Strengthening ERM Independence: A Conceptual Governance and Oversight Framework

Shaharin Abdul Samad[1]

[1] Governance & Assurance Professional, Malaysia

Correspondence: Dr. Shaharin Abdul Samad, Governance & Assurance Professional, Malaysia. E-mail: shaharin.abdulsamad@gmail.com

Received: September 1, 2025 Accepted: October 1, 2025 Online Published: October 23, 2025

doi:10.5430/ijfr.v16n3p63 URL: https://doi.org/10.5430/ijfr.v16n3p63

Abstract

In the rapidly evolving and increasingly volatile global business landscape, robust governance mechanisms are no longer a matter of best practice but are essential for organizational sustainability, resilience, and long-term value creation. At the heart of effective enterprise risk management (ERM) lies not only the sophistication of risk identification and mitigation processes, but also, critically, the unfettered structural independence of the risk management function. This conceptual paper examines the structural and behavioral impediments to ERM independence under prevailing corporate governance models. It analyzes three common reporting structures for the ERM function: reporting to senior management, reporting to the Chief Executive Officer (CEO), and a hybrid model of reporting to the Board of Directors with a "dotted line" to the CEO. This study contends that each paradigm, based on agency theory and corporate governance principles, harbors intrinsic conflicts of interest that undermine the impartiality, authority, and overall efficacy of Enterprise Risk Management (ERM). The CEO's impact on performance evaluations and compensation, even in a dotted-line relationship, is seen as a substantial threat to behavioral independence. Consequently, this paper develops a conceptual framework for an optimal reporting structure. It posits that true independence is only achievable when the ERM function reports directly and exclusively to the Board of Directors or a dedicated Board Risk Committee. Furthermore, the framework asserts that the remuneration, budget, and resources of the ERM function must be determined at the Board level, completely insulated from management's influence. This proposed model, termed the "Unfettered Guardian" framework, is designed to align the ERM function with the Board's oversight duty, ensuring it serves its primary purpose as an objective guardian of shareholder value and long-term organizational sustainability.

Keywords: enterprise risk management, corporate governance, independence, reporting structure, agency theory, chief risk officer, board of directors

1. Introduction

The 2008 financial crisis, the problems with supply chains that followed it, and the instability of geopolitics are just a few examples of global disasters that have reminded us of the need to do a better job of managing risk. Due to a regular stream of high-profile company failures and huge economic shocks, people worldwide are increasingly thinking about risk in a different way. In the early 2000s, Enron and WorldCom faced significant problems with their business operations, demonstrating that inadequate risk governance was not merely a technical failing but an existential threat to both individual firms and the global economic system. The fraudulent scandal expose of 1Malaysia Development Berhad (1MDB), which also involves several other countries, has served as a stark reminder that these lessons are easily forgotten. These seismic events, alongside a steady drumbeat of pervasive modern disruptions from sophisticated state-sponsored cyberattacks and global supply chain breakdowns to the unprecedented operational stress of a global pandemic, have thrust the discipline of enterprise risk management from the corporate periphery to the strategic core (Aabo et al., 2005). Organizations are compelled to look beyond traditional, siloed approaches to risk, embracing a holistic and integrated perspective known as ERM. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value" (COSO, 2017). This definition underscores a critical evolution: ERM is no longer a peripheral, compliance-driven function but a core component of strategic decision-making.

However, the integration of ERM into strategy creates a fundamental tension. The function is tasked with providing an objective, and often challenging, perspective on the very strategies and operations championed by senior management and the CEO. The effectiveness of this challenge function is wholly dependent on its independence. As Fraser and Simkins (2016) contend, "for ERM to be successful, the risk management function must have sufficient authority and independence to ensure that risk is considered in all key business decisions." **In the absence of this independence, the ERM function may devolve into a subservient unit that justifies management's decisions instead of critically evaluating them, thereby neglecting its fundamental responsibility to the organization and its shareholders.**

In response to this new reality, a powerful global consensus has emerged among regulators, investors, and professional bodies: the ultimate accountability for risk oversight rests unequivocally with the board of directors (Brewer & Walker, 2014). This principle is no longer a soft recommendation but a codified expectation. Leading risk frameworks from COSO and the Institute of Internal Auditors (IIA) now view the board's role not as a passive reviewer of historical reports but as an active and engaged governor of the organization's risk appetite and risk-taking activities (COSO, 2017; IIA, 2025). The board is expected to set the "tone at the top," scrutinize management's assumptions, and ensure the strategy is executed within a clearly defined risk framework.

However, in this developed context, a critical and dangerous paradox remains. Despite corporate charters, annual reports, and governance statements emphasizing the "independence" of the risk management function, many organizations exhibit a notable disconnect in practice. The prevailing practice of situating the head of risk management, typically the Chief Risk Officer (CRO), with a direct reporting line to a member of the C-suite, most commonly the CEO or Chief Financial Officer (CFO), creates an inherent and unavoidable structural conflict (PwC, 2025). This arrangement intertwines the risk function, whose primary purpose is to provide objective oversight and challenge, with the very executive management whose strategic decisions and performance it is meant to scrutinize (Corporate Compliance Insights, 2025). The CRO is, in effect, asked to police their own boss, a situation fraught with peril for objective reporting and akin to asking a film critic to write an impartial review of a movie in which they hold the leading role.

This paper addresses a critical and persistent challenge in corporate governance: the structural and behavioral erosion of ERM independence resulting from insufficient reporting lines. The literature emphasizes the significance of Enterprise Risk Management (ERM); however, the necessary organizational framework to uphold its independence is an issue of contention with variable implementation. This conceptual analysis aims to address the essential question: What is the ideal reporting structure that ensures the structural and behavioral independence of the ERM function, thus enhancing its efficacy as a mechanism for board-level oversight and safeguarding shareholder value?

This study reviewed literature on ERM, corporate governance, and the principle of independence, drawing heavily on agency theory. This had led to the development of the study's conceptual framework, which is based on the pillars of structural and behavioral independence. This framework will be used to deconstruct three common reporting scenarios: ERM reporting to senior management, to the CEO, and to the Board, but with a "dotted line" to the CEO. Based on the governance gaps in these scenarios, the **Unfettered Guardian** framework is proposed. In this framework, the ERM function has a direct, solid-line reporting relationship to the Board of Directors, with its remuneration and resources determined exclusively at the Board level. This structure, it is argued, is the only viable path to ensuring the ERM function can fulfill its promise as an impartial and effective guardian of the enterprise.

2. Literature Review: The Strategic Mandate of Modern ERM

The paradigm of risk management has undergone a dramatic shift over the past two decades. Initially viewed as a cost center focused on insurable hazards and financial hedging, risk management has been reconceptualized as a strategic enabler. Nocco and Stulz (2006) were early proponents of this view, arguing that the goal of ERM is not to eliminate risks but to manage the firm's risk profile to maximize shareholder value. The COSO (2017) framework, Enterprise Risk Management - Integrating with Strategy and Performance, emphasizes the significance of aligning risk appetite and tolerance with strategy setting. As Gates and Hexter (2005) noted, a mature ERM program "provides a process for management to have a more holistic view of risks and to understand the interrelationships of risks so they can be managed on an enterprise-wide basis." This holistic view is designed to empower the Board and senior management to make more informed decisions, allocate capital more efficiently, and capitalize on opportunities with a clear understanding of potential downsides. For this strategic partnership to operate effectively, the information and analysis provided by the ERM function must remain impartial and free from internal political influences or conflicts of interest.

2.1 Theoretical Underpinnings of the Principle of ERM Independence

At its core, corporate governance is the system of rules, practices, and processes by which a company is directed and controlled. A central theme in governance literature is the mitigation of the principal-agent problem. Jensen and Meckling's (1976) pivotal work on agency theory suggests that a conflict of interest exists between the principals (shareholders) and their agents (management). Managers may prioritize personal interests, such as short-term bonuses or career advancement, at the expense of long-term value creation for shareholders. The Board of Directors serves as the primary mechanism to oversee management on behalf of shareholders. To be effective, oversight functions must be independent of those they oversee. This principle is firmly established for the external and internal audit functions. The Sarbanes-Oxley Act of 2002, for instance, dramatically strengthened the independence requirements for audit committees and external auditors. Similarly, the Institute of Internal Auditors (IIA) standards state that the chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities and that "the internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results" (IIA, 2017).

This same logic must be rigorously applied to the ERM function. The Chief Risk Officer (CRO) and their team are, in effect, an extension of the Board's oversight capabilities into the forward-looking, strategic realm of risk. If internal audit provides assurance on past and present controls, ERM provides insight and challenge on future uncertainties. Beasley, Clune, and Hermanson (2005) found that organizations with a standalone CRO are more likely to have a fully developed ERM process. They argue that this dedicated leadership role signifies a commitment to risk management, but its effectiveness is contingent upon the organization's standing. Therefore, the independence of the ERM function is not merely a procedural nicety; it is a fundamental prerequisite for effective corporate governance in a complex and uncertain world. As Power (2009) cautions, when risk management becomes overly procedural or "a management-owned process, it can become part of the problem rather than the solution," creating a dangerous illusion of control.

Agency Theory and Information Asymmetry: The agency theory examines the inherent conflicts of interest that arise when control of a firm is separated from its ownership (Jankensgard, 2019). In this model, "principals" (shareholders represented by the board) engage "agents" (executive management) to manage the organization on their behalf. Agency theory suggests that agents may be motivated to adopt strategies that enhance their personal utility, such as short-term bonuses and career progression, instead of focusing on the long-term value for principals. A critical problem arising from this dynamic is **information asymmetry**, a condition where management possesses a far more detailed, timely, and nuanced understanding of the organization's risks and opportunities than the board (Vlerick Business School, 2022). A CRO reporting to the CEO or CFO is susceptible to both explicit and implicit pressure to filter, delay, or dilute risk information that might threaten to reflect poorly on their performance. A direct reporting line to the board acts as a powerful structural mechanism to mitigate this asymmetry, piercing the managerial veil and providing the principals with an unmediated channel for objective risk intelligence (Jankensgard, 2019). This structure directly reduces the "monitoring costs" that principals must incur to oversee their agents.

Stewardship Theory as a Counterpoint: Agency theory presents a critical perspective, whereas Stewardship Theory asserts that managers may not be intrinsically self-interested but can act as effective "stewards" of the organization, driven by aspirations for achievement and organizational success. While this may be true of many executives, governance frameworks cannot be designed only for best-case scenarios. Even well-intentioned stewards are subject to cognitive biases, such as over-optimism or confirmation bias. A structurally independent risk function, therefore, serves a vital purpose even in a stewardship model: it provides objective, data-driven challenges to prevent strategic drift and ensure that decisions are being made with a clear-eyed view of the potential downsides.

The Three Lines Model: The concept of structural independence is further operationalized by the Institute of Internal Auditors' (IIA) widely adopted Three Lines Model. This model delineates clear roles and responsibilities to create a robust system of checks and balances:

i. **The First Line** consists of operational management, which owns and takes risks. This includes the CEO and the C-suite, who make daily decisions and manage business processes.

ii. **The Second Line** is the ERM function (along with compliance, legal, etc.), which provides expertise, oversight, and challenge to the first line. It helps establish risk management frameworks, policies, and tools.

iii. **The Third Line** is internal audit, which provides independent and objective assurance to the board that the first two lines are functioning effectively.

The integrity of this entire model is centered on the independence of the second and third lines from the first. When the CRO (second line) reports directly to the CEO (first line), the lines become fundamentally blurred, compromising the model's design. This reporting structure curtails the second line's ability to objectively challenge the first line, as its leader is beholden to the very executive they are meant to oversee (IIA, 2025).

Foundational ERM Frameworks: Leading ERM frameworks such as the COSO Enterprise Risk Management - Integrating with Strategy and Performance explicitly identify "Governance and Culture" as the foundational component upon which all other ERM activities are built (COSO, 2017). The framework emphasizes that an organization's governance structure is a tangible manifestation of its risk culture and "tone at the top". A structure that subordinates risk management signals that it is a secondary, compliance-driven concern. Similarly, ISO 31000 advocates for a structure that ensures risk management is fully integrated into all organizational activities, a feat that requires the risk function to have the stature and independence to engage at the highest levels of the organization (The Institute of Risk Management, n.d.).

2.2 The Critical Role of Reporting Structures

An organization's reporting structure is the formal framework that governs authority and communication within the organization. It dictates who is accountable to whom and determines the flow of information. For a function like ERM, the reporting line is a powerful signal of its authority, priority, and, most importantly, its independence. A study by Lundqvist (2015) examined the role of the CRO and found that their organizational status and reporting line significantly impact their ability to influence decision-making. A CRO buried within a finance or legal department has a fundamentally different level of influence than one who reports directly to the CEO or the Board. However, a high-level reporting line does not automatically guarantee independence. The distinction between a "solid line" and a "dotted line" relationship is critical. This sentiment is echoed by Leblanc and Gillies (2005), who assert that "independence from management is crucial" for oversight functions and that this independence is "achieved through reporting relationships, terms of reference, and the attitude and actions of the board."

2.3 Remuneration as a Lever of Influence

The relationship between remuneration and behavior is a recognized principle in organizational theory and economics. Executive compensation schemes are designed to align management's interests with those of shareholders. However, they can also create powerful incentives for behavior that may be detrimental to the long-term health of the firm. Bebchuk and Fried (2004) argue that flawed compensation designs can encourage excessive risk-taking and a focus on short-term stock performance at the expense of sustainable growth. This dynamic significantly influences the independence of ERM. A significant conflict of interest arises when the CEO, whose compensation is closely linked to meeting specific financial targets, determines the CRO's bonus, salary increases, and career prospects. The CRO is implicitly (or explicitly) incentivized to downplay or suppress information about risks that could jeopardize the achievement of those targets. A report by the Senior Supervisors Group (2008), was damning in its assessment of this issue. It was found that in many failed financial institutions, the risk management function lacked sufficient stature and its leaders "were not always provided with compensation and other rewards consistent with the stature of their roles." The report strongly recommended that the CRO's compensation be determined independently of the business lines they oversee. This principle must be extended to independence from the CEO, who is ultimately the chief executive of all business lines. The decision-making power over the CRO's livelihood is the ultimate test of their behavioral independence.

2.4 Empirical Evidence and the Regulatory Response

The theoretical arguments for independence are strongly supported by empirical research and regulatory action. Numerous studies have found a positive association between a dedicated, board-facing CRO and superior corporate performance, particularly in terms of reducing stock price volatility and improving risk-adjusted returns (Beasley et al., 2005; Gatzert & Martin, 2015). Other research has linked independent risk oversight to higher-quality, more transparent risk disclosures and greater organizational resilience during economic downturns (Paape & Spekle, 2012). Case-based literature from institutions like North Carolina State University's ERM Initiative further reinforces these findings, highlighting instances where the CRO's independence and direct line to the board were critical factors in successfully navigating crises (North Carolina State University ERM Initiative, n.d.).

Benchmarking studies reveal a clear trend: organizations in highly regulated sectors, such as financial services, are far more likely to have their risk leaders report functionally to the board (Risk Leadership Network, 2022). This is not an accident; it is a direct consequence of the global regulatory response to corporate failures of catastrophic proportions. The 2008 financial crisis accelerated this regulatory focus exponentially. The international banking standards under

Basel III imposed stringent risk management requirements on systemically important financial institutions, including the mandate for board-level risk committees with direct oversight of the risk function (Diligent, n.d.). Similarly, the Solvency II directive in the European insurance industry requires a distinct and independent risk management function. Governance codes, such as the UK Corporate Governance Code, have moved in the same direction, requiring boards to demonstrate explicit and continuous oversight of risk and establish effective controls. Although these regulations mainly focus on large or financial firms, they clearly delineate best practices that are progressively being embraced by prominent organizations in various sectors.

2.5 Challenges and Legitimate Counterarguments

Despite the compelling case for direct board reporting, it is essential to acknowledge and address potential challenges and counterarguments. Critics raise several valid concerns that must be managed for the model to be effective. First is the risk of operational disconnection, where a board-facing CRO may become an "ivory tower" academic, isolated from the daily flow of information, strategic discussions, and operational realities of the business. A second concern is the potential to overburden the board with excessive operational details, blurring the critical line between governance (the board's role) and management (the executive's role) (Harvard Law School Forum on Corporate Governance, 2025). The board's job is not to manage risk on a day-to-day basis, but to ensure that an effective system for doing so is in place. Third, it is contended that a Chief Risk Officer (CRO) reporting to the board may lead to an adversarial relationship with the Chief Executive Officer (CEO), potentially fostering a culture of mistrust instead of collaboration and undermining the cohesion of the executive team.

3. Conceptual Framework: Visualizing the Structural Shift

This paper proposes a conceptual framework to systematically analyze the efficacy of various reporting structures, focusing on two distinct yet interconnected dimensions of independence: Structural and Behavioral Independence. The optimal ERM structure, what we term the "Unfettered Guardian" model, maximizes both dimensions.

3.1 Core Concepts

1. Structural Independence: This refers to the formal placement of the ERM function within the organizational hierarchy, as depicted on an organizational chart. It is defined by the solid-line reporting relationship. High structural independence means the function has a direct, unfiltered, and authoritative channel to the ultimate governing body responsible for shareholder oversight, which is the Board of Directors. It is an objective measure of formal authority and status granted to the function.

Key Indicator: A solid-line reporting relationship directly to the Board of Directors or a primary committee thereof (e.g., the Board Risk Committee).

2. Behavioral Independence: This refers to the ERM function’s freedom from undue influence, coercion, or pressure from management in its day-to-day operations, analysis, and communication. It is independence in fact, as opposed to independence in appearance. While structural independence is a necessary condition, it is not sufficient to guarantee behavioral independence. Behavioral independence is compromised when parties outside the formal reporting line hold significant influence over the function's personnel, resources, or outputs.

Key Indicators:

i. Control over the hiring, firing, and remuneration of the CRO and key ERM personnel.
ii. Control over the budget and resources allocated to the ERM function.
iii. The absence of informal pressures to alter, delay, or soften risk reporting.
iv. The ability of the ERM function to determine its own scope of work and risk assessments without management interference.

3.2 The Central Propositions

Based on this framework, this paper puts forward three central propositions:

Proposition 1: ERM reporting lines directed exclusively to executive management (e.g., the CEO or other C-suite members) critically undermine both structural and behavioral independence. In this model, the ERM function is structurally subordinate to the very individuals and activities it is meant to oversee, creating an irreconcilable conflict of interest.

Proposition 2: A hybrid model featuring a solid line to the Board but a “dotted line” to the CEO creates an illusion of independence while fundamentally compromising behavioral independence. The CEO's influence over performance

management and remuneration through the dotted-line relationship creates a powerful incentive for the CRO to align with management's perspective, thus diluting the objectivity of risk reporting to the Board.

Proposition 3: Optimal ERM independence and effectiveness are achieved only through the Unfettered Guardian model, characterized by (a) an exclusive, solid-line reporting relationship from the CRO to the Board or a Board-level Risk Committee and (b) exclusive Board-level control over the ERM function's remuneration, budget, and resources. This structure maximizes both structural and behavioral independence, aligning the ERM function squarely with the oversight mandate of the Board and the long-term interests of shareholders. This framework provides the analytical lens through which to dissect the common, yet flawed, reporting structures prevalent in many organizations today.

4. Discussion: Analyzing the Scenarios Through the Lens of Independence

The conceptual framework illustrates a clear choice: organizations can either maintain a traditional structure that is administratively simple but fraught with governance flaws, or they can adopt a more contemporary model that structurally embeds the independence necessary for effective risk oversight. This section delves deeper into the practical implications of making this choice, analyzing the primary barriers to its implementation and presenting a comprehensive framework of best practices.

4.1 The Three Common Scenarios

Applying the conceptual framework, we can now systematically evaluate the three common reporting scenarios and demonstrate their inherent weaknesses, ultimately justifying the proposed ideal model.

Scenario 1: ERM Function Reports to Senior Management (e.g., CFO)

In many organizations, particularly those where ERM evolved from a financial or insurance-buying function, the CRO reports to the Chief Financial Officer (CFO) or Chief Operating Officer (COO). This structure is deeply problematic from an independence perspective. From a **structural independence** standpoint, the model fails completely. The ERM function is several steps removed from the Board of Directors. Its reports and concerns are filtered through a C-suite executive whose own role and responsibilities may be a primary source of enterprise risk. For instance, a CFO is responsible for financial reporting, capital structure, and investor relations. Placing the ERM function under the CFO subordinates the holistic view of risk to a predominantly financial one. As Arena, Arnaboldi, and Azzone (2010) observe, when ERM is confined within a specific function like finance, it struggles "to achieve a really 'enterprise-wide' perspective." Strategic or operational risks that might challenge the CFO's financial projections or capital allocation plans may be downplayed or ignored. From a **behavioral independence** perspective, the conflict is even more acute. The CRO reports directly to the CFO. Their performance review, salary, bonus, and career progression are entirely in the CFO's hands. It is organizationally and psychologically untenable to expect a CRO to vigorously challenge the strategic assumptions or operational plans of the very executive who controls their professional fate. The CRO effectively becomes an advisor to the CFO, not an independent assessor for the Board. This structure positions ERM as a support function for management, rather than an oversight function for the Board, fundamentally misaligning its purpose with the principles of sound corporate governance.

Scenario 2: ERM Function Reports to the Chief Executive Officer (CEO)

Positioning the CRO as a direct report to the CEO is often seen as a significant step up from reporting to another C-suite member. It elevates the status of the risk function and signals that risk is a top-level priority for the CEO. Proponents might argue that this structure ensures risk is integrated into top-level strategic conversations. While an improvement on the first scenario, this model still fatally compromises independence. **Structural independence** is moderately improved, as the CRO is only one step from the Board. However, the channel is still fully controlled and filtered by the CEO. The Board receives its risk information from or through the CEO, who has the power to frame, interpret, and potentially omit information. The Board is denied a direct, unfiltered view of the organization's risk landscape as seen by the ERM function. The fundamental flaw, however, lies in the complete erosion of **behavioral independence**. The CEO is the ultimate agent in agency theory, responsible for executing strategy and delivering performance. The ERM function's primary role is to provide an objective challenge and analysis of the risks inherent in a strategy and its execution. This places the CEO in an impossible position, being both the primary risk-taker and the direct superior of the primary risk overseer. As noted by the Walker Review of corporate governance in UK banks, "the effectiveness of the CRO is critically dependent on his or her independence from the executive pressures of the 'business-getters'" (Walker, 2009). The CEO is the chief "business-getter." The CRO's compensation is tied directly to the CEO's appraisal. If the CEO's bonus is contingent on hitting an ambitious revenue target, the CRO faces immense pressure to concur with risk assessments that support the underlying strategy, even if they have private reservations. To raise a significant red flag could be perceived as disloyalty or obstruction, with direct negative consequences for the

CRO's performance rating and financial reward. This structure incentivizes conformity and discourages the very "objective challenge" that ERM is meant to provide. It transforms the CRO from a guardian into a subordinate advisor, whose counsel is valued only as long as it aligns with the CEO's objectives.

Scenario 3: "Dotted Line" to the CEO, Solid Line to the Board

This hybrid model has become increasingly popular as organizations attempt to address the obvious conflicts of the previous two scenarios. On paper, it appears to be the ideal compromise. The solid line to the Board (often to the Chair of the Audit or Risk Committee) grants the CRO the necessary **structural independence** and a direct channel for reporting. The dotted line to the CEO serves to ensure the CRO's involvement in the daily strategic and operational activities of the business. As one risk practitioner noted, "Without a strong relationship with the CEO, the CRO is seen as an 'ivory tower' function, disconnected from the realities of the business" (quoted in Rittenberg & Martens, 2012). Despite its apparent sophistication, this model is deceptive because it creates a veneer of independence that masks a critical weakness in **behavioral independence**. The key question is: who really controls the CRO's fate? In most organizations that employ this model, the "dotted line" to the CEO is where substantive power resides. The CEO typically provides the primary input for the CRO's performance review. The CEO recommends, or has heavy influence over, the CRO's salary adjustment and annual bonus. The CRO depends on the CEO for political capital, access to information, and cooperation from other business units. This dependency creates a powerful "dual reporting" conflict. The CRO is forced to serve two masters with potentially divergent interests. The Board desires unfiltered, objective risk analysis. The CEO, while also concerned with risk, is primarily judged on performance and may desire a more "constructive" or "business-friendly" risk partner. When a major risk issue arises, the CRO faces a difficult choice. Do they report the unvarnished, potentially alarming truth directly to the Board, risking the wrath of the CEO who controls their compensation and daily working life? Or do they work with the CEO to frame the issue in a more palatable way, thereby compromising their duty to the Board?

Lam (2014) emphasizes that the CRO must have "unquestioned independence" and that this is often achieved by having compensation "determined by the board's compensation committee." The dotted-line structure directly contradicts this principle. It creates subtle but pervasive pressure on the CRO to view the CEO as their primary client. The "good news" culture that the user's prompt alluded to becomes a significant risk. The CRO may filter information, use softer language in reports to the Board, or delay reporting on emerging issues until a "management solution" is in place. This filtering process defeats the very purpose of having an independent risk function, leaving the Board with a sanitized view of the organization's risk profile, which can lead to catastrophic failures of oversight.

4.2 The Proposed Solution: The Unfettered Guardian Model

The preceding analysis demonstrates that common ERM reporting structures are built on a foundation of compromised independence. To remedy this, a new model is required, one that is unambiguous in its alignment and uncompromised in its structure. The **Unfettered Guardian** model is founded on the third proposition: true independence requires an exclusive reporting line to the Board, with commensurate Board-level control over resources and remuneration.

This model is defined by two non-negotiable characteristics:

1. Exclusive Solid-Line Reporting to the Board of Directors: The CRO must report directly and solely to the Board, typically through a dedicated Board Risk Committee or, in its absence, the Audit Committee. There should be no reporting line, solid or dotted, to the CEO or any other member of management. This establishes unequivocal **structural independence**. The CRO's mandate flows directly from the shareholders' representatives, not from the management they are tasked with overseeing. Communication is direct and unfiltered. The Board sets the agenda for the ERM function, reviews its findings directly, and participates in executive sessions with the CRO, excluding management. This ensures the Board receives an unvarnished perspective. This does not mean the CRO operates in a vacuum, isolated from the business. A highly effective CRO must maintain strong working relationships with the CEO and the executive team. However, the nature of this relationship changes from one of subordination to one of partnership and constructive tension. The CRO engages with management as an equal peer, empowered by the authority of the Board. Their role is to advise, consult, and challenge management; however, their ultimate accountability lies with the Board.

2. Board-Level Control of Remuneration and Resources: To ensure **behavioral independence**, the structural line must be reinforced by severing all dependencies on management. Under the Unfettered Guardian model:

i. **Remuneration:** The Board's Remuneration Committee, based on input from the Chair of the Risk or Audit Committee, determines the CRO's entire compensation package (salary, bonus, equity). Performance metrics should be based on the quality and effectiveness of the risk framework, the timeliness and accuracy of risk

reporting, and the maturity of the organization's risk culture, not on the company's financial performance, which could create a perverse incentive to condone excessive risk-taking.

ii. **Hiring and Firing:** The decision to hire or terminate the CRO rests solely with the Board. The CEO may be consulted, but the Board holds the final authority.

iii. **Budget and Resources:** The budget for the ERM function is submitted by the CRO directly to the Board's relevant committee for review and approval. This prevents management from starving the function of resources as a means to curtail its activities or express displeasure with its findings.

This model assigns critical levers of power solely to the Board, thereby removing the conflict-of-interest present in alternative scenarios. The CRO's loyalty is now unified, where their objective is to deliver the Board with precise, objective, and future-oriented risk intelligence, thereby fulfilling their responsibility as a genuine guardian of the enterprise for its ultimate owners.

4.2.1 Implications and Recommendations

The adoption of the Unfettered Guardian model has significant implications for corporate practice and governance.

For Boards of Directors: Boards must move beyond merely accepting the appearance of independence and actively design a structure that ensures it. This requires amending committee charters and governance policies to establish a direct, solid-line reporting relationship between the CRO and the Board, and to explicitly state that the Board retains sole authority over the CRO's appointment, evaluation, compensation, and dismissal. Board members, particularly on Risk and Audit committees, must cultivate a direct and open relationship with the CRO, ensuring they are a trusted advisor to the Board, not just a reporter of information curated by management.

For Regulators and Standard-Setters: Regulatory bodies and governance standard-setters, such as COSO and the IIA, should provide clearer and more forceful guidance on the necessity of this reporting structure, particularly in systemically important industries. While principles-based guidance is valuable, the pervasive nature of the conflict of interest in ERM reporting may warrant more prescriptive rules. The standard for ERM independence should be just as rigorous as that for external and internal audits.

For Management: CEOs and senior executives need to adopt a new mindset. An independent ERM function should not be perceived as an internal opponent or a bureaucratic obstacle. It should be regarded as an essential strategic partner that improves decision-making and safeguards the organization against significant blind spots. An independent CRO offers the CEO a credible and objective perspective, essential for effectively navigating a complex risk landscape. By endorsing this model, a CEO communicates to investors and regulators a strong dedication to effective governance and enduring sustainability.

For Future Research: This study introduces a conceptual framework, and empirical research is warranted to validate its propositions. Future research may quantitatively analyze the relationship between ERM reporting structures and business performance, especially in times of economic stress. Qualitative studies that include interviews with board members, CEOs, and CROs may yield deeper insights into the nuanced political and behavioral dynamics affecting the effectiveness of Enterprise Risk Management across various reporting models. This conceptual model could also be extended to cover other governance-related fields such as Internal Audit.

5. Conclusion

The promise of Enterprise Risk Management to protect and create value through intelligent risk-taking can only be realized if its foundational pillar, independence, is unshakeable. This paper has argued that the most common reporting structures in use today, while often well-intentioned, are fundamentally flawed. Reporting to senior management subordinates' risk to a specific silo. Reporting to the CEO creates a direct and untenable conflict of interest. The popular hybrid model, with a dotted line to the CEO, creates a dangerous illusion of independence while leaving the CRO behaviorally beholden to the very executive they are meant to challenge. The conceptual framework proposed, built on the twin pillars of structural and behavioral independence, leads to an unequivocal conclusion. To be a truly effective guardian of shareholder value, the ERM function must be unfettered. The Unfettered Guardian model, characterized by an exclusive, solid-line reporting relationship to the Board and Board-level control over remuneration and resources, is the only structure that eliminates inherent conflicts of interest and aligns the ERM function with its primary stakeholders. **The implementation of this model necessitates determination and commitment from the Boards of Directors**. This necessitates a reassessment of conventional organizational structures and a sophisticated comprehension of the function of constructive tension in effective governance. In a time of significant uncertainty, organizations must empower their risk management professionals without restraint, regardless of the duration or

subtlety of such limitations. An independent ERM function is essential for providing the governance and objective oversight required to address future challenges and achieve long-term, sustainable success.

Acknowledgments

We greatly appreciate the valuable contributions and moral support from Abdul Samad Mohd Haroun, Nurliza Abdullah, Rina Ammy T. Jani, Shaheem Reza Shaharin and Sharmeen Rose Shaharin.

Authors' contributions

The author was responsible for all aspects of this work, including the conceptualization, methodology, investigation, data analysis, and the writing of the manuscript.

Funding

The author independently funded this work as a contribution to the discipline of Governance and Assurance.

Competing interests

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Sciedu Press.

The journal and publisher adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

References

Aabo, T., Fraser, J., & Simkins, B. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at Hydro One. *Journal of Applied Corporate Finance, 17*(3), 5-5.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society, 35*(7), 659-675. https://doi.org/10.1016/j.aos.2010.07.003

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24*(6), 521-531. https://doi.org/10.1016/j.jaccpubpol.2005.10.001

Bebchuk, L. A., & Fried, J. M. (2004). *Pay without performance: The unfulfilled promise of executive compensation*. Harvard University Press.

Brewer, P. C., & Walker, P. L. (2014). Risk oversight: Evolving expectations for boards. *Strategic Finance, 96*(1), 22-33.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*.

Corporate Compliance Insights. (2025). *Positioning the CRO to succeed*. Retrieved from https://www.corporatecomplianceinsights.com/positioning-the-cro-to-succeed/

Diligent. (n.d.). *Corporate governance reporting: Definition, requirements & best practices*. Retrieved from https://www.diligent.com/resources/blog/corporate-governance-reporting

Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons, 59*(6), 689-698. https://doi.org/10.1016/j.bushor.2016.06.007

Gates, S., & Hexter, E. S. (2005). *From the inside out: What makes a company a good risk manager?*. The Conference Board.

Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: Empirical evidence from Germany. *Risk Analysis, 35*(2), 226-246. https://doi.org/10.1111/risa.12285

Harvard Law School Forum on Corporate Governance. (2025, June 23). *Board effectiveness: A survey of the C-suite*. Retrieved from https://corpgov.law.harvard.edu/2025/06/23/board-effectiveness-a-survey-of-the-c-suite-4/

Institute of Internal Auditors (IIA). (2017). *International standards for the professional practice of internal auditing (Standards)*.

Institute of Internal Auditors. (2025). *The IIA's three lines model: An update of the three lines of defense*. Retrieved from https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

Institute of Risk Management, The. (n.d.). *From the cube to the rainbow double helix: A risk practitioner's guide to the COSO ERM frameworks*. Retrieved from https://www.theirm.org/media/6885/irm-report-review-of-the-coso-erm-frameworks-v2.pdf

Jankensgard, H. (2019). A theory of enterprise risk management. *Corporate Governance: The International Journal of Business in Society, 19*(2), 286-304. https://doi.org/10.1108/CG-05-2018-0172

Jensen, M. C., & Meckling, W. H. (1976). 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

Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed.). John Wiley & Sons.

Leblanc, R., & Gillies, J. (2005). *Inside the boardroom: How to be an effective director*. John Wiley & Sons.

Lundqvist, S. A. (2015). Why do firms implement enterprise risk management? The role of the chief risk officer. *Journal of Accounting and Public Policy, 34*(3), 394-419. https://doi.org/10.1016/j.jaccpubpol.2015.04.002

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance, 18*(4), 8-20. https://doi.org/10.1111/j.1745-6622.2006.00106.x

North Carolina State University ERM Initiative. (n.d.). *Revamping ERM: How seven companies improved ERM effectiveness*. Retrieved from https://erm.ncsu.edu/wp-content/uploads/sites/41/migrated-files/Revamping_ERM_-_How_Seven_Companies_Improved_ERM_Effectiveness.pdf

Paape, L., & Spekle, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review, 21*(3), 533-564. https://doi.org/10.1080/09638180.2012.661742

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6-7), 849-855. https://doi.org/10.1016/j.aos.2009.06.001

PwC. (2025). *What's important to the chief risk officer in 2025*. Retrieved from https://www.pwc.com/us/en/executive-leadership-hub/chief-risk-officer.html

Risk Leadership Network. (2022). *What are the most common risk reporting lines and operating models?*. Retrieved from

https://www.riskleadershipnetwork.com/insights/what-are-the-most-common-risk-reporting-lines-and-operating-models

Rittenberg, L. E., & Martens, F. (2012). *Enterprise risk management: Understanding and communicating risk*. The Committee of Sponsoring Organizations of the Treadway Commission.

Senior Supervisors Group. (2008). *Observations on risk management practices during the recent market turbulence*. Retrieved from https://www.sec.gov/news/press/2008/report030608.pdf

Vlerick Business School. (2022). *Effective board-level risk oversight*. Retrieved from https://www.vlerick.com/en/insights/effective-board-level-risk-oversight/

Walker, D. (2009). *A review of corporate governance in UK banks and other financial industry entities*. HM Treasury.