

Rethinking Risk Management: Definition, Analysis, and Response ¹

Ayman Sadek

Abstract

This article negotiates the gap between executive and traditional risk managers when it comes to decision-making. We can see that standards such as PMI and ISO 31000 define the risk as effective uncertainty on objectives, but still deal with risk assessment and response as a practice activity governed by scoring and reporting, rather than strategic insights.

On the other side, the executive evaluates the risk according to the strategic impact, and to gain the executive's cooperation, we present the risk management in their language.

Ultimately, the article highlights the advantages of transforming the concept of uncertainty into an actionable strategic vision.

Introduction

Theoretically, risk management is presented as a sequential, integrated process of planning, identifying, analyzing, and responding.

However, in practice, it is often reduced to a routine reporting process rather than an effective decision-making tool.

To recognize the reasons for that, we need to revisit the main risk management fundamentals.

1- What Is Risk—Really?

The Project Management Institute (PMI) defines risk as: *“Risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more objectives.”*

According to ISO 31000 (2018), *risk* is the *“effect of uncertainty on objectives.”* *“An effect is a positive or negative deviation from what is expected.”*

While both definitions are accurate, they become insufficient when applied to executive decision environments, but they give a narrow conception of risk when it comes to reality, where the executive level cannot deal with uncertainty; they can only handle and understand the defined

¹ How to cite this article: Sadek, A. (2026). Rethinking Risk Management: Definition, Analysis, and Response, commentary, *PM World Journal*, Vol. XV, Issue IX, September.

risks. This perspective transforms everything about risk management, from simply recording events and filling models to a comprehensive understanding of the risk impact upon the strategy, assessing the risk, and planning the proper response for each risk, considering that risk is not the event itself, but what the event *means* for your objectives.

By considering some principles during the following process, we may solve that problem.

2- Risk Identification: The step from unknown- unknown to known-unknown

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.

The Key Principles:

- The acceptability of risk largely depends on the organizations and stakeholders' individual risk perception tolerance, which is influenced by their experience, perception, and exposure to similar situations, as well as the strategic impact.
- 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).
- Risk identification should take place at all organizational levels and departments, not just within the executive suite or on major projects.
- For accurate and practical risk identification, it is preferable to classify risks (External and Internal) and categorize them (**Strategic, Operational, Financial, Compliance, Reputational, and Environmental**).

3- Risk Analysis: Beyond Probability and Impact

After the identification of the risk, we are now moving toward the next operation of assessment (Risk Analysis).

For a risk expert, that means using a proper method, generating a final, accurate heat map to start the next process (Risk Response), but to put that response strategy in reality, we need the executive(s) approval, and actually, we might face a gap mostly because the risk analysis focuses on the probability of the risk and its impact to determine the Risk scoring.

This results in a quite accurate structure, but it misses the clarity for the executive or stakeholder to be fully aware of the risk and the appropriate type of response.

*When was the last time an executive made a decision based on a “0.6 probability”?
Exactly.*

Executives don’t decide based on scores; they decide based on their consideration of:

- What could impact strategic priorities
- What requires immediate attention
- What trade-offs must be made

Without this, risk is not translated into executive language, but it loses its power and turns into reporting... not to insight.

3- Risk Response: Action or Illusion? Risk Response Planning

Although most risk professionals can generate a Risk response plan, they still face some obstacles when executing the plan, not because of the specific characteristics of each risk. But for evaluating the basis of prioritization in coincidence with stakeholders' and executives' approval and perceptions.

Another gap is in the terminology used to describe risk response strategies, which varies across standards and publications, even though the underlying concepts remain largely consistent and still ambiguous for risk-unfamiliar executives.

Risk response is often documented as:

- Avoid, Mitigate, Transfer, Accept, and Escalate (Only in PMI)

In reality, many responses:

- Are not linked to decision-making
- Lack of clear ownership at the right level
- Do not change the outcome significantly

An effective risk response must be:

- **Decision-driven** → What action will leadership take?
- **Outcome-oriented** → What will change as a result?
- **Aligned with authority** → Who can actually act?

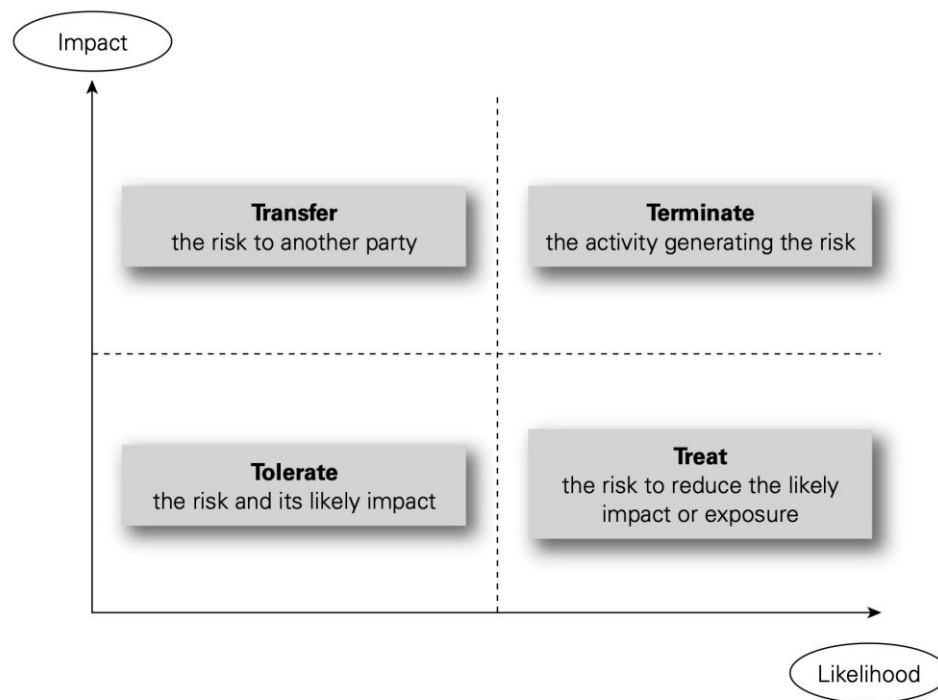
Otherwise, response plans remain theoretical.

Paul Hopkin introduces in his book “*Fundamentals of Risk Management 4th Edition*” other terminologies for risk response as represented in the Orange Book, described as 4Ts, where the 4Ts is short for (Tolerate, Treat, Transfer, and Terminate).

The table below describes the 4Ts Risk Response:

Tolerate / Accept	When risk assessment determines that a risk is of score.
Treat / Mitigate	The purpose of using the treatment is to take the appropriate procedures to control the risk to a manageable and acceptable level by minimizing the probability of occurrence or the risk impact.
Transfer Insurance/contract	It has the same terminology that used to be used as it is obvious for the executives whether by Insurance or fixed price contract.
Terminate Avoid/eliminate	Applied proactively for those risks will only be treatable, by terminating the cause of occurrence, like risks emerging from new ideas

The above terminology might receive the boardroom attention, as Paul Hopkin creates a relation between the risk response and the risk score and indicates it on the risk matrix as shown below:



Example — Expansion into an Unstable Market

Scenario,

A company plans to expand operations into a politically unstable country with high revenue potential, uncertain regulations, currency volatility, and supply-chain disruption risk.

Estimated opportunity:

- Annual profit potential: \$25M

Potential downside:

- Operational shutdown
- Asset seizure
- Currency losses
- Reputational impact

Executive Risk Response Matrix (4Ts)

Response	Practical Executive Action	Cost	Residual Risk	Strategic Impact	Executive Message
Tolerate	Enter market with current structure and monitor conditions	Low	High	Fast market entry	“We accept elevated exposure to capture early market advantage.”
Treat	Add compliance controls, diversify suppliers, hedge currency	Medium	Medium	Balanced expansion	“We reduce operational and financial volatility while maintaining growth.”
Transfer	Use political-risk insurance and local partnerships	Medium	Medium	Shared exposure	“We shift part of the financial and legal exposure to external parties.”
Terminate	Cancel expansion entirely	Opportunity loss	Very Low	No exposure	“We avoid geopolitical exposure but lose market opportunity.”

Why This Matrix Works Better for Executives

Executives usually think in terms of growth, cost, exposure, resilience, and strategic positioning. Not in isolated “risk treatment terminology.”

So instead of saying: “Recommended response: Treat.”

You say: “We recommend a partial treatment strategy combined with transfer to preserve 80% opportunity, as it reduces financial exposure to an acceptable level for the board.”

4- The Missing Link: From Process to Insight.

The real Issue is not a lack of tools; it is a lack of translation between operational risk management and executive decision-making, considering that risk management is not about filling registers, assigning scores, or categorizing responses. It is about answering a critical question: What do we need to understand and decide now?

Executive-Level Observation

But executives actually decide based on:

- strategic gain,
- financial tolerance,
- operational continuity,
- and organizational resilience.

So, the real power of the 4Ts is not the classification itself—it is the ability to compare strategic choices under uncertainty.

That is why a matrix format is often far more effective in boardrooms than traditional risk registers.

Final Thought

Executives don't ignore risk reports because they are careless; they ignore them because the reports don't speak their language.

This Article is based on my Featured Paper on Executive Risk Perspective and reflects the need to bridge the gap between governance frameworks and real-world decision environments.

<https://pmworldjournal.com/article/closing-the-risk-communication-gap>

References

- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. Geneva, Switzerland: ISO. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
- Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). Newtown Square, PA: PMI. <http://www.pmi.org>
- Project Management Institute. (2019). *The Standard for Risk Management in Portfolios, Programs, and Projects*. PMI. <http://www.pmi.org>
- Taleb, N. N. (2007). *The Black Swan: The impact of the highly improbable*. Random House. https://www.researchgate.net/publication/23534737_Nassim_Nicholas_Taleb_The_black_swan_The_impact_of_the_highly_improbable

- Mintzberg, H. (1994). *The rise and fall of strategic planning*. Free Press.
https://www.researchgate.net/publication/316628074_Henry_Mintzberg's_The_Rise_and_Fall_of_Strategic_Planning
- Paul Hopkin. (2017). *Fundamentals of Risk Management*, 4th Edition.
<https://www.amazon.com/dp/0749479612?lv=shuf&channelId=500&plpRedirect=mhFallback>
- Rethinking Risk Management | PDF - Scribd
<https://www.scribd.com/document/1053344585/Rethinking-Risk-Management>
"Rethinking Risk Management: Definition, Analysis, and Response. Ayman Sadek.
Abstract: This article negotiates the gap between executive and traditional risk ..."
- Closing the Risk Communication Gap Between Executives ...
<https://pmworldlibrary.net/article/closing-the-risk-communication-gap-between-executives-and-project-managers-a-standards-based-approach/>
- How to create a risk management plan - PPM Core
<https://ppmcore.com/blog/how-to-create-a-risk-management-plan-preparing-for-the-unexpected/>
- Risk Management Process for PMP®
<https://projectmanagementacademy.net/resources/risk-management-process-for-pmp/>
- Optimizing Project Success: Integrating Risk Management in ...
<https://www.cliffsnotes.com/study-notes/21306605>
- Project Risk Management: Identifying, Assessing, and Mitigating Risks
<https://www.linkedin.com/pulse/project-risk-management-identifying-assessing-risks-david-mccreery-de6pe>
- A practical risk management approach
<https://www.pmi.org/learning/library/practical-risk-management-approach-8248>
- The meaning of risk in an uncertain world
<https://www.pmi.org/learning/library/project-risks-uncertain-world-8392>
- Periodizing Management's Risks of Construction Projects with Gray Relational Analysis and FMEA Approach, Sara Mehrab Daniali, Dmitriy Rodionov & Farzin Mohammadbeigi Khortabi (2021) · IBIMA Publishing · <https://openalex.org/W3167726896>
- Operational Risk Management and Project Success in Rwanda, A Case Study of Lake Victoria Water and Sanitation Project (LVWATSAN) in Nyagatare District, Rwanda
Marie Therèse Masimbi (2023) · Stratford Peer Reviewed Journal & Book Publishing · <https://openalex.org/W4388575755>
- Value of Uncertainty: The Lost Opportunities in Large Projects
Agnar Johansen, Petter Eik-Andresen, Andreas D. Landmark, Anandasivakumar Ekambaram & Asbjørn Rolstadås (2016) · MDPI AG · <https://openalex.org/W2518357873>
- Error management for musicians: an interdisciplinary conceptual framework
Silke Kruse-Weber & Richard Parncutt (2014) · Frontiers Media SA,
<https://openalex.org/W2019475600>
- Risk Management in Biobanks, Karine Sargsyan, Brigitte Jaksa, Gabriele Hartl & Tanja Macheiner (2020) · IntechOpen · <https://openalex.org/W3043029117>
- The Impact of Risk Management on Project Success: A Field Study at Humanitarian Organizations in Yemen, Mohammed Ahmed Shujaa Aldeen & Nashwan Abdulwahid Sarhan (2024) · University of Science and Technology, Sana'a · <https://openalex.org/W4403416389>
- Mapping risks in UNILA acquisitions, Robinson Alexander Sturmer, Eduardo César Dechechi & Elias Garcia (2023) · Seven Editora · <https://openalex.org/W4379619332>

- Investigation of Risks and Risk Management Practices in The Fast-Moving Consumer Goods Sector in Turkey with an Interview Study, Recep Şababoğlu & Ünal Halit Özden (2024) · OPUS - Uluslararası Toplum Araştırmaları Dergisi <https://openalex.org/W4393359524>
- International Risk Management, Daniel V. Murphy (2008) · Society of Petroleum Engineers · <https://openalex.org/W2331619213>
- SS: Panel- Session on Risk Management in the Offshore Energy Industry International Risk Management, Daniel V. Murphy (2008) · OTC · <https://openalex.org/W1980848184>

About the Author



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, PgMP, 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 polypropylene products. He then joined a maritime company as a Technical Superintendent, overseeing technical operations and projects for ship repairs and shipbuilding. 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