Closing the Risk Communication Gap Between Executives and Project Managers: A Standards-Based Approach[1]

Ayman Sadek PMP, RMP, PBA

Abstract

With over 25 years of practical experience, primarily in executive management, I have found that the most common obstacles organizations face are problems arising from unforeseen or uncertain events. This stems from a lack of understanding of the concept of risk management. Consequently, risk management has become a core discipline for organizations striving to achieve their goals in increasingly complex and uncertain environments. Executives often encounter conflicts with project managers, site managers, and function managers due to a lack of familiarity with appropriate risk responses when implementing organizational strategy, whether through launched projects, management changes, or system modifications. This paper aims to examine the principles and practices of key risk management objectives, in accordance with international standards such as ISO 31000:2018 and ISO 31010:2019, as well as the PMI PMBOK Guide. This paper highlights specific objectives that all executive management personnel within an organization are advised to understand, thereby increasing organizational strength and enabling faster, more effective decision-making.

Introduction

As long as organizations remain in business and continue to grow, all the managers are facing uncertainties each in their own field, even for organizations which haven`t any innovation strategies, they are facing a different kind of uncertainties generated from various external sources like market growth, new environmental requirements, political changes, global pandemic, etc.
Most of these changes represent a case study to become a core for projects initiatives, or management changes inside the organization, and from that point, uncertainties are generated.
The defamiliarization with risk management, due to a lake of standards knowledge and/or not enough training, leads to confusion in choosing the proper tool and technique at the right time, let such uncertainties impede performance, compromise safety, or diminish value if not managed through a disciplined and systematic approach.

[1] How to cite this work: Sadek, A. (2026). Closing the Risk Communication Gap Between Executives and Project Managers: A Standards-Based Approach, *PM World Journal*, Vol. XV, Issue I, January.

Therefore, most managers chose to avoid any changes and new projects, unless it is Mandatory, and as a result of that methodology, the organization may lose many opportunities and become fragile when facing issues. On the other side, the senior executives operate with a strategic perspective on risk that differs from the operational mindset of the function and project managers; this culture disconnect creates a "translation barrier" between project teams and executive leadership. This misalignment occurs when project managers do not clearly understand what senior executives expect from them regarding risk responses and that case generates a critical business problem. In addition, for other managers when facing a problem and they are capable of tacking the right decision to solve it, they may not be aware to identify any secondary risk may generate from that decision. The purpose of this paper is to help closing that gap by defining risk management objectives according to standards such as ISO 31000:2018, ISO 31010:2019, and PMI PMBOK® Guide. as they address the responsibilities of both project managers and executives in the risk management process.

By analyzing the principles, practices, and processes within these frameworks, the paper seeks to clarify what is practically applicable, how these standards can be interpreted consistently across organizational levels, and how project managers can better meet the expectations of the senior executives when communicating and addressing risks. Through this analysis, the study aims to enhance mutual understanding, support more effective collaboration, and strengthen organizational capability in managing uncertainty. The purpose of this paper is to help to close that gap by defining risk management objectives according to standards such as ISO 31000:2018, ISO 31010:2019, and PMI PMBOK® Guide. as they address the responsibilities of both project managers and executives in the risk management process. By analyzing the principles, practices, and processes within these frameworks, the paper seeks to clarify what is practically applicable, how these standards can be interpreted consistently across organizational levels, and how project managers can better meet the expectations of the senior executives when communicating and addressing risks. Through this analysis, the study aims to enhance mutual understanding, support more effective collaboration, and strengthen organizational capability in managing uncertainty.

Key objectives of Risk Management covered in this paper are:

Objective	Description
Risk Assessment	Detect internal and external factors that might affect objectives, and evaluate likelihood and impact to prioritize response
Risk Response Planning	Design and implement actions to reduce threats or enhance opportunities.
Risk Management Monitoring and Control	Ensure that risk response strategies are executed as planned.
Support Decision Making	Provide better visibility for strategic and

Objective	Description
	operational decisions.

Table (1-1) Key Objectives of Risk Management

1 Risk Assessment Process

Definition:
According to British Standard BS 31100, risk assessment is the overall process of risk identification, risk analysis, and risk evaluation. It offers a structured process to identify, analyze, and evaluate risks that could impact an organization's objectives either negatively (threats) or positively (opportunities).

Benefits:
A well-executed risk assessment helps to highlight common or recurring risk areas, recognize high-priority threats and opportunities, and guide the selection and Implementation of mitigation and control measures, to contribute organizational decision making, and to allocate resources to the most significant risk.

Key Considerations:
Key considerations include involving the Sponsor and/or CEO to shape risk attitude and financial priorities, while also engaging individuals with cultural and organizational insight to ensure alignment with current policies and processes.

1.1 Identification of Risks

You can only manage things you are aware of.
"(John M. Nicholas & Herman Steyn, n.d.)

The first and most essential step after risk management scope and objective are agreed upon (PMI, P. M. Institute. (2024). *Risk Management in Portfolios, Programs, and Projects: A Practice Guide)*, is to actively identify potential risks-both threats and opportunities-early enough to allow for an effective response. Risk identification involves more than simply listing possible worst-case scenarios or opportunities; the potential risk owner should also be identified during this process.

Key Principle

The acceptability of risk largely depends on the organizations and stakeholders "individual risk tolerance", which is influenced by their experience, perception, and exposure to similar situations.

According to ISO 31000:2018, risk attitude and appetite vary across individuals and organizations, shaped by cultural, contextual, and experiential factors (ISO, 2018).

Such differences in experience and perception can influence project-level risks, including persistent issues such as loss of funding or weak management commitment.

Proactive Recognition

Risk identification should be structured, forward-looking, and inclusive of:

Threats: Events that could harm objectives (e.g., cost overruns, data breaches)
Opportunities: Events that could enhance value (e.g., early project delivery, new markets).

Also, it involves recognizing uncertainties that may affect strategic goals, disrupt operations or supply chains, damage financial health, compliance standing, and impact brand and stakeholder trust**.**

Categorizing Risk:

We categorize risks because it makes risk management more systematic, transparent, and effective. Table (1-2) describes some of the risk categorization.

	Category	Examples
1	Strategic	Market competition, mergers, regulatory change
2	Operational	Equipment failure, workforce shortage, cyberattacks
3	Financial	Budget cuts, currency fluctuations, funding risks
4	Compliance	Changes in laws, audit risks, non-adherence
5	Reputational	Media incidents, customer dissatisfaction
6	Environmental	Natural disasters, climate change risks
7	Technological	System failures, obsolescence, integration risks

Table (1-2) Risk Categorization Examples

Example:
A construction & Infrastructure company may consider: Crane collapse or equipment malfunction causing injury, as (Operational Risk), non-adherence to building codes, labor laws, or environmental assessments as (Compliance Risk), and Delays or quality failures leading to public scrutiny and client dissatisfaction as (Reputational Risk).

Comprehensive Coverage

Risk identification should take place at all organizational levels and departments, not just within the executive suite or on major projects. The risk level in which we are studying is important to figure out, for example:

> ***Strategic level:*** Risks to long-term vision, investments, market positioning
> ***Tactical level:*** Risks in programs, departments, or IT systems
> ***Operational level:*** Day-to-day process risks, safety issues, logistics

Using the appropriate tools for identification.

Tool	Use to
SWOT Analysis	Identify strategic threats and opportunities
PESTLE Analysis	Scan political, economic, social, tech, legal, environmental risks
Process Mapping	Identify weak points or failure modes
Risk Checklists	Ensure no common risks are missed
Interviews & Workshops	Get input from various departments
Historical Data & Incident Logs	Learn from past risk events
Root Cause Analysis (RCA)	Find underlying triggers of known issues

Table (1-3) Tools for Risk Identification

Risk Classification (Internal vs External Risks)
As can be seen in Table (1-4), risk in projects can be classified as internal risks and external risks, for example:

Internal Risks	**External Risks**
Staff turnover	Regulatory changes
Data loss	Material or labor resources (shortages)
Inadequate training or skill gaps among team members.	Physical environment (weather, terrain)
	Market conditions Competitors

Table (1-4) Internal and External Risks

Outputs of Risk Identification

According to the PMBOK® Guide, Sixth Edition, the outputs of this process include the Risk Register Figure (1), Risk Report, and updates to project documents. The Risk Register specifically records the details of identified individual risks, documents the results of risk analysis and response planning, tracks the implementation of those responses, and provides the current status. It serves as a tool to monitor risk information throughout the project's life cycle.

RISK REGISTER

Project Title: _____ Date Prepared: _____

ID	Risk Statement	Owner	Probability	Impact				Score	Response
				Scope	Quality	Schedule	Cost		

Revised Probability	Impact				Revised Score	Responsible Party	Actions	Status	Comments
	Scope	Quality	Schedule	Cost					

Page 1 of 1

A PROJECT MANAGER BOOK OF FORMS 3rd Edition
Figure (1-1) Risk register example

1.2 Risk Analysis Methods

Risk analysis and evaluation are essential parts of the risk management framework as they provide the evidence needed for risk treatment decisions and help organizations transform uncertainty into informed action, before committing resources or launching a project, it's essential to identify where the highest identified risks originate, understand their potential impact, and determine if and how they can be managed or mitigated and to reach that point, we start analyzing and evaluating risk by determining the Risk value as a result of its probability of occurrence and severity of its impact

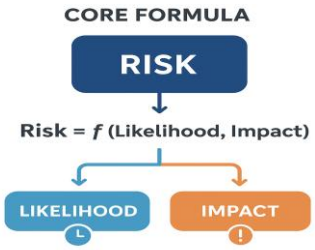

Figure (1-2) Risk likelihood and impact

Understanding Likelihood and Impact

Likelihood
Figure (1-3)

Impact (-/+)
Figure (1-4)

Figure (1-3) shows the meaning of likelihood "when sky is cloudy then it might rain and it is better to get an umbrella".

Figure (1-4) shows the meaning of the raining Impact "Negative for construction worker and Positive for farmers"

Likelihood and impact address two essential questions:

- *What could happen, and why?*
- *What would the impact be if this occurred?*

	Likelihood	Impact (-/+)
Definition	Probability of the risk occurring. Expressed numerically. (1 = certain, 0 = impossible).	The severity of consequences if the risk occurs, wither (-) Threat or (+) Opportunity.
Example Scale	Rare / Unlikely / Possible / Likely / Almost Certain	Minor / Moderate / Major / Critical / Catastrophic

Table (1-5) Risk Likelihood and Impact

The most common approaches to risk analysis are qualitative analysis (using descriptive rankings such as low, medium, or high), quantitative analysis (applying numerical probabilities, statistical models, and data-driven methods), and semi-quantitative analysis (blending descriptive rankings with numerical scoring) for greater precision.

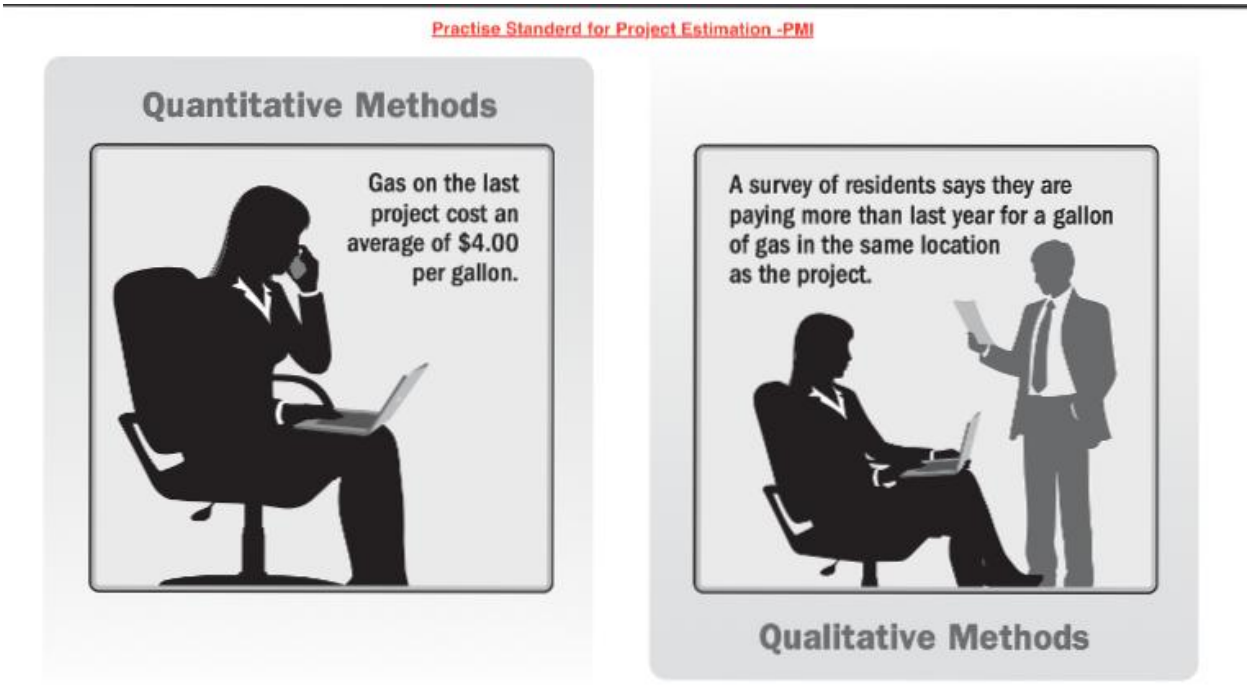

Figure (1-5) Quantitative and Qualitative Methods of Risk Analysis

Risk Analysis Integrated **Tools and Techniques**

Based on IEC/ISO 31010, ISO 31000:2018, and PMBOK® Guide Ed. 6.

Why Combining Quantitative and Qualitative Methods Matters?

- ISO 31000 brings depth and domain-specific techniques for comprehensive risk profiling—from root causes to probabilistic outcomes.
- PMI's approach emphasizes project context and decision clarity, focusing on stakeholder-aligned, phased analysis.
- Together, they form a robust toolkit: users can choose methods based on project complexity, data availability, and required analytical rigor.

Category	ISO 31000 Techniques	PMI PMBOK® Tools & Techniques	Purpose / Notes
Qualitative Analysis	- Checklists - Brainstorming - Delphi technique - SWIFT (Structured What-If Technique) - Risk Matrix - SWOT analysis	- Expert Judgment - Risk Probability & Impact Assessment - Probability & Impact Matrix - Risk Categorization - Prompt Lists	Quickly identify and prioritize risks based on expert insights, probability, and impact without heavy numerical analysis.
Semi-Quantitative Analysis	- Risk Scoring - Risk Ranking - Bow-Tie Analysis	- Probability & Impact Matrix (with scoring) - Risk Data Quality Assessment	Combines scoring systems with qualitative inputs to allow more nuanced prioritization.
Quantitative Analysis	- Simulation (Monte Carlo) - Decision Tree Analysis - Sensitivity Analysis - Event Tree Analysis (ETA) - Fault Tree Analysis (FTA)	- Simulation (Monte Carlo) - Decision Tree Analysis - Sensitivity Analysis - Influence Diagrams	Uses numerical data, models, and simulations to measure risk exposure and support decision-making.
Root Cause / Diagnostic	- Failure Mode and Effects Analysis (FMEA) - Cause-and-Effect Analysis (Fishbone Diagram) - HAZOP (Hazard and Operability Study)	- Root Cause Analysis - Failure Mode and Effect Analysis (FMEA)	Identifies underlying causes of risks and potential points of failure to target preventive measures.

Table (1-6) Mapping of Common Risk Analysis Tools

The output of a risk assessment

The output of a risk assessment is essentially the documented results of identifying, analyzing, and evaluating risks, plus the basis for deciding how to treat them. According to ISO 31000, IEC/ISO 31010, and the PMBOK® Guide, the key outputs include:

1.2.1.1 Risk Register Update (or Risk Log)

The risk register mentioned in Figure 1, updated with risk prioritization, and risk score or level, as well as minimizing the risks with low impacts.

1.2.1.2 Risk Matrix / Heat Map

A risk matrix, also known heat map is a visual tool that plots risks based on their probability and potential severity, allowing decision-makers to quickly identify and prioritize those requiring immediate action. Beyond its analytical value, it also serves as an effective communication tool

by providing stakeholders with a clear visualization of the organization's overall risk landscape and highlighting the areas of most significant concern. See Figure (1-6).

1.2.1.3 Risk Treatments

Initial recommendations may involve mitigation, prevention, transfer, or acceptance strategies, as well as defined control measures and assigned responsibility owners.

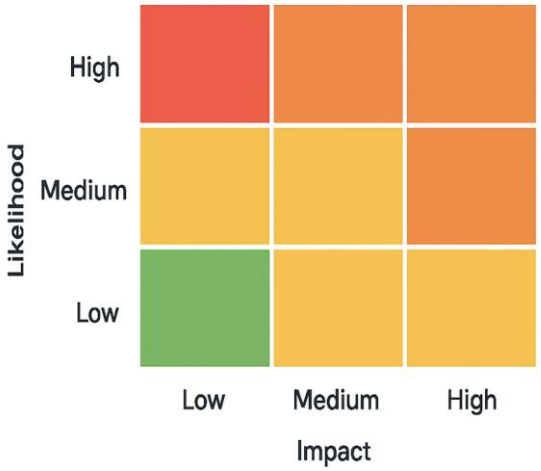

Figure (1-6) Heat Map

1.2.1.4 Supporting Analysis

Probability models, simulations (e.g., Monte Carlo), cause-and-effect diagrams, or SWOT outputs any quantitative or qualitative evidence used

1.2.1.5 Basis for Decision-Making

A clear, evidence-backed foundation for the risk treatment plan and resource allocation this may be incorporated directly into a Risk Assessment Report.

2 Risk Response Planning

At this stage, the expertise of the project manager is particularly significant, as it informs the selection of strategies most suitable for addressing the specific characteristics of each risk. The overarching aim of this process is twofold: to mitigate the adverse consequences associated with threats and to enhance the potential advantages offered by opportunities. The outcomes of the preceding risk assessment provide an evaluative basis for prioritization, enabling the differentiation between risks that require heightened attention and those of comparatively lesser significance. This prioritization applies irrespective of whether the risk manifests as a threat or as an opportunity.

Formulation of the risk response plan must be consistent with the organization's strategic orientation, the objectives of the project, the risk attitudes of key stakeholders, and the principles articulated in the risk management framework. A further dimension of consideration lies in the potential emergence of secondary risks. These are risks that arise as unintended consequences of implementing a given response. In instances where secondary risks exhibit a high probability of occurrence or a substantial potential impact, it may become necessary to re-evaluate and adapt the planned response to ensure that it remains viable and proportionate. The risk register serves as the principal instrument for operationalizing response strategies, as it clearly identifies both the designated risk owners and the associated response actions. It is therefore essential that risk owners possess not only the authority but also the capability to implement and continuously monitor the effectiveness of these responses.

Finally, it is important to acknowledge that the appropriateness of a particular response strategy is context-dependent: a response deemed effective in one project or time period may require modification or substitution in another, reflecting the dynamic and situational nature of risk management. Although the terminology used to describe risk response strategies may vary across different standards and publications, the underlying concepts remain largely consistent. In this section, Figure (2-1) describes the PMI framework for risk response strategies will be applied in detail, while also highlighting alternative approaches referenced in other standards and academic sources.

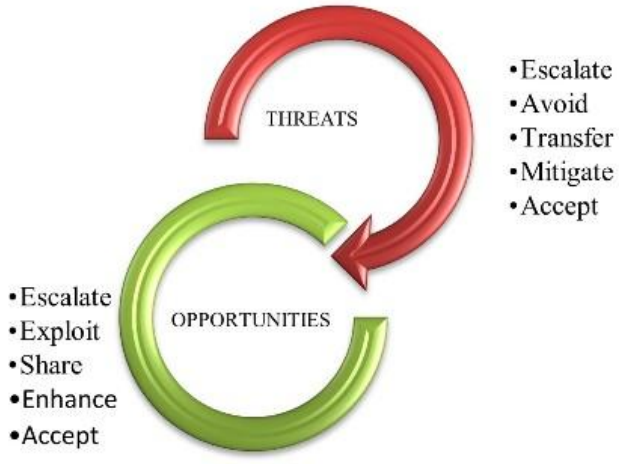

Figure (2-1) Risk Response Strategies

When implementing the above strategies, we take into consideration the stakeholders' risk attitude, risk priorities, and the project management plan.

The appropriate risk response has been developed for both threats and opportunities (PMI /THE STANDARD FOR RISK MANAGEMENT).

2.1 Escalate as a Threat & Opportunities Response Strategy

ISO 31000 does not explicitly mention "escalate" as a risk treatment option. However, the principle of assigning risks to the right level of authority is closely aligned with ISO's governance and accountability framework. PMI PMBOK, on the other hand, formally defines "Escalate" as a response strategy.

When Do You Escalate?

Escalation is used when the risk is important, but the project manager and project team are not the right authority to handle it. Instead of trying to control it, you hand it over to the right organizational level (program, portfolio, or senior manager)

Escalate for Threats

You escalate a threat when:

- The risk is outside the scope of the project.
- The impact is too large for the project's budget, schedule, or authority.
- The organization has better mechanisms to handle it.

Escalate for Opportunities

You escalate an opportunity when:

- The benefit is beyond the project's objectives and affects the whole organization.
- The project lacks the authority, budget, or capacity to capture the opportunity.
- Another organizational level can realize greater value.

Key Difference Between Threat & Opportunity Escalation

- Threat Escalation: Protects the project/organization from a risk that is too large or external.
- Opportunity Escalation: Ensures the organization can capture benefits that are wider than the project's scope.

Escalation ensures risks are managed by the right level of authority — rather than wasting time trying to control something the project team cannot influence.

It's not about ignoring the risk — it's about passing it to the right owner.

2.2 Avoidance as a Threat Response Strategy

For many project managers, risk avoidance is often considered the most effective strategy, particularly when dealing with high-priority threats or risks with potentially severe impacts. Avoidance involves altering the project plan to eliminate the source of risk or to protect project objectives from its potential consequences.

However, there are situations where risks cannot be avoided, such as compliance with legal requirements or the adoption of new regulatory standards. In such cases, as clarified by PMI, if the risk is not escalated to a higher authority, the decision to apply an avoidance strategy remains under the responsibility of the project manager. In practice, risk avoidance can also be applied proactively to risks emerging from new ideas, operational changes, or innovations intended to enhance the project lifecycle or achieve strategic objectives. Examples include implementing a fast-track schedule**,** adopting new materia**ls**, or integrating emerging technologies. These decisions often involve weighing potential threats against long-term benefits, requiring careful judgment and alignment with organizational risk appetite.

2.3 Exploitation as an Opportunity Response Strategy

The exploit strategy, as defined in the PMBOK® Guide and aligned with ISO 31000's concept of maximizing positive risk, seeks to ensure that an identified opportunity is fully realized. Unlike strategies such as "enhance" or "share," which only increase the probability of occurrence, exploitation involves taking deliberate and proactive actions to guarantee that the opportunity materializes.

This approach requires careful consideration of:

- Regulatory and governance requirements – ensuring compliance with legal frameworks and organizational policies.
- Roles and responsibilities – clearly assigning accountability for seizing the opportunity.
- Budget and investment needs – allocating sufficient resources to secure the opportunity.
- Return on Investment (ROI) – evaluating the potential benefits to confirm that exploitation creates measurable value.

2.4 Transfer as a Threat Response Strategy

Transferring risk means assigning responsibility for managing that risk to a third party. The best example of this strategy is when an insurance company covers the impact of potential damages, even if the coverage is only partial. It is the role of the project or financial manager to select a suitable third party for dealing with that risk after it has been transferred. Insurance is not the only method for transferring risk; a service agreement, such as a fixed-price contract, can also fulfill this role. A fixed-price contract ensures that the agreed-upon work will be completed for a predetermined amount, specified before work begins.

2.5 Sharing as an Opportunity Response Strategy

Sharing is a risk response strategy in which the benefits of an opportunity are deliberately shared with a third party that possesses the necessary expertise, resources, or capabilities to maximize its realization. The key consideration in this approach is the careful selection of the partner or new opportunity owner, ensuring that they are best positioned to capture and deliver the benefits in alignment with the project's objectives.

Practical examples of the sharing strategy include establishing partnerships, forming joint ventures, creating special-purpose entities, or assembling cross-functional teams. Such arrangements must remain consistent with the organization's policies, governance structures, and applicable legal or regulatory requirements.

2.6 Mitigation as a Threat Response Strategy

Mitigation is one of the most critical risk response strategies, as it reflects both the project manager's expertise and the organizations or stakeholders' risk appetite**.** The essence of mitigation lies in reducing either the likelihood of a risk occurring or its potential impact on project objectives. In some cases, this may even require initiating a separate project, such as developing a prototype, to address uncertainties proactively.

Effective mitigation emphasizes early action—it is far more beneficial to reduce risks before they materialize than to wait until they occur, at which point they escalate into issues requiring reactive management.

2.7 Enhancement as an Opportunity Response Strategy

Enhancement, as a risk response strategy, serves as the counterpart to mitigation in the management of negative risks (threats). While mitigation focuses on reducing the probability or impact of adverse events, enhancement aims to increase the likelihood of an opportunity occurring or to amplify its positive effects once realized (PMI, *PMBOK® Guide*, 2021; ISO 31000:2018).

Importantly, early enhancement actions are often recommended, as they enable organizations to capture greater benefits from opportunities before they diminish or are seized by competitors. By proactively enhancing opportunities, organizations strengthen project outcomes, maximize value delivery, and ensure stronger alignment between initiatives and strategic objectives.

2.8 Acceptance as a Threat / Opportunity Response Strategy

When risk assessment determines that a risk is of low priority—either due to its limited probability or negligible impact—the project manager may decide not to implement any proactive response strategy. This approach is referred to as risk acceptance (PMI, *PMBOK® Guide*, 2021; ISO 31000:2018).

- **Active Acceptance**: This involves preparing contingency reserves (budget, time, or resources) to respond if the risk materializes.
- **Passive Acceptance** : This involves taking no proactive measures, simply acknowledging the risk and dealing with it if it occurs.

Approach	**ISO 31000 (Risk Treatment Options)**	**PMI PMBOK® Guide (Risk Response Strategies)**	**Notes / Alignment**
Avoid	Avoid the risk by not starting or stopping the activity.	Avoidance – eliminate the threat entirely (e.g., change scope, cancel risky task).	Direct alignment.
Reduce likelihood / consequences	Modify likelihood or impact to lower risk level.	Mitigation – take action to reduce probability or impact.	ISO calls this "modifying risk"; PMI uses the explicit word "Mitigation."
Remove risk source	Eliminate the cause of the risk.	Mitigation / Avoidance depending on context.	Example: replacing faulty equipment (ISO: remove source; PMI: mitigate).
Share / Transfer	Share the risk with another party	Transfer (Threats) **or** Share (Opportunities).	Both standards match here.
Take / Increase risk (to pursue opportunity)	Deliberately accept higher exposure to achieve benefit.	Exploit – guarantee the opportunity occurs. Enhance – increase chance/impact.	Same concept, PMI splits into two terms.

Retain risk	Accept the risk when further treatment isn't cost-effective or necessary.	Accept (Passive/Active).	Direct alignment.

Table (2-1) Comparison between ISO 31000 vs. PMI Risk Response Strategies

3 Risk Management Monitoring and Control

According to the PMBOK® Guide (PMI, 2021) and ISO 31000:2018, the main purpose of risk monitoring and control is to ensure that risk response strategies are executed as planned, while also continuously tracking existing risks and addressing new or secondary risks as they arise. This helps keep the risk management plan dynamic, adaptive, and aligned with both project and organizational goals.

A key enabler of effective control is the use of well-defined metrics and performance indicators that measure the effectiveness of response actions.

Peter Drucker wrote (*The Practice of Management*. New York: Harper & Row.), "Effective management requires measurement", according to this Metrics must be applied, such as technical performance indicators, reserve consumption analysis, and schedule variance tracking can provide early warnings when risk responses are deviating from expectations or proving ineffective.

The below example shows a significant risk and the implemented strategy to deal with:

Example*: Machine Maintenance in a Manufacturing Plant*

Identified Risk:

Unexpected machine breakdowns are causing production delays, leading to delays in product(s) delivery, allowing other competitors to have our market share and lose reputation.

Risk Control Applications:

a) Preventive Control (Terminate / Stop the risk):
   - Schedule preventive maintenance (oil change, part replacement) to avoid unexpected breakdowns.
   - Install surge protectors to prevent damage from electrical faults.

b) Corrective Control (Treat the impact):
   - Maintain an on-site spare parts inventory so faulty components can be replaced immediately.
   - Have a backup machine available to take over production if one fails.

c) Directive Control (Transfer through instructions/behavior):
   - Develop and enforce standard operating procedures (SOPs) for machine operation.
   - Provide training to machine operators on correct handling and emergency shutdown processes.

d) Detective Control (Tolerate, but detect quickly):
   - Install condition monitoring sensors to detect vibrations, overheating, or unusual sounds.
   - Conduct regular inspections to identify early warning signs of wear and tear.

However, it is essential to balance the sophistication of the monitoring system with its cost.

The expense of implementing measurement and monitoring processes should not exceed the potential impact of the risks being managed. A well-designed monitoring framework provides timely insights and early notifications without becoming a burden on project resources.
Fostering risk awareness across the project team is crucial. Continuous monitoring demands vigilance to recognize triggers, spot early warning signs, and detect emerging risks. By creating a proactive culture, risks are not only tracked but also actively managed throughout the project life cycle.

Control Area	ISO 31000:2018	PMBOK® Guide (2021)
Framework & Governance	Establishes principles, framework, and integration with organizational governance (Clauses 4–5).	Defines the Risk Management Plan within the overall project management plan. Identifies roles, responsibilities, and risk appetite.
Risk Identification & Assessment	Clause 6.4.2 – Identify risks, analyze them, and evaluate against risk criteria.	Identify Risks & Perform Risk Analysis (qualitative & quantitative) processes.
Risk Response	Clause 6.5 – Select and implement risk treatment options (avoid, mitigate, transfer, accept, exploit, enhance, share).	Plan Risk Responses & Implement Risk Responses processes, assigning ownership and ensuring execution.
Monitoring & Review	Clause 6.6 – Continuous monitoring of risks, treatment actions, and effectiveness. Adjust as necessary.	Monitor Risks process ensures tracking, auditing, and updating risk register. Includes reassessment and identifying new risks.
Recording & Reporting	Clause 6.7 – Document results, decisions, lessons learned, and communicate to stakeholders.	Risk register, risk report, and lessons learned repository are updated regularly.
Continuous Improvement	Encourages feedback and learning for enhancing future risk management performance.	Updates to Organizational Process Assets (OPAs)with lessons learned for continuous improvement.

Table (3-1) differences & alignments in risk management controls ISO 31000 and PMI PMBOK® Guide.

4 Support Decision-Making

When implementing a structured, evidence-based risk management process, organizations can make sound decisions at both strategic and operational levels.

Managers employ tools like risk registers, scenario analysis, and quantitative techniques to assess uncertainties in relation to objectives methodically. This systematic approach helps optimize resource allocation and strengthen the justification for strategic decisions. Furthermore, the Project Management Institute (PMI) reports that embedding risk management within project governance enhances transparency and stakeholder confidence in the decision-making process. Moreover, the process of risk assessment and evaluation provides project managers, functional managers, and sponsors with timely and reliable insights, enabling them to make informed decisions confidently.

Ongoing risk management allows organizations to adopt a progressive elaboration approach, as lessons learned and new insights guide future initiatives.

This approach not only helps prevent potential losses, but also allows organizations to capitalize on new opportunities, fostering both innovation and sustainable growth.

Conclusion

Ensuring compliance in risk management requires a structured and systematic approach that integrates international and local standards, organizational policies, and continuous monitoring:

- The adoption of recognized frameworks such as ISO 31000:2018, which provides guidelines for risk identification, analysis, evaluation, and treatment, and the PMI PMBOK® Guide (2021, 7th Edition) for project-based risk compliance, establishes a strong foundation for practice.

- Organizations should develop clear risk management policies aligned with external regulations while supporting these with standard operating procedures that guide daily practices and ensure adherence to legal and contractual requirements.

- Regular audits and reviews are essential for compliance assurance, with internal audits verifying conformity to internal standards and external audits providing independent oversight; ISO 19011:2018 serves as a key reference for auditing management systems.

- Training and awareness programs further strengthen compliance by equipping employees with knowledge of safety measures.

- Finally, leveraging technology and tools, such as compliance management systems (CMS) and Governance, Risk, and Compliance (GRC) platforms, combined with

automated monitoring systems for cybersecurity and environmental performance, enhances efficiency and ensures timely detection of non-compliance. Collectively, these practices foster a proactive, evidence-based approach that not only satisfies regulatory requirements but also supports organizational resilience and stakeholder confidence.

References:

- Kerzner, Harold, PhD. A Systems Approach to Planning, Scheduling, and Controlling, 12th Edition, https://www.wiley.com/en-se/Project+Management%3A+A+Systems+Approach+to+Planning%2C+Scheduling%2C+and+Controlling%2C+12th+Edition-p-9781119165361
- British Standard BS 31100 https://www.dinmedia.de/en/standard/bs-31100/348993300
- BS EN 13306:2017 – Maintenance — Maintenance terminology; British Standards Institution (BSI). Provides definitions and concepts useful in preparing a structured maintenance-related risk report. BS EN 13306:2017 - TC | 31 Jan 2018 | BSI Knowledge
- Fundamentals of Risk Management: Understanding, evaluating, and implementing effective risk management, 4th Edition, (Paul Hopkin) https://www.amazon.com/Fundamentals-Risk-Management-Understanding-implementing/dp/0749479612
- ISO 31000:2018 – Risk management — Guidelines; International Organization for Standardization (ISO). Provides the general principles and framework for risk management processes, including assessment and reporting. https://www.iso.org/standard/65694.html
- IEC/ISO 31010– Risk management — Risk assessment techniques; International Organization for Standardization (ISO). Details a wide range of techniques for risk analysis and evaluation, applicable to machinery maintenance scenarios. https://www.iso.org/standard/72140.html
- Practical Project Risk Management; The ATOM Methodology Second Edition David Hillson and Peter Simon, https://www.amazon.com/Practical-Project-Risk-Management-Methodology/dp/1567263666
- Project Management Institute (PMI). (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition. Newtown Square, PA: PMI. www.pmi.org
- Project Management for Business, Engineering, and Technology Principles and Practice 6th Edition, John M. Nicholas (Loyola University Chicago)
- Herman Steyn (University of Pretoria) https://doi.org/10.4324/9780429297588
- Risk Management in Portfolios, Programs, and Projects: A Practice Guide), www.pmi.org
- The Practice of Management, By Peter Drucker; https://doi.org/10.4324/9780080942360

Acknowledgments

I would like to express my sincere gratitude to my mentor, Mr. Thomas Walenta, for his continuous support and guidance throughout this research, which could not have been completed without his support and help, and his effort in guiding the planning of my roadmap.

This manuscript was proofread using [Chat GPT] for some figures and photos generation, and [Grammarly] for grammar and clarity improvement.

Finally, I appreciate my wife for her encouragement during this journey.

About the Author

Eng Ayman Sadek

Egypt

Eng. Ayman Sadek graduated from Helwan University in 1992 with a Bachelor's degree in Mechanical Engineering. He has been a member and volunteer at PMI, the Project Management Institute, and has been certified as PMP, RMP-PMI, and PBA-PMI. He began his career as a Maintenance Engineer, later advancing to Site and Project Manager in industrial construction projects for example, but not limited to, petrochemicals, cement products, polymers and polyproline products. He then joined a maritime company as a Technical Superintendent, overseeing technical operations and projects for ship repairs and ship building. Over time, he progressed to Execution Management, involved in Digital transformation and change management at many companies. He currently serves as the Managing Director of the company and a member of the Board. He can be contacted at: tam330@hotmail.com