [1] [2]. PM techniques are applicable in complex, multidisciplinary settings. There are ten key areas of project management: project integration management, scope management, time management, cost management, quality management, resource management, stakeholder management, communication management, procurement management, and risk management [1]. In particular, risk management emphasizes the importance of identifying, analyzing, and responding to project risks promptly to ensure the project's success.

Project risk is defined as “an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, or quality [1] [3]. Risk management in projects involves a logical sequence of actions taken by decision-makers to maintain project execution under controlled conditions [4]. Decision-makers must identify, analyze, and evaluate risks throughout the

V. Mardiansyah and B. A. Prasetyo (eds.), *Proceedings of the Widyatama International Conference on Engineering 2024 (WICOENG 2024)*, Advances in Engineering Research 252,
https://doi.org/10.2991/978-94-6463-618-5_6

project life cycle and utilize their organizational structures and administrative practices to address risks in a way that benefits the project [5].

Every project carries risk, and one of the key responsibilities of project management is to minimize, if not eliminate, these risks [6]. Risks can be either manmade or natural, and their impacts can be devastating, highlighting the need for effective measures to address them. However, many existing risk mitigation strategies have proven to be ineffective in various ways. Over the years, numerous tools have been developed to help project managers manage risks. ISO 31000, Risk Management – Guidelines, offers principles, a framework, and a process for managing risk. It can be applied by organizations of any size, industry, or sector. Utilizing ISO 31000 helps organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and optimize the allocation of resources for risk treatment. In an uncertain world, ISO 31000 provides clear guidance on effective risk management for any organization [7].

This paper shows extensively show of the comprehensive framework on project risk management based on ISO 31000. The primary goal of this paper is to provide the way in risk identification, analysis and respond, that is mostly in use, in other to clarify the different groups of risk sources.

2 Risk Project Management Based on ISO 31000

ISO 31000 standard is intended to help organizations to manage in a systematic and comprehensive manner diverse types of risk by offering a universal framework to assist the organization to integrate risk management into its overall management system [8]. It details a holistic method for identifying, analyzing, assessing, addressing, monitoring, and communicating risks throughout an organization. According to [9], the benefits of ISO 31000 are (a) principles, framework, and processes for managing risk in a structured way, (b) guidelines for applying risk management techniques, (c) methods to adapt risk management to fit any organization, (d) standards for tracking, evaluating, and continuously enhancing risk management efforts, and (e) a basis for embedding risk management across the organization. A systematic approach to risk management communicates to stakeholders, including investors and customers, that the organization is well-equipped to handle uncertainties, thereby strengthening trust and credibility.

Project risk management is the process of identifying, analyzing, and responding to potential risks that may arise during the execution of a project to ensure it continues smoothly and achieves its objectives [10]. Project risks are typically reactive, meaning that responses need to be swift in order to find the best solutions for addressing the risks at hand. Project risk management is crucial because it reduces the likelihood of failure and increases the chances of success in a project. With project risk management, a project manager can minimize the risk of losses that could lead to project failure [11]. Here are several reasons why project risk management is important: (a) helps reduce the risk

of project failure, (b) improves project efficiency, (c) enhances product quality, (d) prevents budget overruns, and (e) increases stakeholder confidence. The following Fig. 1 used as a framework to identify, analyze, evaluate, and respond to project risks.

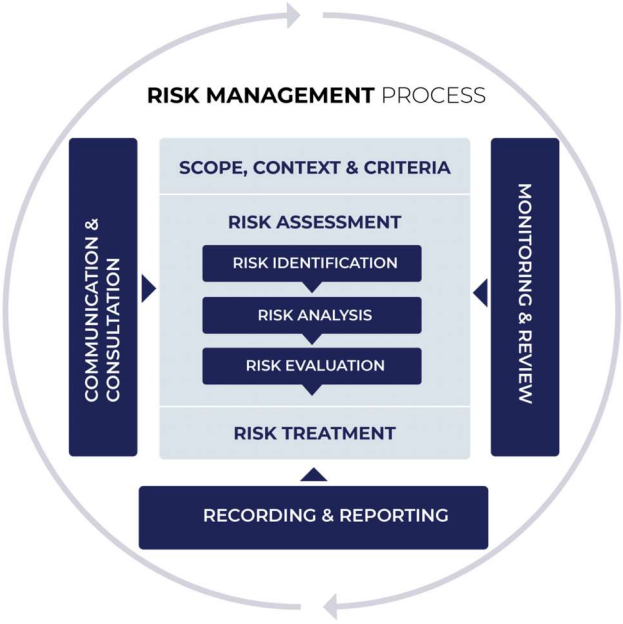

Fig.1. Project risk framework based on ISO 31000

Based on Fig. 1 depicted, here are the steps for project risk management based on ISO 31000

2.1 Establishing the Context

The purpose of context setting is to identify and clarify the organization's objectives, the environment in which these objectives are to be achieved, the relevant stakeholders, and the diverse risk criteria. These elements help to reveal and assess the nature and complexity of the risks involved. There are four key contexts that need to be determined during context setting: the internal context, external context, risk management context, and risk criteria.

a. The internal context focuses on the internal aspects of the organization, including its organizational structure, culture, and other factors that can influence the achievement of organizational goals.
b. The external context defines the external aspects of the organization, such as competitors, authorities, technological developments, and other factors that can affect the achievement of organizational objectives.

c. The risk management context considers how risk management is implemented and how it will be applied in the future.
d. Lastly, in the establishment of organizational risk management, it is essential to define agreed-upon parameters to be used as risk criteria.

2.2 Risk Assessment

Risk assessment consists of:
a. Risk identification: identifying potential risks that may affect the achievement of organizational objectives.
b. Risk analysis: analyzing the likelihood and impact of the identified risks.
c. Risk evaluation: comparing the results of the risk analysis with risk criteria to determine the appropriate risk management measures to be applied

Risk Identification

A process that is systematically and continuously carried out to identify the potential occurrence of risks or losses to the company's assets, liabilities, and personnel. There are many kinds of methods to identify project risk i.e. brainstorming, delphi method, risk assessment workshop, incident investigation, inspection, checklist, risk breakdown structure, in depth interview, and document review. Risk register is the output of project risk identification. Risk register is a document that contains the results of risk identification and other risk management processes [12]. As risk management activities are carried out, the risk register is continually updated with new information over time. The format for creating a risk register is presented in the following Table 1.

Table 1. Format for project risk register

No	Project Risk	Root Cause	Effect
List of Number	List all potential project risks that may occur	Write down the root causes of the risks.	Write down the effect of the risks

Risk Analysis

Risk analysis is assessing the likelihood of an adverse event occurring that may negatively affect a business, investment, or project. Quantitative Analysis use numerical methods to estimate the probability and impact of risks (e.g., statistical analysis, modeling). Meanwhile qualitative approach is the process involves determining: (a) the impact (consequences or severity) and (b) the likelihood (frequency or probability) of the risks that may occur. Severity refers to the extent or intensity of an event's impact on the process output. Likelihood refers to the probability of a risk occurring within a given time period. A common method used to calculate likelihood is frequency. Severity consist of five levels is presented following Table 2, meanwhile likelihood also consist of five levels is presented following Table 3.

Table 2. Severity level

Level	Defining	Example	
1	Insignificant	Cost	: insignificant cost increase
		Time	: insignificant schedule slippage
		Quality	: quality degradation barely noticeable
2	Minor	Cost	: < 5% cost increase
		Time	: overall project slippage < 5%
		Quality	: only very demanding application are affected
3	Moderate	Cost	: 5 – 10 % cost increase
		Time	: overall project slippage 5 – 10%
		Quality	: quality reduction requires client approval
4	Major	Cost	: 10 – 20% cost increase
		Time	: overall project slippage 10 – 20%
		Quality	: quality reduction unacceptable to the client
5	Catastrophic	Cost	: > 20% cost increase
		Time	: overall project slippage > 20%
		Quality	: project end item is effectively unusable

Table 3. Likelihood level

Level	Defining	Example
1	Rare	It can happen every month
2	Unlikely	It can happen several times a year
3	Moderate	It can occur every 1 to 2 years
4	Likely	It can occur every 3 to 5 years.
5	Almost Certain	It can occur more than once every 5 years

Risk Evaluation

Risk evaluation is the determination of risk levels and risk priorities. The risk level is the multiplication of severity and likelihood. The lowest risk level is valued at 1, while the highest is valued at 25. The result of the risk evaluation is the risk map or risk grading matrix (Fig. 1) and risk priority. Generally, the risk map is a graphical representation of risk events based on the levels of impact and likelihood within a specific business unit, while risk priority is the ranking of risks that need to be addressed immediately. Prioritizing risks based on the magnitude of the risk is done with the following provisions:

a. The highest magnitude of risk receives the highest priority.
b. If there is more than one risk with the same magnitude, the risk priority is determined based on the order of impact areas from highest to lowest according to impact criteria.

c. If there are still multiple risks with the same magnitude and impact area, the priority is determined based on the order of risk categories from highest to lowest according to risk categories.
d. If there are still multiple risks with the same magnitude, impact area, and category, the priority is determined based on the judgment of the risk owner

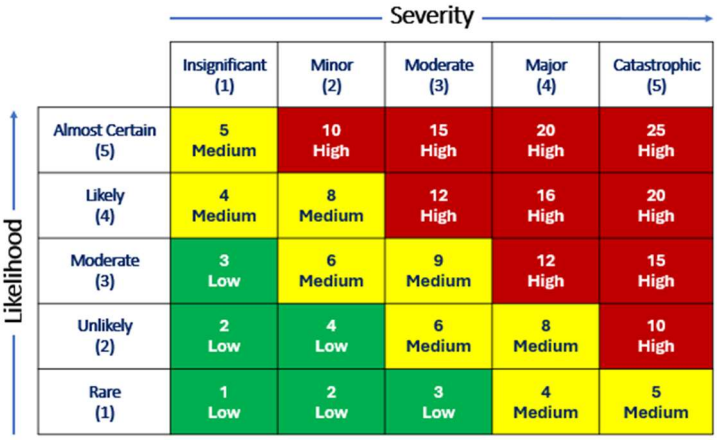

Fig. 2. Risk map or risk grading matrix

Based on Fig. 2, the risk levels are categorized into three levels: low, medium, and high. The low level falls within the range of values from 1 to 4, the medium level is within the range of values from 4 to 9, and the high level falls within the range of values from 10 to 25.

2.3 Risk Treatment

The best way to handle potential risk events is through risk treatment. It involves managing potential risks in accordance with the risk mitigation action plan outlined in the risk register. The framework of project risk treatment depicted in Fig. 3. There are four types of risk treatment:

a. Avoid is avoiding risk by not engaging in activities or stopping activities that increase risk.
b. Mitigate is reducing the likelihood and/or impact of a risk.
c. Transfer is sharing the risk with another party.
d. Accept is accepting the risk (within the risk tolerance) and maintaining it so that it does not escalate to a higher level.

Avoid can be applied when the risk is in a condition of high likelihood and high severity. Mitigate can be applied when the risk is in a condition of low likelihood and high severity. Transfer can be applied when the risk is in a condition of high likelihood

and low severity. Accept can be applied when the risk is in a condition of low likelihood and low severity.

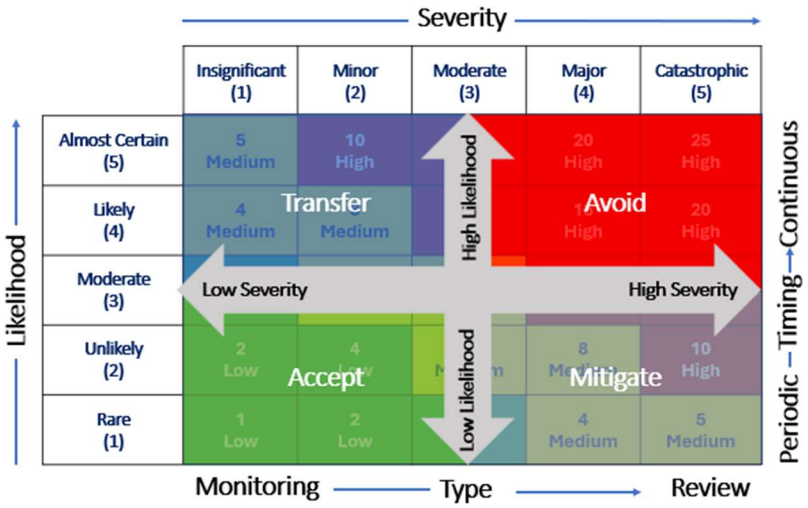

Fig. 3. Type of risk treatment

2.4 Monitoring and Review

Monitoring and review are carried out in the form of a reassessment of the implementation of risk management. The review focuses on:

a. The methods, assumptions, and variables used to measure risk.
b. The comparison between risk measurement results obtained from simulations/projections and actual outcomes.
c. The consistency in language among risk takers in terms of understanding, identifying, and measuring risk.

The implementation of the risk action plan requires regular monitoring and review of its progress. During the monitoring and review process, new risks may be identified that need immediate action, and it should be assessed whether any risks should be removed from the risk register

2.5 Communication and Consultation

Communication and consultation involve a two-way dialogue among stakeholders, with efforts focused on consultation. Effective internal and external communication is crucial to ensure that those responsible for implementing risk management, as well as other relevant parties, understand the basis for decision-making and why certain actions are necessary

2.6 Recording and Reporting

Recording and reporting in risk management are critical components that ensure transparency, accountability, and informed decision-making throughout the risk management process. Recording involves documenting all relevant information related to the identification, assessment, and treatment of risks. Proper documentation is essential for tracking risks over time and ensuring consistent application of risk management practices. Reporting involves communicating risk-related information to relevant stakeholders in a clear and timely manner, enabling appropriate risk responses.

3 Conclusion

Effective project risk management is essential for the successful delivery of projects across all industries. Project risk management is not just a compliance activity but a critical component of successful project execution. By adopting a proactive, structured approach to identifying and managing risks, organizations can significantly improve their project outcomes and foster a culture of continuous improvement. A comprehensive framework for effective project risk management based on ISO 31000, emphasizing the importance of integrating risk management into organizational processes. Adhering to ISO 31000 principles not only enhances the effectiveness of project risk management but also contributes to the overall resilience and success of the organization. It encourages a culture of continuous improvement and proactive risk management, aligning risk practices with organizational goals and stakeholder expectations.

References

[1] PMI, “PMBOK Guide 6 edition,” *Pmi*, p. 168, 2017, [Online]. Available: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

[2] A. Rahmana, “Framework of project quality management.,” *Cent. Asia Caucasus*, vol. 23, no. 1, 2022.

[3] P. Rehacek, “Risk management in construction projects,” *J. Eng. Appl. Sci.*, vol. 12, no. 20, pp. 5347–5352, 2017, doi: 10.3923/jeasci.2017.5347.5352.

[4] S. Bushuyev and K. Pilyugina, “Value-oriented proactive management in high-tech project teams,” *Manag. Dev. Complex Syst.*, no. 53, pp. 5–15, 2023, doi: 10.32347/2412-9933.2023.53.5-15.

[5] L. H. Rodrigues-da-Silva and J. A. Crispim, “The Project Risk Management Process, a Preliminary Study,” *Procedia Technol.*, vol. 16, pp. 943–949, 2014, doi: 10.1016/j.protcy.2014.10.047.

[6] Y. Zou, A. Kiviniemi, and S. W. Jones, “A review of risk management through BIM and BIM-related technologies,” *Saf. Sci.*, vol. 97, pp. 88–98, 2017, doi: 10.1016/j.ssci.2015.12.027.

[7] D. Makajić-Nikolić, “ISO 31000: Risk Management Guidelines,” in *Encyclopedia of Sustainable Management*, 2023, pp. 2078–2080. doi: 10.1007/978-3-031-25984-5_314.

[8] C. Lalonde and O. Boiral, “Managing risks through ISO 31000: A critical analysis,” *Risk Manag.*, vol. 14, no. 4, pp. 272–300, 2012, doi: 10.1057/rm.2012.9.

[9] D. W. Wilbanks and T. Byrd, “The Relevance & Benefit of ISO 31000 to OSH Practice,” *Prof. Saf.*, vol. 65, no. 10, pp. 32–38, 2020, [Online]. Available: https://ezp.lib.cam.ac.uk/login?url=https://www.proquest.com/scholarly-journals/relevance-amp-benefit-iso-31000-osh-practice/docview/2448438011/se-2?accountid=9851%0Ahttps://libkey.io/libraries/603/openurl?genre=article&au=Wilbanks%2C+David+W%3BByrd%2C+Trac

[10] M. D. Nguyen, P. Q. Tran, and H. B. Nguyen, “An Application of Analytic Network Process (ANP) to Assess Critical Risks of Bridge Projects in the Mekong Delta Region,” *Eng. Technol. Appl. Sci. Res.*, vol. 13, no. 3, pp. 10622–10629, 2023, doi: 10.48084/etasr.5802.

[11] M. AL Jarrah, B. Jarah, and I. Altarawneh, “Toward successful project implementation: Integration between project management processes and project risk management,” *Probl. Perspect. Manag.*, vol. 20, no. 3, pp. 258–273, 2022, doi: 10.21511/ppm.20(3).2022.21.

[12] J. Uzulans, “The project risk registers analysis based of the project risk management notion ‘risk register’.,” *Proj. Manag. Dev. - Pract. Perspect.*, pp. 79–88, 2019, [Online]. Available: https://bd.univalle.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=136233995&lang=es&site=eds-live