From Compliance Theater to Authentic Governance: A Framework for Risk Culture Integrating Structural Independence and Behavioral Science

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: January 6, 2026 Accepted: February 9, 2026 Online Published: March 11, 2026

doi:10.5430/ijfr.v17n2p1 URL: https://doi.org/10.5430/ijfr.v17n2p1

Abstract

Risk culture has become a decisive factor in organizational resilience, ethical conduct, and strategic foresight. However, leading frameworks like COSO ERM and ISO 31000, while emphasizing culture, neglect the critical influence of structural and behavioral realities that dictate risk transparency. This paper argues that genuine improvement in risk culture is unattainable without foundational governance reform, specifically, ensuring the structural independence of the organization's Chief Risk Officer. We integrate organizational structure theories, psychological safety research, and behavioral science to interrogate how reporting lines, incentive systems, and board dynamics fundamentally shape risk behavior. The paper proposes a new conceptual model, derived from a comparative analysis, that integrates governance reform, behavioral enablers, and structural alignment. We conclude that a positive risk culture is achievable only through a triad of board-controlled independence, active cultural reinforcement, and systemic behavioral integration. Implications for boards, regulators, and practitioners are discussed, mandating a paradigm shift from 'compliance theater' to authentic governance.

Keywords: risk culture, corporate governance, compliance theater, structural independence, psychological safety, Chief Risk Officer (CRO), conceptual framework

1. Introduction

Risk culture has become one of the most contested and yet underdeveloped dimensions of corporate governance. At its core, risk culture refers to the shared values, beliefs, and behavioral norms that shape how individuals and organizations perceive, evaluate, and respond to risk (Bogale & Debela, 2024). It is not merely a technical construct but a deeply human one, embedded in organizational structures, incentive systems, and leadership dynamics. In recent decades, catastrophic failures across industries from the governance breakdowns at Enron and WorldCom to the systemic collapse of the 2008 global financial crisis have demonstrated that risk culture is often the decisive factor separating resilient organizations from those that collapse under pressure (Rashid, 2020).

In response to these failures, regulators and oversight bodies heavily promoted formal risk management frameworks. Standards such as COSO's Enterprise Risk Management (ERM) and ISO 31000 were updated to emphasize the importance of governance and culture (COSO, 2017; ISO, 2018; Jerab, 2023; Gleißner & Berger, 2024). Yet, this emphasis has proven insufficient. High-profile failures persist, illustrating a clear disconnect between frameworks on paper and the structural realities of organizations. The Boeing 737 MAX crisis revealed how cost-saving pressures and a culture of silence could override engineering safety (Jong & Broekman, 2021). The Wells Fargo account fraud scandal demonstrated how misaligned incentive systems could actively encourage mass misconduct, all while formal risk and audit functions failed to escalate the risk (Witman, 2018). Similarly, the collapses of Wirecard in Germany and the 1MDB scandal in Malaysia highlighted how risk and audit functions could be systematically sidelined or manipulated, rendering governance structures useless (Low & Heyd, 2024; Jones, 2020).

These cases reveal a recurring pattern: formal frameworks are necessary, but they are ineffective when undermined by structural and behavioral realities. The central problem which this paper addresses is that governance assurance leaders such as CROs often face structural conflicts of interest, such as reporting administratively to the very executives they are meant to oversee. This erodes psychological safety, discourages candor, and ensures that boards receive filtered, "safe" information, leaving them blind to emerging threats.

Despite the clear importance of this problem, academic and practitioner debates remain fragmented. COSO and ISO provide high-level principles but lack granular mechanisms to address these structural power dynamics (IRM, 2017). Behavioral science, meanwhile, highlights the importance of psychological safety but often fails to connect it to the hard wiring of structural independence (Edmonson, 2018). Organizational structure theories explain how hierarchy and incentives shape behavior but are rarely integrated into governance reform discussions (Aguilera & Jackson, 2003).

This paper seeks to bridge this critical gap. We provide a holistic model that integrates these fragmented fields, addressing why current governance frameworks fail to embed positive risk culture and how organizational structure theories explain this persistent failure. We explore the role of psychological safety as an enabler for transparency and, most importantly, identify the specific governance reforms necessary to protect governance assurance officers' independence.

The contribution of this paper is threefold. First, we provide a theoretical integration by synthesizing organizational structure theories, behavioral science, and governance frameworks to create a more robust explanation of risk culture. Second, we propose a practical reform agenda centered on board-controlled independence and charter-protected autonomy for the CRO. Finally, we introduce the Risk Culture Reform Model (RCRM), a novel conceptual framework that aligns structural reform, behavioral enablers, and governance oversight.

2. Literature Review: The Strategic Mandate of Modern ERM

Risk culture sits at the intersection of governance frameworks, organizational structure, and behavioral science. To understand why reforms are necessary, it is important to examine the existing literature. This review first examines the dominant governance frameworks, highlighting their inherent limitations. It then explores the behavioral and structural dimensions for psychological safety and independence that these frameworks fail to address. Finally, it integrates organizational structure theories to explain why these failures are systemic and predictable.

2.1 Governance Frameworks: A Record of Insufficiency

COSO ERM

The COSO ERM framework (2017) emphasizes five components: governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting. The inclusion of "Governance and Culture" as the first component reflects recognition that risk management is not purely technical but cultural. COSO highlights tone at the top, ethical values, and organizational competence as critical elements (COSO, 2017).

However, critics argue that COSO remains principle-based. It provides guidance but lacks mechanisms to enforce independence of risk functions. Organizations may adopt COSO for legitimacy but fail to embed its principles in practice (Power, 1997). For example, Wells Fargo claimed adherence to COSO principles, yet its incentive systems encouraged misconduct, and its risk culture failed to prevent widespread fraud.

ISO 31000

ISO 31000 (2018) provides international standards for risk management, emphasizing integration, transparency, and continual improvement (Jerab, 2023). It highlights the importance of human and cultural factors, recognizing that risk management must be embedded across organizational processes. Yet, ISO 31000 also suffers from vagueness. It outlines what organizations should do but not how to overcome structural conflicts. As Gleißner and Berger (2024) noted, ISO 31000 risks becoming symbolic compliance rather than substantive reform. Organizations may adopt ISO certification for reputational purposes without addressing incentive misalignment or psychological safety.

Basel Committee Principles

The Basel Committee on Banking Supervision provides stronger guidance, particularly for financial institutions. It requires CRO independence and direct access to the board risk committee (Basel, 2024). Basel emphasizes that CROs must be free from executive influence and protected from retaliation. This reflects lessons from the 2008 financial crisis, where CROs were often sidelined or ignored. Basel's principles are more prescriptive than COSO or ISO, but their application is largely limited to banking. Non-financial sectors often lack equivalent safeguards, leaving CROs vulnerable to CEO influence.

Institute of Internal Auditors (IIA) Standards

The entire suite of governance assurance functions requires this structural reform. We can see an example of this need by examining the internal audit function, which is a critical area. The IIA emphasizes that internal audit must report

functionally to the board or audit committee, even if administratively to the CEO. This dual reporting line is intended to balance independence with operational convenience (IIA, 2024). However, in practice, CEOs often control compensation and career progression, undermining independence (Johari et al., 2018). The 1MDB scandal in Malaysia illustrates this weakness. Internal audit functions were formally independent but practically subordinated, unable to challenge executive power. This highlights the need for structural reform beyond dual reporting lines.

2.2 The Behavioral Prerequisite: Psychological Safety

Psychological safety, defined by Edmondson (2018), is critical for risk culture. It enables employees to speak up, report errors, and escalate concerns without fear of punishment. Research shows that psychological safety fosters learning, adaptability, and transparency (Shih & Koch, 2020). In risk culture, psychological safety ensures that CROs can challenge executives. Without it, silence prevails.

The Boeing 737 MAX crisis illustrates this: engineers raised safety concerns but feared retaliation, leading to suppressed warnings. Similarly, Wells Fargo employees feared losing their jobs if they did not meet unrealistic sales targets, discouraging candor. Psychological safety is not merely a cultural attribute; it requires structural protection. If CEOs control compensation, psychological safety is compromised. Boards must create environments where candor is rewarded, not punished.

2.3 The Structural Prerequisite: Independence of CROs

Independence is the cornerstone of effective risk culture. CROs must be free to challenge executives and escalate concerns. Yet, in practice, they often report administratively to CEOs, creating conflicts of interest (Fraser et al., 2021). CEO control over bonuses and increments undermines independence. CROs may hesitate to escalate risks that conflict with CEO priorities. This dynamic erodes psychological safety and creates blind spots. Scholars argue that true independence requires board-controlled compensation, charter-protected autonomy, and direct board access (Jameel et al., 2024; Abdul Samad, 2025). Without these safeguards, risk culture remains vulnerable to executive influence.

2.4 The Structural Underpinnings of Risk Culture Failure

Organizational structure theories provide powerful lenses for understanding why the frameworks in 2.1 fail and why the independence in 2.3 is so rare. The design of a firm's hierarchy, authority, and reporting lines directly shapes behavior, often in ways that undermine the "principles" of COSO and ISO.

Weber's Bureaucratic Theory

Max Weber's bureaucratic model emphasizes hierarchy, rules, and formal authority (Kumar, 2016). Bureaucracy ensures predictability and accountability, but it also suppresses candor. Employees may fear consequences for speaking up, leading to compliance theater. In the Wirecard scandal, for example, bureaucratic structures existed on paper, but risk and audit functions were subordinated to executive authority. Reports were produced, but candor was suppressed. This illustrates how bureaucracy can create the illusion of control while masking cultural weaknesses. Bureaucratic structures therefore require charter-protected independence to prevent this suppression of candor.

Fayol's Administrative Theory

Henri Fayol emphasized principles of management such as division of work, unity of command, and scalar chain (Edwards, 2018). While these principles ensure accountability, they reinforce top-down control. At Wells Fargo, "unity of command" reinforced CEO control over risk functions. Even the internal auditors reported administratively to executives, creating conflicts of interest, and incentives tied to CEO's approval which discouraged candor. Administrative structures thus require board-controlled compensation and direct committee access to be effective.

Human Relations (Mayo)

Elton Mayo's Hawthorne Studies highlighted social needs and group dynamics. This theory emphasizes motivation, trust, and psychological safety (Bruce & Nyland, 2011). Boeing's engineers raised safety concerns about the 737 MAX but lacked psychological safety. Group dynamics discouraged dissent, and executives prioritized cost pressures. This illustrates how, even with technical expertise, a failure in human relations (a lack of psychological safety) leads to failure.

McGregor's Theory X and Theory Y

Douglas McGregor conceptualized the contrast between Theory X, a control−oriented view of management, and Theory Y, an empowerment−oriented approach (Kopelman et al., 2008). Theory Y cultures support openness and candor, while Theory X cultures create fear and silence. Enron exemplified a Theory X culture, where the executives

controlled information and suppressed dissent. Risk culture thrives in empowerment-oriented (Theory Y) environments, which must be encouraged by boards.

Contingency Theory

Burns and Stalker (1961) argued that structure depends on environment. Mechanistic structures suit stable environments, while organic structures suit dynamic contexts. In volatile industries (e.g., oil and gas, technology), organic structures foster adaptability and openness. Mechanistic structures, by contrast, can suppress early warnings, leading to failures. Governance must adapt to its environment.

Systems Theory

Katz and Kahn (1978) viewed organizations as open systems where risk culture must be embedded across all subsystems. Failures in one subsystem (e.g., incentives) can undermine the whole. Wells Fargo's incentive subsystem undermined its entire risk culture. Even though other subsystems (audit, compliance) existed, distorted incentives corrupted behavior. This illustrates the need for holistic, integrated governance reform.

Institutional Theory

DiMaggio and Powell (1983) argued that organizations conform to institutional norms for legitimacy. This theory is critical, as it provides the theoretical basis for "compliance theater." Organizations may adopt COSO and ISO certification symbolically for reputational purposes but fail to embed the principles substantively. Boards must be pushed to move beyond symbolic compliance to substantive independence.

Modern Structures: Matrix and Agile

Ethical business practices have become foundational elements in shaping the identity and legitimacy of modern organizations. Increasingly, these values are not peripheral but embedded within governance structures, strategic decision-making, and stakeholder expectations (Jerab & Mabrouk, 2023). Matrix structures involve dual reporting lines, balancing accountability but creating confusion. CROs may still face CEO influence unless compensation is board-controlled. Agile structures emphasize decentralization and adaptability, supporting psychological safety but requiring board oversight. While these structures encourage openness, they risk fragmentation. Without board oversight to ensure consistency, risk culture may fail.

Table 1. Comparative Analysis of Structure Theories

Theory	Core Features	Strengths	Weaknesses	Implications for Risk Culture	Governance Reform Needs
Weber's Bureaucratic Theory	Hierarchy, rules, formal authority	Predictability, accountability	Rigid, suppresses candor	Ensures compliance but risks "compliance theater"	Charter-protected independence
Fayol's Administrative Theory	Division of work, unity of command	Clear accountability	Overemphasis on control	CROs subordinated to CEOs	Board-controlled compensation
Human Relations (Mayo)	Social needs, motivation	Recognizes human factors	Overlooks independence	Psychological safety emphasized	Boards must embed safety structurally
McGregor's Theory X/Y	X: control; Y: empowerment	Y supports openness	X creates fear	Theory Y fosters candor	Boards must encourage Y-style leadership
Contingency Theory	Structure depends on environment	Adaptive, flexible	No universal model	Organic fosters openness	Governance must adapt
Systems Theory	Organizations as open systems	Holistic, feedback loops	Complexity obscures accountability	Risk culture embedded across subsystems	Integration across governance

Institutional Theory	Conformance to norms	Legitimacy	Symbolic compliance	COSO/ISO adopted for legitimacy	Move beyond symbolic compliance
Matrix Structures	Dual reporting lines	Balances accountability	Confusion, conflict	CROs vulnerable to CEO influence	Board must clarify independence
Agile Structures	Decentralized, adaptive	Transparency, rapid response	Risk of fragmentation	Supports psychological safety	Board oversight required

2.5 Integrating Behavioral Science Enablers

While structural reform (2.3) and a supportive organizational design (2.4) are essential, behavioral science identifies the cultural enablers that must be cultivated simultaneously. Beyond the foundational need for psychological safety (Edmondson, 2018), a resilient risk culture is fostered by a growth mindset that encourages learning from mistakes rather than hiding them (Dweck, 2006). This is reinforced by leader role modeling (Bandura & Walters, 1977) and organizational systems that build trust and fairness. Finally, behavioral economics shows how incentives and nudges (Thaler & Sunstein, 2008) can be designed to shape behavior, moving beyond the purely rational models assumed by compliance frameworks, while building resilience supports the capacity to cope with uncertainty. These factors explain why structural reforms must be complemented by active cultural reinforcement.

2.6 Summary of Literature Review and the Identified Gap

The literature reveals a consistent theme: frameworks exist, but structural and behavioral realities undermine their effectiveness. COSO and ISO provide principles but lack mechanisms. Basel provides stronger safeguards but is limited to banking. Organizational structure theories (Weber, Fayol, etc.) explain *how* hierarchy and incentives shape behavior, while institutional theory (DiMaggio & Powell, 1983) explains *why* organizations settle for "compliance theater." Behavioral science highlights enablers like psychological safety and trust, but these cannot survive without structural protection.

Together, these insights reveal a critical gap: a lack of a holistic model that integrates structural reform (independence), behavioral enablers (psychological safety), and governance oversight (board control). This paper aims to build that model.

3. Conceptual Framework: The Risk Culture Reform Model (RCRM)

The literature review reveals a critical tension: existing governance frameworks are insufficient because they fail to address the structural and behavioral realities of organizations. Bureaucratic and administrative theories emphasize control but suppress candor; human relations theories emphasize openness but lack the structural safeguards to protect it. Institutional theory confirms that, in the absence of a mandate, firms will default to "compliance theater" (DiMaggio & Powell, 1983).

To resolve this, this paper introduces the **Risk Culture Reform Model (RCRM)**. This is not merely a list of components, but a dynamic, integrated system that argues for a specific causal pathway. The RCRM posits that a positive risk culture is not an abstract goal but an **outcome** that is only achievable when **Governance Reform** is implemented as the foundational intervention. This reform is the prerequisite that enables **Structural Alignment** and **Behavioral Enablers** to function. The model is visualized in Figure 1 and operates on three core propositions.

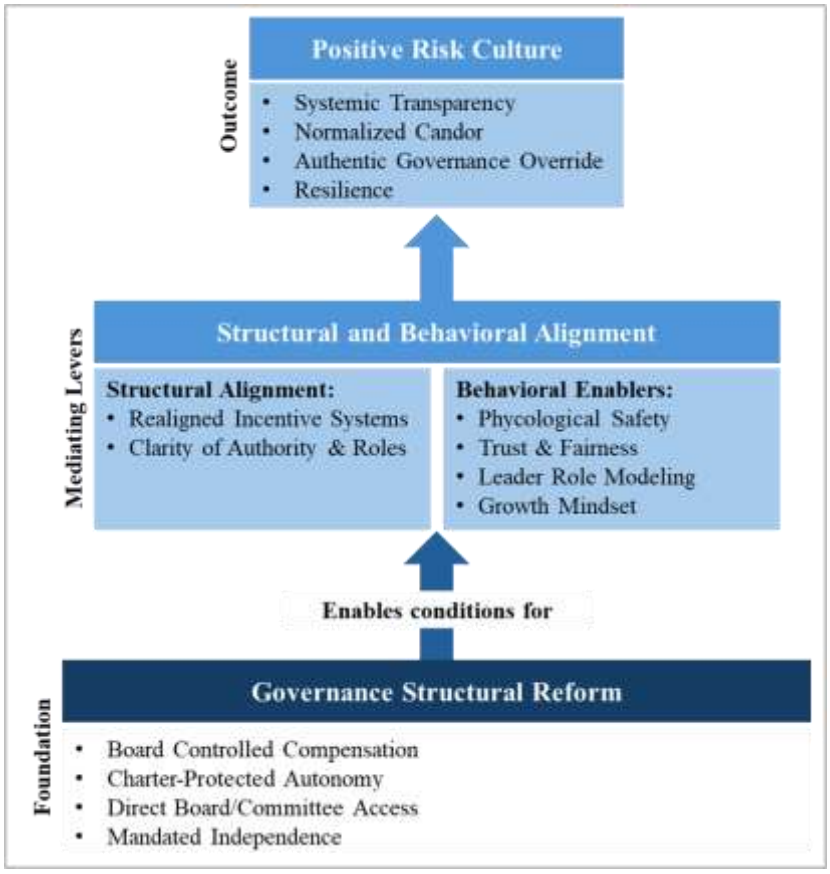

Figure 1. The Risk Culture Reform Model

3.1 Proposition 1: Governance Reform as the Foundational Prerequisite

This is the central intervention of the RCRM. The model argues that no meaningful change in risk culture is possible as long as risk function is structurally subordinated to the CEO. This "compliance theater" is only broken by formal governance-level changes.

This pillar is not a principle; it is a set of non-negotiable structural actions:

- **Board-Controlled Independence:** The board (or its relevant committee) must have sole authority over the hiring, firing, and critically, the compensation and budget of the Chief Risk Officer.
- **Charter-Protected Autonomy:** The "right to speak" must be formally codified in the charters of the risk function, guaranteeing unfettered access to the board without executive presence.
- **Direct Reporting Lines:** Establishing a "hard" functional reporting line to the board committee that supersedes the "soft" administrative line to management.

Without this foundation, any efforts to build psychological safety or align structure will fail, as they can be overridden by executive influence.

3.2 Proposition 2: Structural and Behavioral Alignment as Mediating Levers

Once the governance foundation is set, it creates the "space" for structural and behavioral levers to function. These two pillars are interdependent and mediate the relationship between governance reform and the final cultural outcome.

- **Structural Alignment:** This pillar draws from organizational theories (Contingency, Systems) to ensure the *entire* organization is aligned with the governance reforms. This includes:
- **Incentive Systems:** Re-aligning performance metrics and compensation *across the entire business* to reward risk-aware behavior and candor, not just short-term profit. This directly addresses the failures seen at Wells Fargo.

- **Clarity of Authority:** Using administrative and bureaucratic principles (Weber, Fayol) to define clear roles and responsibilities for risk, preventing the confusion of matrix or agile structures from creating blind spots.
- **Behavioral Enablers:** With structural protection in place, behavioral factors can be actively cultivated. This is the "Theory Y" component of the model.
- **Psychological Safety** (Edmondson, 2018): This is the primary enabler. Because the CRO and auditors are protected by the board, they can challenge executives without fear, which *role-models* (Bandura & Walters, 1977) candor for the rest of the organization.
- **Trust and Fairness:** This culture of candor builds trust that the system is fair and that "speaking up" is a rewarded, not-punished, behavior.

3.3 The Outcome: Positive and Authentic Risk Culture

The RCRM posits that risk culture is a dependent variable. It is the *result* of the interactions between the first two pillars. A positive risk culture is defined as a self-reinforcing system (Katz & Kahn, 1978) where:

1. **Transparency is Systemic:** Information flows freely because structures mandate it.
2. **Candor is Normal:** Individuals speak up because they feel safe and incentivized to do so.
3. **Governance is Authentic:** The board receives unfiltered information, allowing it to provide genuine oversight rather than participate in compliance theater.

In summary, the Risk Culture Reform Model provides a clear, causal pathway. It moves beyond a simple "list" of factors and argues that authentic governance *enables* aligned structures and behaviors, which in turn *produces* a positive risk culture (Outcome).

4. Discussion: From Compliance Theater to Authentic Governance

The preceding analysis identified a critical gap in governance: existing frameworks are "principle-based" and enable symbolic compliance, while the structural and behavioral realities of power, incentive, and hierarchy are ignored. The Risk Culture Reform Model (RCRM) proposed in Section 3 was designed to solve this problem. This discussion explores the theoretical and practical implications of this model.

4.1 Theoretical Implications: Reframing Culture as a Structural Outcome

The primary contribution of the RCRM is that it reframes risk culture as a dependent variable, an *outcome* of governance structure, not an independent "value" to be managed.

- **Challenging Principle-Based Frameworks:** The RCRM is a direct challenge to the vague, "principle-based" approach of COSO and ISO 31000. Where COSO places "Governance and Culture" as a co-equal component, the RCRM argues for a causal pathway: Authentic Governance is the *prerequisite* for a positive culture, not its equivalent**.** The failures at Wells Fargo and Boeing are not evidence that COSO's principles were "wrong," but that they were structurally impossible to implement without the RCRM's foundational reforms.
- **Solving the "Compliance Theater" Paradox:** Institutional Theory (DiMaggio & Powell, 1983) explains *why* organizations adopt frameworks symbolically. The RCRM offers the *solution*. It argues that "compliance theater" is the rational response to a system where risk functions lack real power. By mandating board-controlled independence, the model breaks this dynamic, making authentic governance possible.
- **Integrating Power and Psychology:** The model connects the "hard" structural theories (Weber, Fayol) with "soft" behavioral ones (Edmondson, 2018). It posits that psychological safety cannot be "built" by HR initiatives, as many firms attempt. It can only be *unlocked* when its structural prerequisite is independent from executive retaliation, guaranteed by the board, is in place.

4.2 Contextual Considerations: Hierarchy, Culture, and the RCRM

The RCRM is proposed as a universal model, but its application will be mediated by national and organizational culture, a point underscored by the Malaysian 1MDB scandal.

The model may, in fact, be *more* critical in high power-distance or collectivist cultures, not less. In Western governance models (as seen at Wells Fargo or Wirecard), failure often stems from misaligned *incentives*. In Asian governance models, as the 1MDB case suggests, failure can stem from hierarchy, harmony, and political influence undermining formal structures.

In such a context, the "soft" behavioral enablers like psychological safety are much harder to achieve. Therefore, the "hard" structural protections (board-controlled independence) become the *only* mechanism strong enough to protect a risk leader and guarantee their candor. The RCRM's emphasis on structure over "values" makes it a more robust model for cross-cultural application.

4.3 Limitations of the Model

As a conceptual paper, this model has necessary limitations. The RCRM is, by nature, theoretical. It proposes a causal pathway but does not provide empirical evidence of its efficacy. It also assumes a board of directors that is *willing* to exercise its authority; it does not solve the problem of a captured or negligent board. These limitations provide clear avenues for the future research agenda outlined in the following section.

5. Implications

The findings of this paper and the RCRM carry profound implications for multiple stakeholders. Risk culture reform is not simply an internal organizational matter; it has systemic consequences for boards of directors, regulators, practitioners, and scholars.

5.1 Implications for Boards of Directors

Boards are the ultimate guardians of governance. Yet, in many organizations, they remain dependent on filtered information provided by executives. This creates blind spots that undermine oversight.

Key Implications:

- **Board-Controlled Compensation:** Boards must assume responsibility for setting the compensation of CROs. CEO-controlled incentives compromise independence. By controlling pay, boards signal that candor is valued over compliance.
- **Charter-Protected Independence:** Governance charters must explicitly safeguard risk functions from retaliation. Without formal protection, independence remains vulnerable.
- **Direct Access:** Boards must ensure their CRO has private sessions with risk committee. This creates safe channels for candor.
- **Cultural Reinforcement:** Boards must commend candor publicly, signaling that transparency is valued. Role modeling by directors sets norms for the entire organization.

Case Example: In the Wells Fargo scandal, the board relied on filtered information from executives. Had the board controlled CRO compensation and mandated private access, employees may have felt safer escalating concerns.

5.2 Implications for Regulators and Standard-Setters

Regulators shape governance codes and standards. Yet, many codes remain principle-based, allowing organizations to adopt frameworks symbolically.

Key Implications:

- **Mandating Independence:** Regulators must require board-controlled compensation and direct access for risk functions. Principle-based codes are insufficient.
- **Auditing Psychological Safety:** Regulators should audit psychological safety as part of risk culture assessments. This ensures that candor is embedded.
- **Incentivizing Transparency:** Regulators can incentivize transparency through scoring systems and public reporting. Organizations with strong risk culture should be recognized.
- **Expanding Basel Principles:** Basel-style independence should be extended beyond banking to other sectors.

Case Example: In Malaysia, the 1MDB scandal revealed weaknesses in governance codes. Regulators must strengthen codes to prevent political influence from undermining independence.

5.3 Implications for Executives and Practitioners

Executives and practitioners shape daily risk culture. Their behaviors, incentives, and decisions determine whether transparency thrives or fails.

Key Implications:

- **Fostering Psychological Safety:** Executives must create environments where employees feel safe to escalate concerns. This requires humility and openness.

- **Modeling Transparency:** Executives must model candor in decision-making. If leaders conceal risks, employees will emulate silence.
- **Aligning Incentives:** Incentives must reward integrity, not short-term performance. Wells Fargo illustrates the danger of misaligned incentives.
- **Integrating Behavioral Science:** Risk training must integrate behavioral science, emphasizing psychological safety, trust, and resilience.

Case Example: Boeing executives prioritized cost pressures over safety. Had they modeled transparency and rewarded candor, engineers may have felt safer escalating concerns.

5.4 Implications for Scholars (Future Research Agenda)

Scholars play a critical role in advancing theory and practice. This paper's conceptual model opens several avenues for future empirical research.

Key Implications:

- **Integrating Theories:** Scholars must integrate organizational structure theories, behavioral science, and governance frameworks. Fragmented approaches are insufficient.
- **Empirical Studies:** Scholars should conduct empirical studies on the impact of board-controlled compensation on CRO candor.
- **Cross-Sector Comparisons:** Scholars should compare risk culture maturity across sectors and geographies.
- **Behavioral Audits:** Scholars should develop tools for auditing psychological safety in risk reporting environments.
- **Longitudinal Studies:** Scholars should study the long-term impact of governance reform on risk outcomes.

Case Example: Research on Wells Fargo, Boeing, Wirecard, and 1MDB can provide comparative insights into risk culture failures across contexts.

6. Conclusion

Risk culture is not a peripheral concern; it is the invisible architecture that determines whether governance frameworks succeed or fail. The evidence reviewed in this paper demonstrates that failures persist because principle-based frameworks are undermined by CEO-dominated power dynamics, a neglect of behavioral science, and cultural contexts that can erode transparency.

The **Risk Culture Reform Model (RCRM)** introduced in this paper provides a new framework to solve this. By integrating structural reform (board-controlled independence), behavioral enablers (psychological safety), and governance oversight, the model ensures that risk leaders are structurally insulated from executive influence, psychologically safe to escalate concerns, and culturally reinforced to speak truth to power.

This model is particularly relevant in contexts like Malaysia. The 1MDB scandal revealed how governance structures can be manipulated, with risk and audit functions unable to challenge executive power. This tension reflects the broader challenge of embedding risk culture in contexts where hierarchy is strong. By adopting the RCRM, such jurisdictions can bridge global standards with local realities, moving beyond symbolic compliance.

Ultimately, risk culture reform is not merely a technical adjustment; it is a moral and strategic imperative. Organizations that fail to protect the independence and psychological safety of their risk leaders are not just vulnerable, they are complicit in creating blind spots that lead to ethical breaches, financial losses, and reputational damage.

This paper calls for a paradigm shift:

- From **compliance theater** to **authentic governance**.
- From **symbolic frameworks** to **structural integrity**.
- From **fear-driven silence** to **psychologically safe candor**.

Only then can risk culture become a source of strength rather than a hidden liability. The time for symbolic compliance has passed; the time for authentic governance has arrived.

Acknowledgments

This work is lovingly dedicated to the late Abdul Samad Mohd Haroun and Nurliza Abdullah, whose wisdom, kindness, and enduring spirit continue to guide and inspire us. It is also dedicated to Rina Ammy T. Jani, Shaheem Reza Shaharin, and Sharmeen Rose Shaharin, whose unwavering love, encouragement, and presence have been a constant source of strength throughout this journey.

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 authors declare 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

Abdul Samad, S. (2025). Strengthening ERM independence: A conceptual governance and oversight framework. *International Journal of Financial Research, 16*(3), 63-78. https://doi.org/10.5430/ijfr.v16n3p63

Aguilera, R. V., & Jackson, G. (2003). The cross-national diversity of corporate governance: Dimensions and determinants. *Academy of management Review, 28*(3), 447-465. https://doi.org/10.2307/30040732

Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1, pp. 141-154). Englewood Cliffs, NJ: Prentice Hall.

Basel Committee on Banking Supervision Core Principles for effective banking supervision. (2024). https://doi.org/10.5089/9798400286636.007

Bogale, A. T., & Debela, K. L. (2024). Organizational culture: a systematic review. *Cogent Business & Management, 11*(1), 1-23. https://doi.org/10.1080/23311975.2024.2340129

Bruce, K., & Nyland, C. (2011). Elton Mayo and the deification of human relations. *Organization studies, 32*(3), 383-405. https://doi.org/10.1177/0170840610397478

Burns, T., & Stalker. G. M. (1961). *The Management of Innovation.* Tavistock: London.

COSO. (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission.

DiMaggio, P. J., & Powell, W. W. (1983). 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

Dweck, C. (2006). *Mindset: The new psychology of success.* Random House.

Edmondson, A. C. (2018). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. John Wiley & Sons.

Edwards, R. (2018). An elaboration of the administrative theory of the 14 principles of management by Henri Fayol. *International Journal for Empirical Education and Research, 1*(1), 41-51. https://doi.org/10.35935/edr/21.5241

Fraser, J. R., Quail, R., & Simkins, B. (Eds.). (2021). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives.* John Wiley & Sons.

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

Institute of Internal Auditors. (2024). *Global Internal Audit Standards*.

Institute of Risk Management. (2017). *From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks*.

ISO. (2018). *ISO 31000: 2018, Risk management - guidelines*. Vernier, Geneva International Organization for Standardization.

Jameel, S. Z. M., Hamoody, K. M. T., & Al-Shmam, M. A. (2024). The impact of independence, organizational commitment strategy, good governance, and role ambiguity on the performance of internal auditors. *Corporate & Business Strategy Review, 5*(4), 152-162. https://doi.org/10.22495/cbsrv5i4art14

Jerab, D. (2023). *Effectiveness of ISO 31000 in risk management.* Academia.edu.

Jerab, D., & Mabrouk, T. (2023). *The evolving landscape of organizational structures: A contemporary analysis.* Available at SSRN 4584643. https://doi.org/10.2139/ssrn.4584643

Johari, R. J., Hati, M. T., Hadi, M., & Rashid, N. (2018). A Revisited Note on Internal Audit Function and Good Corporate Governance. *International Journal of Academic Research in Business and Social Sciences, 8*(12), 716-728. https://doi.org/10.6007/IJARBSS/v8-i12/5067

Jones, D. S. (2020). 1MDB corruption scandal in Malaysia: a study of failings in control and accountability. *Public Administration and Policy, 23*(1), 59-72. https://doi.org/10.1108/PAP-11-2019-0032

Jong, W., & Broekman, P. (2021). Crisis history and hindsight: a stakeholder perspective on the case of Boeing 737-Max. *Public Relations Inquiry, 10*(2), 185-196. https://doi.org/10.1177/2046147X211001350

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations* (Vol. 2, p. 528). New York: Wiley.

Kopelman, R. E., Prottas, D. J., & Davis, A. L. (2008). Douglas McGregor's theory X and Y: Toward a construct-valid measure. *Journal of Managerial Issues,* 255-271. https://doi.org/10.1037/e518532013-388

Kumar, R. (2016). Bureaucratic Theory by Max Weber–A Review Study. *Journal of Advances and Scholarly Researches in Allied Education, 12*(23), 212-216.

Low, E., & Heyd, R. (2024). *The Audit Failures of the Wirecard Scandal*. Springer Books. https://doi.org/10.1007/978-3-031-59854-8

Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.

Rashid, M. M. (2020). Case analysis: Enron; Ethics, social responsibility, and ethical accounting as inferior goods?. https://doi.org/10.2139/ssrn.3550618

Shih, Y. W., & Koch, A. (2020). Psychological Safety for Organizational Cultural Change: An exploratory study in a Swedish multinational chemical engineering company.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Witman, P. D. (2018). "What gets measured, gets managed" The Wells Fargo account opening scandal. *Journal of Information Systems Education, 29*(3), 131-138.