

Turning Risk Reports into Action: A Critical Review of Behavioral Barriers to Effective Enterprise Risk Management

Tri Gunarsih^{a,1}, Muh Arief Effendi^{b,2}, Fran Sayekti^{*,c,3}

^{a,c} Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia

^b Trisakti School of Management, Jakarta, Indonesia

¹trigunarsih@uty.ac.id, ²mac@tsm.ac.id, ³fran.sayekti@uty.ac.id

Article Info

Article history:

Received 2026-04-22

Accepted 2026-07-06

Published 2026-07-07

Keywords:

Behavioral Finance,
Cognitive Biases,
Decoupling, Enterprise
Risk Management,
Risk Culture, Strategic
Decision-Making

Abstract

This article provided a critical review of why enterprise risk management (ERM) often failed to turn risk reports into timely risk actions. Drawing on behavioral finance (prospect theory) and bounded rationality, we explained how cognitive biases and attention constraints distort risk appraisal (probability/impact estimation and prioritization) and risk response (mitigation execution and escalation), creating a persistent gap in risk reporting and action. Agency theory and upper echelons theory clarified how incentive misalignment and executive biases shaped organizational risk-taking, while institutional theory highlighted ERM decoupling between formal structures and actual decision practices. We synthesized these perspectives into an integrative framework that positions ERM maturity and risk culture as mechanisms that could either transmit or buffer the effects of bias. Finally, the review then outlined a toolkit of bias-aware risk controls, standardized scenario framing, pre-mortems, independent challenge, action triggers, and stop-loss/kill criteria to strengthen strategic decision discipline.

DOI: <https://doi.org/10.46923/ijbhes.v8i1.683>

Open access under Creative Common Attribution Share A like 4.0 International Licence

(CC-BY-SA) 

1. Introduction

Organizations are increasingly adopting Enterprise Risk Management (ERM), compiling risk registers, conducting risk assessments, and producing periodic risk reports. In contemporary practice, ERM is positioned as a system that integrates risk with strategy and performance, including risk appetite setting, objective monitoring, and organizational learning (COSO, 2017). This integration is particularly salient in the service sector, where value creation depends heavily on intangible assets (e.g., trust, brand reputation, customer experience, and information quality), and where operations are often characterized by high customer contact, real-time delivery, and extensive reliance on human judgment and digital systems. As a result, service organizations, such as banks, insurers, fintech firms, hospitals, transportation and logistics providers, and hospitality businesses, face a distinctive risk profile in which operational disruptions, conduct risk, cyber and data risks, and regulatory compliance risks can quickly escalate into strategic threats. In such settings, ERM is expected to function not only as a compliance mechanism but also as a strategic capability that safeguards service reliability and customer trust while enabling calculated risk-taking to align with organizational objectives (COSO, 2017; ISO, 2018).

In practice, the risk reporting-action gap may manifest differently across service industries. In financial services (e.g., banking, insurance, and fintech), ERM is closely tied to prudential constraints and systemic confidence, where weaknesses in risk appraisal or delayed responses can amplify liquidity, solvency, conduct, and model risks, rapidly triggering market and regulatory reactions. In non-financial services (e.g., healthcare, hospitality, transportation, and logistics), ERM is often tested through service continuity, safety and quality assurance, cyber resilience, and customer-facing operational reliability, domains where frontline discretion and real-time service delivery create strong exposure to behavioral and communication failures. Across both settings, risk reports may become bureaucratic artifacts rather than decision tools when attention is overloaded, incentives favor short-term targets, or escalation channels are muted. The risk reports are reinforcing the need for a behavioral lens and bias-aware controls to convert risk insights into timely action (COSO, 2017; ISO, 2018; Simon, 1955).

On the other hand, various governance failures and organizational crises point to a paradox. The risk information is available, but it does not always translate into concrete decisions and mitigation actions. This persistent gap, which is called the risk reporting-action gap, describes a condition in which an organization is aware of the risks but it fails to act in a timely, proportionate, and consistent manner. The gap is strategic because it involves allocating resources under uncertainty. If risk reporting is not acted on, organizations are vulnerable to downside risks, strategic failures, reputational damage, and high regulatory costs. Therefore, the effectiveness of ERM cannot be judged solely by the existence of formal procedures, but rather by its ability to encourage strategic decision-making discipline such as decisions that are consistent with the organization's risk appetite and risk capacity. (COSO, 2017).

This conceptual article argues that the risk reporting action gap cannot be adequately explained by technical approaches alone (e.g., model refinement or the addition of indicators). The root of the problem is often behavioral for example risk control is carried out by humans and teams who are susceptible to cognitive biases, emotions, and social and organizational dynamics. In prospect theory, risk preferences can change due to loss aversion and framing and are influenced by reference points (Kahneman & Tversky, 1979). The concept of bounded rationality emphasizes the limitations of attention and cognitive capacity that encourages decision makers to rely on heuristics that can lead to systematic biases, especially when information is complex and under time pressure (Simon, 1955). At the governance level, agency theory explains how misaligned interests and incentive structures can lead to risk tolerance exceeding risk appetite making monitoring and incentive alignment crucial (Jensen & Meckling, 1976). At the leadership level, upper echelons theory emphasizes that organizational strategy and outcomes reflects the characteristics of top managers. It means that executive bias can shape risk appetite and responses to risk signals (Hambrick & Mason, 1984). At the institutional level, institutional theory describes decoupling, in which the formal structure of ERM is adopted for legitimacy but it remains separated from decision-making practices and resource allocation (DiMaggio & Powell, 1983; Meyer & Rowan, 1977).

The purpose of this article is to present a critical review of behavioral barriers that explains why risk reporting fails to become action and then to develop an integrative framework that links behavioral bias to ERM effectiveness through two mechanism pathways: (1) the risk appraisal path and (2) the risk response path. The article further develops a bias-aware control perspective by showing how ERM maturity and risk culture may either amplify or buffer the effects of bias on decision quality and the follow-through of mitigation efforts.

Despite the growing prominence of enterprise risk management (ERM), much of the existing literature has focused on formal structures, governance architecture, and implementation processes, while giving

comparatively less attention to the behavioral conditions under which risk information fails to trigger timely managerial action. This article addresses that gap by shifting the analytical focus from the existence of ERM mechanisms to the conversion of risk reports into concrete risk actions. Specifically, this study contributes to the ERM literature in four ways. First, it identifies the principal behavioral barriers that interrupted the translation of risk information into action. Second, it distinguishes conceptually between distortions that arouse in risk appraisal and those that arise in risk response, thereby offering a more precise explanation of why organizations may recognize risks yet they still fail to act. Third, it integrates behavioral, governance, leadership, and institutional perspectives into a single framework explaining how the risk reporting action gap emerges and persists. Fourth, it proposes a bias-aware control toolkit that links conceptual diagnosis with practical ERM design. Accordingly, this article extends prior ERM reviews by emphasizing action conversion, rather than utilizing only formal ERM adoption.

Afterwards, this article is structured in the following sections. Section 2 outlines the critical review approach and the scope of the literature. Section 3 presents the theoretical foundations that underpin the behavioral and organizational mechanisms underlying the risk reporting action gap. Section 4 synthesizes the main behavioral barriers that prevents risk reports from being acted on. Section 5 develops an integrative framework. Section 6 translates the barriers to control design and the last, section 7 concludes and describes the limitations.

2. Literature Review

A. Prospect Theory: Decision Behavior Under Risk

Prospect Theory explains that individuals evaluate the outcomes of decisions relative to the reference point and exhibit loss aversion, such losses are felt to be greater than gains of equal value; in addition, risk preferences are influenced by how information is presented (framing) (Kahneman & Tversky, 1979). The implications for ERM are direct: risk reported that frame mitigation as a fixed cost may delay action. At the same time, below target conditions can encourage risk-seeking decisions to cover perceived losses. Thus, Prospect Theory provides a behavioral foundation for why even objective risk reporting can produce different responses depending on framing and reference points.

B. Bounded Rationality: the Limitations of Attention and Heuristics

Bounded rationality asserts that decision-makers are not always able to optimize choices due to limited information, time, and computing capacity; as a result, they tend to be satisfied (Simon, 1955). In the context of ERM, bounded rationality explains why overly dense risk dashboards can degrade decision quality: attention is divided, important risk signals do not stand out, and teams revert to heuristics or intuition. The framework also justifies the need for controls that facilitated the assessment process, such as scenario standardization, restriction of key metrics, and challenge mechanisms, to make appraisal and response more consistent.

C. Agency Theory: Risk Control as Monitoring and Coordination of Incentives

Agency Theory views the company as a contract between a principal and an agent, where misaligned interests acquires agency costs; therefore, monitoring and incentive mechanisms are needed (Jensen & Meckling, 1976). In ERM, this concept positions risk limits, risk committees, audits, and reporting as governance tools that suppress moral hazard and opportunistic behavior. The interaction between agency theory and behavioral lenses is important because biases (e.g., overconfidence) can increase risk tolerance

under target/bonus pressure. Thus, risk reporting might fail to translate into action when incentive and monitoring structures do not ensure follow-through, even when risk information is available.

D. Upper Echelons Theory: executive bias and strategic risk-taking

Upper Echelons Theory states that organizational strategy and outcomes reflect the characteristics of top managers (Hambrick & Mason, 1984). For ERM, this theory explains why the "quality of conversion" of risk reports into action is strongly influenced by leadership: executives determine risk appetite, mitigation priorities, and attitudes toward warning signals. If executives view risk as an obstacle to achieving targets, they may encourage a disproportionate risk response (e.g., delaying mitigation or loosening limits). Instead, leadership that values strategic resilience will use risk reporting to inform decisions and resource allocation.

E. Institutional Theory: decoupling ERM and legitimacy

Institutional Theory explains that organizations often adopt formal structures to gain legitimacy, but this practice can be separated from operational activities and actual decision-making (Decoupling) (Meyer & Rowan, 1977). Under institutional pressure and isomorphism, organizations can mimic the ERM framework because it is considered a best practice, even though it has not been internalized (DiMaggio & Powell, 1983). In this framework, the risk reporting action gap is understood as a symptom of decoupling: risk reports are produced as a compliance ritual but do not influence strategic decisions or resource allocation.

F. ERM as a risk–strategy–performance integration (the basis of practice)

As a foothold in practice, COSO places ERM as a framework that integrates risk with strategy and performance, including governance & culture, strategy & objective-setting, performance, review & revision, and information, communication & reporting (COSO, 2017). Meanwhile, ISO 31000 emphasizes risk management principles and processes that can be applied across organizations and embedded in decision-making (ISO, 2018). These two references clarify the standard of "what should have been", so this review focuses on "why it does not happen often": i.e., the behavioral and institutional barriers that interfere with the conversion of reports into action.

3. Method

This study employed a critical narrative review to synthesize cross disciplinary literature and developed a theoretically integrated explanation of the risk reporting action gap in enterprise risk management (ERM). Unlike a systematic review or meta-analysis, this approach did not seek exhaustive coverage of all available studies. Instead, it emphasized interpretive synthesis, conceptual integration, and framework development to explain why risk reports often failed to translate into effective action.

A. Units of analysis and coverage of the literature

The unit of analysis in this review included peer-reviewed journal articles, reputable review articles, and standard documents and practice guidelines referenced by ERM. The literature was organized into three clusters: (1) Behavioral decision-making/behavioral finance (prospect theory, bounded rationality, and cognitive bias in risk decisions), (2) ERM and risk governance (risk reporting, risk culture, escalation mechanism, risk appetite/limit, review-revision, and implementation issues such as decoupling/recoupling), and (3) Strategic management (executive role, discipline in strategic decision-making, and risk, strategy, performance integration). As a normative reference for defining expected ERM practices, this study used COSO ERM and ISO 31000 (COSO, 2017; ISO, 2018).

B. Search Strategy and Literature Identification

To improve methodological transparency, the review was conducted using a purposive, theory-driven literature identification process. The authors first identified anchor sources from core ERM, behavioral decision-making, governance, and institutional theory literature. These anchor sources were selected on the basis of two criteria: (i) foundational importance; it meant that the work had enduring theoretical relevance; and/or (ii) high conceptual relevance to the risk reporting–action gap, ERM implementation, risk appraisal, risk response, governance, or institutional embeddedness. The strategy of using key sources as a foothold for theoretical synthesis and integration was aligned with the practice of conceptual review that emphasized the coherence of arguments and the relevance of the theme, rather than just the number of studies (Grant & Booth, 2009; Snyder, 2019).

The initial identification of anchor literature was supported by searches in major academic databases and scholarly search engines, particularly Scopus, Web of Science, and Google Scholar, complemented by citation tracing. The search emphasis was not on exhaustive retrieval, but on locating literature that was conceptually central to the review objective. Search terms included combinations of keywords such as enterprise risk management, risk reporting, risk culture, cognitive bias, prospect theory, bounded rationality, strategic decision-making, agency theory, upper echelons, decoupling, and risk governance.

C. Inclusion and Exclusion Logic

Sources were retained when they provided clear conceptual, theoretical, or empirical relevance to at least one of the following: (a) behavioral distortions in risk appraisal, (b) barriers in risk response or mitigation follow-through, (c) governance and leadership mechanisms affecting risk decisions, (d) institutional explanations for ERM decoupling, or (e) practical implications for control design. Sources were excluded when they were only loosely related to ERM, focused on risk in a purely technical or quantitative sense without behavioral or organizational implications, duplicated conceptual arguments already sufficiently represented in the selected corpus, or offered limited relevance to the central objective of explaining the risk reporting action gap

D. Literature Expansion through Snowballing

After the anchor sources had been identified, the literature base was expanded through backward and forward snowballing. Backward snowballing involved reviewing the reference lists of anchor studies to locate earlier influential works relevant to risk appraisal, risk response, ERM implementation, governance, and institutional dynamics. Forward snowballing involved identifying more recent studies that cited the anchor sources to capture newer conceptual developments, particularly in risk culture, decision oriented ERM, and decoupling/recoupling. This iterative process continued until theoretical saturation was reached. It was when additional sources no longer yielded materially new themes, mechanisms, or actionable implications relevant to the proposed framework (Grant & Booth, 2009; Snyder, 2019; Wohlin, 2014).

E. Conceptual data extraction and thematic synthesis

Each article that passed the selection was extracted on four elements: (1) key constructs (e.g., framing, loss aversion, overconfidence, speak up, decoupling), (2) mechanisms (how constructs affect risk appraisal or risk response), (3) context (sector, organizational level, strategic decisions, governance), and (4) control implications (practices/tools that resist bias or force action).

Furthermore, a thematic synthesis was conducted to identify a high-level theme and develop an integrative framework that explained the appraisal response mechanism and the barrier to control mapping.

This thematic synthesis approach aligned with the thematic synthesis procedure, which emphasized coding findings, developing descriptive themes, and elevating analytical themes to construct conceptual explanations (Thomas & Harden, 2008).

F. Methodological Position and Reporting Logic

Because this study did not adopt an exhaustive systematic review protocol, it did not claim to cover all available studies in the field. Its strength instead lied in the transparency of the source-selection logic, explicit snowballing procedures, cross disciplinary synthesis, and the development of an integrative conceptual framework with practical implications for control. The analysis was reported in four stages. First, the article established a theory based coding lens by synthesizing behavioral, governance, leadership, and institutional perspectives. Second, it identified the main behavioral barriers that prevented risk reports from being acted on. Third, it integrated these barriers into a two path mechanism comprising a risk appraisal path and a risk response path, with ERM maturity and risk culture serving as key organizational mechanisms. Fourth, it translated these insights into a set of bias-aware risk controls designed to reduce distortion and strengthen action discipline.

4. Result and Discussion

A. Behavioral Barriers: Why Risk Reports Do Not Become Action?

This section synthesizes the literature on behavioral barriers arising at two crucial points: risk appraisal (when risk is assessed and prioritized) and risk response (when mitigation decisions are made and implemented). In addition, social-organizational dynamics, the quality of risk communication, and incentive pressures strengthen the risk-action gap.

1) Bias in Risk Appraisal

In the appraisal stage, the organization converts the information into probability/impact estimates, risk priorities, and mitigation needs. In practice, this process is prone to over-optimism and overconfidence (assessing risk too low and control ability too high), availability bias (the risk of recall was considered greater), and confirmation bias (information that is in line with the initial belief is more trustworthy) (Kahneman & Tversky, 1979; Simon, 1955). As a result, risk registers might appear well-structured while still reflecting bias in risk selection, measurement, and prioritization.

Quantitative studies on civil works mega projects show that cognitive bias influences risk register practices and mitigation effectiveness; for example, *over-optimism* can lower the quality of mitigation decisions because risk is judged "more controlled" than objective conditions (Dulin et al., 2025). Within the COSO framework, appraisal distortion weakens the performance component (risk assessment and prioritization) and disrupts the integration of risk-strategies by allocating mitigation resources to the "wrong" risks (COSO, 2017). In ISO 31000, appraisal bias means that the organization fails to produce the best available information for the basis of decisions (ISO, 2018). The literature points to controls that help with appraisal: scenario standardization, external validation, and structured challenge mechanisms, so that estimates are not only based on internal beliefs (Dulin et al., 2025; ISO, 2018).

2) Bias in Risk Response (Risk Response and Execution)

Even when risks have been reported, mitigation decisions are often delayed, disproportionate, or inconsistent. Prospect theory explains the tendency to delay mitigation actions that are perceived as "definite costs", especially when the benefits probabilistic and long-term (Kahneman & Tversky, 1979). On

the other hand, when an organization feels "below target", risk preferences can shift to more risk-seeking, increasing tolerance for boundary violations or escalation of aggressive strategies.

As a organizational manifestation, response barriers often appear as first, escalation of commitment (maintaining the strategy/project even if the indicators deteriorate). Second, status quo bias (refusal to change resource configuration). And last, delay bias (delaying difficult decisions such as de-risking, hedging, or strengthening capital/liquidity). This mechanism prevents the risk report from becoming a binding corrective decision. The response gap weakens the review and revision (COSO) function because the organization neither learns nor corrects decisions based on risk signals. Governance-wise, this is also related to the misalignment of incentives, as explained by agency theory: short-term targets can override the risk appetite discipline (COSO, 2017; Jensen & Meckling, 1976). Effective response control is usually "binding": automatic triggers when limits are exceeded, dual sign-offs for high-risk decisions, and kill criteria defined from the start so that organizations do not get caught defending wrong decisions (ISO, 2018).

3) Social-Organizational Barriers: Groupthink, Authority Bias, and the "Silence Climate"

Many risks go unaddressed because information does not reach decision-makers or is not prioritized in strategic meetings. Authority bias makes the team reluctant to challenge the leadership's assumptions; Groupthink suppresses the diversity of perspectives; and the "silence climate" weakens the culture of reporting (speak up). In the context of safety/at risk industries, the literature shows the importance of safety voice as a prerequisite for incident prevention (Mathisen et al., 2022).

This barrier explains why risk reporting is often a formality: information is recorded but not "heard" or acted upon. Institutionally, these conditions heightens the potential for decoupling between formal ERM structures and actual decision-making practices (Meyer & Rowan, 1977). Strengthening the speak-up system, protecting whistleblowers, and institutionalizing challenge process practices (e.g., forum risk challenges, red teams) are needed so that risk information do not remain in documents (COSO, 2017; Mathisen et al., 2022).

4) Framing and Risk Communication Failures: When Reports Are Not "Decision-Useful"

Risk reports often fails to drive action because they are not decision-useful: too technical, too many indicators, or inconsistent framing, leading decision-makers to experience attention dilution. Bounded rationality asserts that attention is a scarce resource; reports full of metrics can actually reduce the quality of decisions (Simon, 1955).

In COSO, the information, communication, and reporting domain emphasizes that reporting should support decision-making and accountability. If reporting is not connected to action options, ownership, and priorities, then the ERM function becomes an administrative (COSO, 2017). The ERM literature emphasizing a "decision-oriented" approach encourages reporting that focuses on value drivers and alternative decisions, rather than just a risk inventory (Gleißner & Berger, 2024).

5) Incentive & Target Pressure: Misalignment of KPI and Risk Appetite

Target and incentive pressures can lead organizations to ignore risk signals or delay mitigation. Agency theory posits that without incentive alignment, managers may be driven to pursue short-term growth/returns even though this increase tails risk (Jensen & Meckling, 1976). At the executive level, the upper echelons theory asserts that leadership preferences and biases can shape an organization's risk tolerance (Hambrick & Mason, 1984).

Incentive misalignment can lead to situations in which risk reporting is "correct," but the decision remains unchanged because the reward system supports risky behavior. This explains why improving the report's format alone is often not enough. Strengthening risk-adjusted performance metrics and governance (board oversight and an independent risk committee) is needed for risk appetite to become a truly binding "rules of the game" (COSO, 2017; Jensen & Meckling, 1976).

B. Integrative Framework: Turning Risk Reports into Action

Based on the mentioned synthesis, this article proposes an integrative framework linking behavioral barriers to ERM effectiveness and strategic outcomes through two pathways, Risk Appraisal and Risk Response.

1) Risk Appraisal Path

Appraisal bias (overconfidence, over-optimism, framing, confirmation) → the quality of probability/impact assessments decreases → erroneous mitigation priorities → ineffective mitigation resource allocation → residual risk increases → downside risk/strategy failure. This path emphasizes that the risk reporting–action gap may begin with biased inputs, such as subsequent decisions, even when taken, fail to address the root of the risk problem (Dulin et al., 2025; Kahneman & Tversky, 1979).

2) Risk Response Path

Response bias (status quo, escalation of commitment, delay bias) + target/incentive pressures → delays or inconsistencies of mitigation actions → limit violations/decreased control compliance → increased tail risk/incidents → strategic losses. This path describes cases in which the risk report already highlights the problem, but the organization remains inactive due to behavioral and political factors.

3) The Role of ERM: Mediators and Buffers

ERM as a mediator plays behavioral bias affects the quality of appraisal/response through the effectiveness of the ERM (assessment, monitoring, reporting, review) process. ERM as a buffer (moderator): ERM maturity and a strong risk culture can weaken the impact of bias, for example, through challenge processes, speak-ups, and automatic action triggers (COSO, 2017; ISO, 2018). This is also consistent with the institutional perspective that ERM failures often occur due to decoupling; therefore, a measure of "effectiveness" should assess whether ERM actually influences decisions and resource allocation, rather than exists formally (Jemaa, 2022; Meyer & Rowan, 1977).

C. Bias-Aware Risk Controls: From Barriers to Control Design

This section argues that the risk reporting action gap cannot be addressed simply by increasing reporting frequency or multiplying indicators. What organizations need instead are bias-aware risk controls, namely control mechanisms explicitly designed to reduce behavioral distortions in risk appraisal, strengthen discipline in risk response, and prevent decoupling through governance and risk culture. In this sense, the purpose of control is not merely to generate reports, but to ensure that risk information changes decisions, priorities, and resource allocation in ways that remain consistent with risk appetite.

1) Design Principles of Bias-Aware Controls

First, controls must be decision-oriented: each risk report must be associated with action options, risk owners, deadlines, and consequences if not addressed. This aligns with the idea of risk strategy performance

integration emphasized by COSO, in which reporting and review should facilitate decision making rather than serving as mere risk accounting (COSO, 2017). Second, controls must be in place at critical decision points, such as major investment approvals, expansions, portfolio changes, or product launches, because the most dangerous bias arises when large-value decisions are made under time pressure. Third, control must acknowledge bounded rationality: risk information must be intelligently simplified (not naively simplified), so that decision-makers' attention is directed to the main risk drivers (Simon, 1955). Fourth, control needs to provide space for structured challenge; without an institutionalized "challenger" mechanism, organizations tend to fall into confirmation bias and groupthink, making risk reporting a formality that do not alter initial beliefs.

2) Controls for Risk Appraisal: Resisting Bias in Risk Appraisal

Bias in appraisal leads organizations to mis assess probability and impact. It may cause mitigation priorities to be missed. For this reason, appraisal control needs to strengthen three things: consistent framing, estimation calibration, and assumption validation.

a. Standardization of Scenarios (Base–Downside–Worst Case) and Assumption Sensitivity

Prospect theory suggests that framing influenced risk preferences (Kahneman & Tversky, 1979). Therefore, risk reporting should use a consistent scenario format to reduce "manipulation framing" (both intentional and unintentional). The standardization of scenarios also supports the ISO 31000 principle that risk assessments should provide adequate information for decisions, including the uncertainties and assumptions (ISO, 2018). In practical terms, scenario standardization requires that every strategic risk be reported under at least three conditions (base/downside/worst) and accompanied by sensitivity analyses of key assumptions (e.g., interest rates, liquidity, demand, input costs). Thus, organizations are not only looking at the "averages" but also focusing on the often-overlooked tail.

b. Reference-Class Forecasting and Historical Comparison (Outside View)

Over optimism often arises because organizations rely too heavily on the inside view: "we are different, we can control." To mitigate this distortion, appraisals need to include an outside view by using reference-class forecasting, which compares the estimated risk/probability of success with similar project/product/strategy classes in the past. Empirical findings on megaprojects indicated that cognitive bias can undermine the effectiveness of mitigation by making risks appear more optimistic than they were (Dulin et al., 2025). With historical comparisons, organizations have an empirical anchor that reduces the likelihood of wishful thinking. In ERM practice, the reference class can be historical internal data, industry data, or cross-project/subsidiary benchmarks.

c. Pre-Mortem to Expand Risk Search and Contain Confirmation Bias

Pre-mortem is a technique that asks the team to assume a decision/project that will fail in the future and write down the reasons for the failure. This technique is effective because it forces the team out of the "we will make it" narrative and it expands the set of risks considered. From the perspective of bounded rationality, pre-mortem directs attention to risks that are not usually included in the risk register because they are not "easy to remember" or are considered to disrupt consensus (Simon, 1955). Institutionally, pre-mortems also help reduce social pressure to be "always positive" by providing an official forum to express concerns.

d. Independent Challenge / Red Team as Validation Control

Institutional theory emphasizes that formal structures can be ritualized without any actual defiance (Meyer & Rowan, 1977). Therefore, the appraisal control needs to include an independent challenger function. The red team not only criticizes but also requires to compile a counter-scenario and supporting evidence. In the COSO logic, this strengthens governance, culture, and performance COSO (2017), as risk assessment becomes more robust and less dependent on a single group of decision-makers.

3) Controls for Risk Response: Ensure Mitigation Actions Occur Promptly

The biggest barrier is often the response: risks are already reported, but actions are delayed, deferred, or disproportionate. For this reason, bias-aware response controls need to emphasize commitment devices and automated mechanisms.

a. Hard Limits and Automatic Triggers (Action Triggers)

In many cases, risk reports do not result in action because the decision is still "debated," even though the indicator has crossed the threshold. Hard limits (e.g., concentration limits, duration limits, RBC/solvency thresholds, minimum liquidity buffer) translate risk signals into mandatory actions. COSO emphasizes that risk appetite and tolerance must be linked to performance measurement and response (COSO, 2017; ISO, 2018). Automatic triggers reduce the space for bias, such as delay bias or escalation of commitment: when the threshold is exceeded, actions are pre-set (e.g., hedging, de-risking, capital/liquidity addition, product termination).

b. Dual Sign-Off for High-Risk Results

Agency theory reminds us that managerial decisions can deviate from the organization's interests when monitoring and checks and balances are weak (Jensen & Meckling, 1976). Dual sign-off reduces the risk of biased single point decisions: large investment decisions, aggressive expansions, or portfolio changes can be made only with approval from both the business function and the independent risk/committee function. This mechanism prevents executive overconfidence and, at the same time, reduced the pressure on the target to ignore the risk.

c. Stop-Loss and Kill-Criteria (Exit Rules)

Prospect theory suggests that in the loss domain, decision-makers can become more risk-seeking to cover losses (Kahneman & Tversky, 1979). This explains why organizations sometimes maintain a bad strategy/project (escalation). Stop-loss/kill criteria are exit rules set at the beginning (e.g., a specific drawdown, an RBC falling below the threshold, an ALM mismatch indicator, or a specific risk KPI). Because exit rules are approved before pressure mounts, they serve as a pre-commitment that protects the organization from its own emotional and political decisions.

d. Contingency Playbook to Reduce Reactive Responses

Many risks response fail. It is not because organizations do not know the risks, but because they lack a crisis-ready plan of action (e.g., liquidity runbooks, communication protocols, escalation paths). In high-pressure situations, bounded rationality deteriorates: the organization panics, attention narrows, and decisions become reactive. Playbooks reduce cognitive burden during crises and accelerate action.

4) Controls for Governance and Risk Culture: Prevent Decoupling and Ensure Follow-Through

Institutional theory suggests that ERM failures often involve decoupling: formal structures existed, but do not change practices (Meyer & Rowan, 1977). Therefore, bias-aware controls require strengthening governance and risk culture so that reporting truly influenced decisions.

a. Speak up System + Whistleblower Protection + Risk Culture Metrics

Without speaking up, the risk does not rise to the level of the decision-maker. In the context of safety and at-risk industries, the literature indicates that the ability to voice safety concerns is associated with incident prevention and control quality (Mathisen et al., 2022). An effective speak-up system requires protection against retaliation, follow-up mechanisms, and metrics (e.g., number of near-misses, issue closure time, escalation rate). This shifts organizational culture from passive report archiving to action-oriented risk communication.

b. Risk-Adjusted Incentives

Agency theory emphasizes the importance of incentives; if KPIs focuses solely on growth/return, risk control is easily undermined (Jensen & Meckling, 1976). Therefore, organizations need to link rewards to risk-adjusted indicators (e.g., compliance, downside risk, mitigation quality) to ensure that expected behavior aligned with risk appetite. Within the COSO framework, this strengthens governance and culture while reinforcing the integration of ERM and performance (COSO, 2017).

c. Board Risk Oversight with a Concise and Decision-Focused Dashboard

Board oversight is important to prevent ERM from becoming administrative. However, effective surveillance does not mean many indicators; it should be concise and led to decisions, focusing on concentration, leverage, liquidity, solvency, and tail risk indicators. This kind of reporting reduces bounded rationality and strengthened accountability for (COSO, 2017; Simon, 1955).

5) Integrative Summary: How Bias-Aware Controls "Turn Reports into Action"

Conceptually, bias-aware risk controls work through two simultaneous functions. First, appraisal control improves the quality of decision inputs by resisting framing distortion and over-optimism (Dulin et al., 2025; Kahneman & Tversky, 1979). Second, response control and governance create commitment devices that ensure follow-up, close the delay bias space, and reduce decoupling (COSO, 2017; Meyer & Rowan, 1977). Thus, ERM becomes a strategic decision-making discipline: risk reporting do not stop at a document but become a mechanism that consistently influences priorities, resource allocation, and strategic choices.

The research agenda can place the risk reporting–action gap as an outcome that can be measured and explained through behavioral mechanisms (Prospect Theory, bounded rationality), governance (agency), leadership (upper echelons), and institutional context (decoupling). Thus, future research contributions not only add to the evidence that bias "exists" but also test the effectiveness of specific control and governance designs in transforming risk reporting into risk actions that are consistent with strategy and risk appetite.

5. Conclusion

This review argued that the effectiveness of enterprise risk management should not have been assessed merely by the existence of formal procedures, dashboards, or reporting routines, but also by the extent to which risk information was translated into timely, proportionate, and disciplined action by integrating prospect theory, bounded rationality, agency theory, upper echelons theory, and institutional theory, this article explained the risk reporting action gap through two distinct yet interconnected mechanisms:

distortions in risk appraisal and failures in risk response. In contrast to prior ERM reviews that primarily emphasizes governance structures or implementation architecture, this article highlighted the behavioral and organizational frictions that prevented risk reports from shaping actual decisions. Its main contribution lied in offering an integrative framework that connected behavioral bias, ERM effectiveness, and strategic outcomes, while also proposing a bias aware risk control toolkit to strengthen action discipline. Accordingly, the study advanced the ERM literature by repositioning risk reporting not as an end in itself but as a mechanism that must have culminated in action for ERM to support resilience and strategic performance.

This study had several limitations. First, as a critical narrative review, it did not follow the exhaustive search and screening protocols used in systematic reviews or meta-analyses. Its purpose was conceptual integration rather than comprehensive evidence aggregation. Second, because the ERM and behavioral literature spanned multiple disciplines, key constructs such as risk culture, speak-up behavior, and decoupling may have varied in meaning and operationalization across studies. Third, the control recommendations proposed in this article remained conceptual and should have therefore been validated through future empirical research, including longitudinal, comparative, or quasi experimental designs.

For practitioners, the review suggested that risk reporting became valuable only when accompanied by mechanisms that compelled follow through. Organizations should have therefore complemented conventional ERM routines with bias aware controls, such as scenario standardization, pre-mortems, independent challenge mechanisms, action triggers, dual sign-off procedures, and predefined exit criteria. In addition, governance arrangements and risk culture metrics should have been designed to ensure that reported risks were escalated, discussed, and acted upon rather than merely documented. In this sense, ERM became most effective when it functioned not only as a reporting system, but as a discipline of strategic action.

References

- COSO. (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*.
- DiMaggio, P. J., & Powell, W. W. (1983a). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48(2), 147. <https://doi.org/10.2307/2095101>
- DiMaggio, P. J., & Powell, W. W. (1983b). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Dulin, S., Bredikhin, A., Bridges, N., Williams, L., Keisler, J., Russo, E., & Linkov, I. (2025). Civil works megaprojects: Cognitive biases and lessons for effective risk mitigation. *Project Leadership and Society*, 6, 100198. <https://doi.org/10.1016/j.plas.2025.100198>
- Gleißner, W., & Berger, T. B. (2024). Enterprise Risk Management: Improving Embedded Risk Management and Risk Governance. *Risks*, 12(12), 196. <https://doi.org/10.3390/risks12120196>
- Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>

- Hambrick, D. C., & Mason, P. A. (1984a). Upper Echelons: The Organization as a Reflection of Its Top Managers. *Academy of Management Review*, 9(2), 193–206. <https://doi.org/10.5465/amr.1984.4277628>
- Hambrick, D. C., & Mason, P. A. (1984b). Upper Echelons: The Organization as a Reflection of Its Top Managers. *Academy of Management Review*, 9(2), 193–206. <https://doi.org/10.5465/amr.1984.4277628>
- ISO. (2018). *ISO 31000:2018 Risk management — Guidelines*.
- Jemaa, F. (2022). Recoupling work beyond COSO: A longitudinal case study of Enterprise-wide Risk Management. *Accounting, Organizations and Society*, 103, 101369. <https://doi.org/10.1016/j.aos.2022.101369>
- Jensen, M. C., & Meckling, W. H. (1976a). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Jensen, M. C., & Meckling, W. H. (1976b). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Kahneman, D., & Tversky, A. (1979a). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263. <https://doi.org/10.2307/1914185>
- Kahneman, D., & Tversky, A. (1979b). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263–292. <https://doi.org/10.2307/1914185>
- Mathisen, G. E., Tjora, T., & Bergh, L. I. V. (2022). Speaking up about safety concerns in high-risk industries: Correlates of safety voice in the offshore oil rig sector. *Safety Science*, 145, 105487. <https://doi.org/10.1016/j.ssci.2021.105487>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Simon, H. A. (1955a). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(1), 99. <https://doi.org/10.2307/1884852>
- Simon, H. A. (1955b). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(1), 99–118. <https://doi.org/10.2307/1884852>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8(1), 45. <https://doi.org/10.1186/1471-2288-8-45>
- Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, 1–10. <https://doi.org/10.1145/2601248.2601268>