Scientific Research Publishing

Open Journal of Business and Management, 2026, 14(3), 1338-1356
https://www.scirp.org/journal/ojbm
ISSN Online: 2329-3292
ISSN Print: 2329-3284

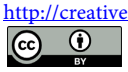
From ERM to HERM: A Holistic Enterprise Risk Management Framework for Banks in a Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) World

Christopher Goh

Centre of Graduate Studies and Lifelong Learning, University of Information Technology and Management, Rzeszow, Poland
Email: drchrisgoh88@gmail.com

How to cite this paper: Goh, C. (2026). From ERM to HERM: A Holistic Enterprise Risk Management Framework for Banks in a Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) World. *Open Journal of Business and Management, 14,* 1338-1356.
https://doi.org/10.4236/ojbm.2026.143076

Received: February 25, 2026
Accepted: April 10, 2026
Published: April 13, 2026



Abstract

The increasing Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) of the global financial environment has exposed fundamental weaknesses in traditional Enterprise Risk Management (ERM) frameworks. Major banking scandals—including Wells Fargo, Commonwealth Bank of Australia, and Barclays—illustrate that conventional ERM systems remain fragmented, compliance-driven, and insufficiently integrated with strategy, governance, and execution. This paper proposes a Holistic Enterprise Risk Management (HERM) framework as a next-generation risk governance model for banks operating in a VUCA world. Drawing on design thinking, systems thinking, and action research principles, the study reconceptualizes ERM as an integrated strategic capability rather than a technical compliance function. The paper synthesizes insights from COSO (2017), ISO 31000 (ISO, 2018), and Basel III (BCBS, 2010) to develop a unified conceptual model that aligns corporate strategy with risk appetite, risk capacity, and operational execution. The proposed HERM framework is structured around three core mechanisms: 1) an Input-Process-Output-Control risk system, 2) a 6As change management model (Awareness, Alignment, Action, Adoption, Assurance, Anticipation), and 3) a HERM Balanced Scorecard linking Key Risk Areas (KRAs), Key Risk Indicators (KRIs), and Key Performance Indicators (KPIs). Using three African banks—Afreximbank, Cooperative Bank of Oromia, and Barclays Bank of Zimbabwe—as illustrative case contexts, the paper demonstrates how HERM can bridge the persistent strategy-execution gap in banking risk management. The framework advances theoretical understanding of ERM by integrating strategy, governance, people, processes, and technology into a single holistic architecture.

Keywords

Holistic Enterprise Risk Management (HERM), VUCA, Banking Risk, Design Thinking, Risk Governance, COSO, ISO 31000, Basel III

1. Introduction

The global financial crisis of 2008 significantly transformed scholarly, regulatory, and practitioner perspectives on risk within banking and financial institutions (Oluloni, 2024). Despite substantial progress in risk modelling, regulatory oversight, and governance frameworks, major corporations continue to experience catastrophic failures that cannot be attributed solely to technical deficiencies. These failures instead expose deeper systemic weaknesses in how organizations conceptualize, integrate, and implement Enterprise Risk Management (ERM) (Gleißner & Berger, 2024). The continued occurrence of large-scale risk failures in sophisticated institutions indicates that the prevailing risk management paradigm is insufficient for addressing the complexities of the Volatile, Uncertain, Complex, and Ambiguous (VUCA) global business environment (Goh, 2018).

Numerous high-profile corporate scandals illustrate that risk failures are seldom isolated operational incidents; rather, they often reflect misaligned strategy, weak governance, fragmented controls, and problematic organizational culture (Andersen & Young, 2023). For instance, Wells Fargo Bank became involved in a significant scandal in which millions of retail accounts were opened without customer consent. The bank's corporate strategy prioritized aggressive growth in new account openings, yet the lack of comprehensive risk oversight enabled unethical practices to proliferate at lower levels of the organization (Grunewald et al., 2017). The consequences extended beyond reputational harm to include billions of dollars in compensation, regulatory fines, and a sustained erosion of stakeholder trust (Bloomberg, 2016).

The primary challenge does not stem from managerial naivety or incompetence. Instead, it arises from the design and implementation of risk management systems that fail to align corporate strategy with risk governance, operational execution, and organizational culture. Many organizations continue to perceive risk management as a technical function assigned to specialists, rather than as an enterprise-wide capability integrated into leadership, decision-making, and performance management (Goh, 2018). This challenge is particularly pronounced in the banking sector, where risk is inherently systemic, interconnected, and dynamic. Banks function at the intersection of financial markets, regulatory frameworks, technological innovation, and societal expectations. The rapid expansion of digital banking, fintech, cybersecurity threats, and global financial interconnectedness has further increased the complexity of risk management. In this environment, a compliance-driven approach to ERM is inadequate; instead, a holistic, integrated, and adaptive framework is required to align risk with strategy, governance, culture, and technology

(Moeller, 2011).

The shortcomings of conventional ERM are especially apparent in emerging markets, where banks operate under pronounced VUCA conditions. In response to these gaps, this study advocates for a paradigm shift from traditional Enterprise Risk Management (ERM) to Holistic Enterprise Risk Management (HERM). HERM is defined not simply as a collection of policies or procedures, but as an organizational capability that integrates strategy, governance, personnel, processes, and technology into a unified risk architecture (Gleißner & Berger, 2024). In contrast to conventional ERM, which frequently functions as a separate compliance activity, HERM situates risk management at the core of strategic planning, operational execution, and leadership decision-making (Samad, 2025).

Fundamentally, HERM asserts that risks do not originate at the point of identification but instead emerge during strategy implementation. Consequently, risk management and strategy execution must be closely aligned across corporate, business, and operational levels (Bromiley et al., 2014). A holistic approach requires personnel with appropriate skills, supported by effective processes and robust technological infrastructure, to systematically monitor, control, and mitigate risks (Goh, 2018). The HERM framework builds upon and extends established global standards, such as COSO (2017), ISO 31000 (ISO, 2018), and Basel III (BCBS, 2010). Although these frameworks offer important principles for risk governance, they do not comprehensively address how organizations can translate risk strategy into actionable execution across various levels of the enterprise (Oluloni, 2024). HERM addresses this limitation by incorporating design thinking, systems thinking, critical thinking, and lateral thinking into risk management practice (Brown, 2008).

To develop and validate the HERM framework, this study utilizes action research conducted with three African banks: Barclays Bank of Zimbabwe, Afreximbank in Cairo, and Cooperative Bank of Oromia in Ethiopia (Yang et al., 2017). These institutions were purposefully selected to represent diverse risk environments, governance challenges, and strategic contexts within the African banking sector. Each bank had encountered significant risk-related issues that required a reassessment of its ERM practices. Barclays Bank of Zimbabwe underwent significant restructuring after regulatory penalties were imposed on its parent company in the United Kingdom. Afreximbank revised its five-year strategic plan and risk governance framework following the appointment of a new CEO and board (Kunz & Heitz, 2021). Cooperative Bank of Oromia experienced severe governance failures following allegations of fraud involving its board of directors, prompting intervention by the National Bank of Ethiopia. These real-world cases offer a robust empirical foundation for analyzing the practical application of HERM (Lelissa, 2014).

The central research question guiding this paper is: How can banks design and implement a Holistic Enterprise Risk Management (HERM) framework that effectively aligns strategy, governance, and execution in a VUCA environment? This

question underscores the need to move beyond traditional ERM toward a more integrated, adaptive, and systemic approach (Agarwal & Ansell, 2016). By synthesizing insights from established risk standards, management theory, and action research in three African banks, this study contributes to both theoretical and practical domains. The proposed HERM model integrates corporate vision, risk culture, data governance, cybersecurity infrastructure, and six principal risk pillars—strategic, market, credit, liquidity, compliance, and operational risk—into a unified framework (Mathrani & Mathrani, 2013). Ultimately, this paper contends that effective risk management in contemporary banking necessitates a fundamental shift in perspective: risk should be regarded not merely as a factor to be minimized, but as an essential element of strategy, innovation, and organizational resilience. In an increasingly interconnected and unpredictable environment, banks that adopt a holistic risk management approach will be better equipped to survive, adapt, and prosper (Nuhić-Mešković & Mešković, 2023).

2. Research Design

This study adopts an action-research methodology, which enables iterative learning through real-world problem solving in organizational contexts. Action research is particularly appropriate for governance and risk management research because it combines theoretical reflection with practical intervention (Dürst & Kunz, 2025). The study draws on three banking engagements conducted between 2014 and 2018 involving Barclays Bank of Zimbabwe, Afreximbank (Cairo), and Cooperative Bank of Oromia (Ethiopia). Data sources included:

- Executive strategy workshops with senior leadership and board members.
- Risk governance documentation (risk appetite statements, internal policies, and audit reports).
- Observations from risk-management implementation meetings.
- Informal interviews and discussions with risk officers and operational managers.
- Strategic planning documents and performance dashboards.

Participants included board members, chief risk officers, strategy officers, compliance officers, and senior operational managers responsible for risk governance.

The action-research process followed four iterative stages:

Diagnosis: Identification of gaps in existing ERM practices and governance structures.

Design: Development of the Holistic Enterprise Risk Management (HERM) architecture using systems thinking and design thinking principles.

Implementation: Introduction of HERM mechanisms, including the IPOC framework, KRAs/KRIs/KPIs integration, and the 6As change model.

Evaluation and refinement: Continuous feedback from executives and operational teams to refine the HERM framework. Through these cycles, the study derived the three core components of HERM: the IPOC closed-loop system, the 6As implementation model, and the HERM Balanced Scorecard (Goh, 2018).

3. The Evolution of Risk Management

3.1. The Conceptualization of Risk Management

The conceptualization and practice of risk management have undergone significant transformation over the past seven decades. What began as a narrow focus on insurance and loss prevention has evolved into a complex, multi-layered enterprise-wide governance function that is deeply intertwined with strategy, technology, and organizational culture (Brown et al., 2009). This evolution is not linear but cumulative, with each phase building upon and responding to the limitations of its predecessor. Drawing on the continuum of risk management development presented in **Figure 2** of this study, risk management can be broadly understood as progressing through four major eras: 1) the Pure Risk Era (1950-1970s), 2) the Silo-Based Risk Management Era (1970s-2000s), 3) the Standardized ERM Era (2000s-2010s), and 4) the Holistic Risk Era (2010s-present).

3.2. Pure Risk Era (1950-1970s): Insurance and Loss Prevention

The formal origins of modern risk management are commonly traced to the post-World War II period, particularly the 1950s and 1960s. During this era, risk management was largely synonymous with insurance management and focused primarily on pure risk—situations in which outcomes could only result in loss or no loss, but never gain (D'Arcy, 1999). Organizations sought to protect tangible assets such as buildings, machinery, and inventory through risk prevention measures and insurance contracts (Dionne, 2013; Tziakou et al., 2023).

However, this approach had an inherent limitation: it considered risks in isolation rather than as interconnected organizational phenomena. The absence of a systemic perspective meant that firms were ill-prepared for the more turbulent economic conditions that would emerge in subsequent decades (Goh, 2018).

3.3. Silo-Based Risk Management (1970s-2000s): Financialization and Fragmentation

The collapse of the Bretton Woods agreement in 1972 marked the beginning of a more volatile global financial environment. Oil price shocks, rising inflation, and fluctuating interest rates exposed corporations to new forms of financial risk that could not be managed through traditional insurance alone. This period saw the rise of market risk, credit risk, and operational risk as distinct managerial domains (Przetacznik, 2022).

In response, scholars and practitioners developed increasingly sophisticated quantitative models to measure and manage financial risk. Markowitz's (1952) mean-variance portfolio theory laid the foundation for modern financial risk analysis, while Sharpe and Lintner's Capital Asset Pricing Model (CAPM) provided a formal framework for understanding risk-return trade-offs. The Black-Scholes (Black & Scholes, 1973) options pricing model revolutionized derivatives markets, enabling firms to hedge financial exposures more precisely (Merton, 1989).

3.4. Standardized ERM (2000s-2010s): The Rise of Frameworks

The corporate scandals of the early 2000s, including Enron and WorldCom, exposed severe deficiencies in governance, internal controls, and financial reporting. This regulatory shift catalyzed the formalization of Enterprise Risk Management (ERM) as a structured managerial discipline (Blaskovich & Taylor, 2011).

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) introduced its first integrated ERM framework, positioning risk management as a board-level responsibility rather than a purely operational function. COSO's revised 2017 framework further emphasized the integration of risk with strategy and performance, defining ERM as a process applied in strategy-setting and across the enterprise to manage risk within appetite levels (COSO, 2017).

Parallel to COSO, the International Organization for Standardization released ISO 31000 in 2009, later revised in 2018. ISO defined risk management as "coordinated activities to direct and control an organization with regard to risk", framing risk as the effect of uncertainty on objectives (ISO, 2018). Unlike COSO, ISO adopted a more flexible, principles-based approach applicable across industries (Jedynak & Bąk, 2021).

However, as highlighted in this paper, these frameworks remained largely procedural. They provided checklists, policies, and reporting structures but did not sufficiently address how risk should be embedded into day-to-day decision-making, leadership behavior, or strategic execution (Moeller, 2011). Many firms treated ERM as a compliance exercise rather than a transformational capability (Viscelli et al., 2017).

3.5. Holistic Risk Era (2010s-Present): Integration and Transformation

The current phase of risk management is characterized by recognition that risk is systemic, interconnected, and deeply embedded in organizational systems. Scholars and practitioners increasingly acknowledge that risk cannot be managed effectively through technical controls alone; it must be integrated with strategy, culture, governance, and technology.

Holistic thinking ensures that risks are viewed as part of an interconnected organizational ecosystem rather than isolated events. Systems thinking emphasizes coordination across corporate, business, and operational levels. Critical thinking eliminates redundant or ineffective controls, while lateral thinking fosters continuous innovation in risk processes.

4. Holistic Enterprise Risk Management (HERM)

4.1. Definition

The evolution of risk management outlined in Section 3.1 demonstrates that while Enterprise Risk Management (ERM) has matured significantly, it remains predominantly procedural rather than transformational. Most ERM frameworks em-

phasize identification, assessment, and control of risks but do not sufficiently explain how risk should be embedded within strategy execution, organizational culture, leadership behavior, and digital infrastructure. To address this gap, this study advances the concept of Holistic Enterprise Risk Management (HERM) as a paradigm shift from compliance-driven risk management to an integrated, strategy-centered, and systems-based model of risk governance.

Traditional ERM, as articulated by COSO (2017) and ISO 31000 (ISO, 2018), defines risk management as a process to manage uncertainty in relation to organizational objectives. COSO emphasizes risk appetite, internal controls, and board oversight, while ISO frames risk as the "effect of uncertainty on objectives". While these definitions provide valuable structural guidance, they do not fully capture the dynamic interplay between strategy formulation, execution capability, organizational culture, and technological readiness in highly volatile environments (Jengwa & Pellissier, 2022). **Table 1** in this paper highlights key differences between COSO and ISO definitions of risk management, revealing that both standards conceptualize risk largely in procedural terms rather than as a strategic capability (Nuhić-Mešković & Mešković, 2023)

Table 1. Comparison of risk management definitions by COSO and ISO 31000.

ISO 31000	COSO
ISO 31000: Guide 73, 2009 defined risk management as: "Coordinated activities to direct and control an organization with regard to risk, which is described as the effect of uncertainty on objectives". ISO 31000, February 2018, retained the same definition.	COSO ERM 2014 defined ERM as: "A process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". COSO ERM 2017: redefined ERM as: "The possibility that events will occur and affect the achievement of strategy and business objectives".

In contrast, HERM reconceptualizes risk as an organizational competency rather than a compliance function. The model is rooted in the premise that risks do not originate at the point of identification; they emerge at the point of strategy implementation. Consequently, effective risk management must be embedded in how organizations design, execute, and monitor their strategies across corporate, business, and operational levels. This insight is central to the HERM framework and differentiates it fundamentally from conventional ERM approaches (Mishra et al., 2019).

4.2. Structural Architecture of HERM

In the paper, **Figure 1** presents the Holistic Enterprise Risk Management Model, which serves as the conceptual backbone of HERM. At the foundation of the model

lie Corporate Vision, Mission, and Values, which shape the organization's risk culture and strategic priorities. This reflects the view that risk governance must be value-driven rather than purely rule-driven. Corporate risk culture—defined as "the way we work"—is positioned as a central pillar, recognizing that formal policies are ineffective without consistent behavioral norms that prioritize ethical decision-making and accountability (Gleißner & Berger, 2024).

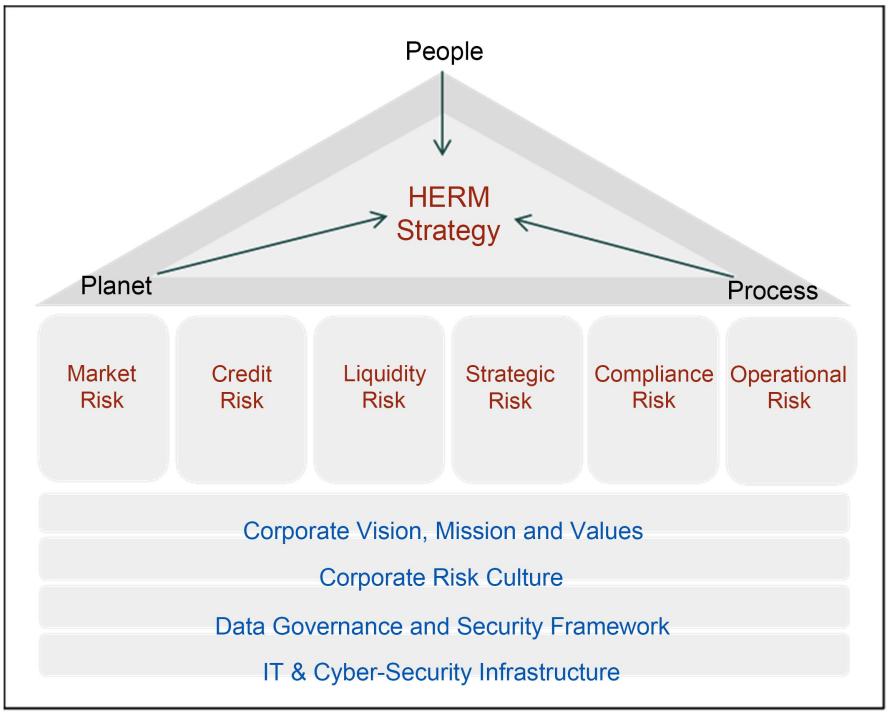


Figure 1. Holistic enterprise risk management model.

The model also emphasizes Data Governance and Cybersecurity Infrastructure as essential enablers of modern risk management. In line with Basel's principles for effective risk data aggregation and reporting (BIS, 2012), HERM assumes that banks must possess robust technological systems capable of real-time risk monitoring, scenario analysis, and predictive analytics. This is particularly relevant in the digital era, where cyber risks, fintech disruption, and algorithmic decision-making introduce new layers of complexity (Monazzam & Crawford, 2024).

At the core of the HERM model are six interconnected risk pillars: strategic, market, credit, liquidity, compliance, and operational risk. These align with Basel's categorization of banking risks but extend beyond regulatory compliance to include strategic risk as a primary driver of organizational success or failure. The inclusion of strategic risk is a distinctive feature of HERM, reflecting the argument that many banking crises originate not from technical failures but from flawed strategic choices or misaligned incentives (Sax & Andersen, 2018). Crucially, the "roof" of the HERM model is composed of People-Process-Planet (technology). This triad underscores that effective risk management depends not only on policies but on competent personnel, well-designed processes, and advanced technological

tools. The paper argues that risk owners must be certified professionals capable of interpreting data, exercising judgment, and coordinating across organizational silos (Koldovskiy, 2024).

4.3. HERM as a Closed-Loop System

To operationalize this architecture, the paper introduces the Input-Process-Output-Control (IPOC) HERM Framework (Figure 2). This model conceptualizes risk management as a continuous learning cycle rather than a static control mechanism. The Input stage involves crafting a holistic corporate strategy that explicitly incorporates risk appetite and capacity in response to VUCA conditions. This requires leaders to anticipate external shocks, regulatory changes, and technological disruptions rather than reacting to them retrospectively. The Process stage focuses on implementing HERM policies, assigning clear risk ownership, and aligning Key Performance Indicators (KPIs) with specific processes and projects. Unlike traditional ERM, where risk metrics often remain at the board level, HERM ensures that KRIs and KPIs cascade down to middle and functional management.

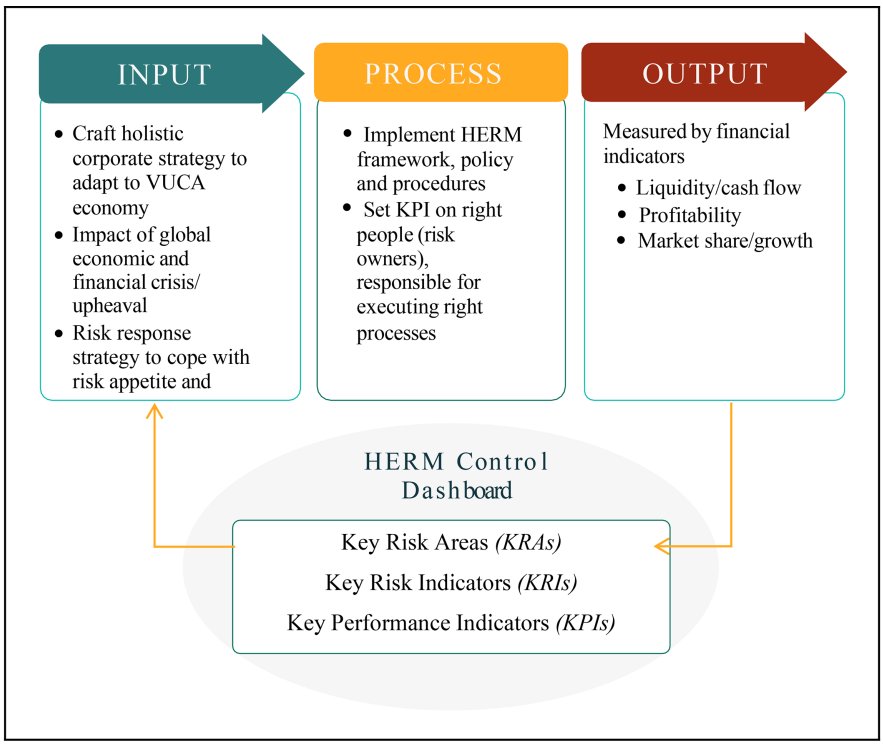


Figure 2. The input-process-output-control HERM framework.

The Output stage evaluates performance through financial and operational indicators such as liquidity, profitability, and market share. However, HERM emphasizes that financial performance must be interpreted alongside risk performance, rather than treated as an independent outcome. Finally, the Control stage uses a risk dashboard to monitor Key Risk Areas (KRAs), Key Risk Indi-

cators (KRIs), and KPIs in real time. This closed-loop structure ensures continuous feedback, learning, and adaptation—a key requirement in VUCA environments.

4.4. The 6As of HERM Implementation

Recognizing that technical frameworks alone cannot drive change, the paper introduces the 6As of transition management as a behavioral and organizational mechanism for embedding HERM into corporate practice (Table 2).

Table 2. The six as of implementation for the HERM model.

People	Process	Risk
AWARENESS	Identity	The internal and external environmental risks faced by a company using What, Why and How?
ALIGNMENT	Map	Map out the HERM policy which includes the KRAs and KRIs
ACTION	Set	KRIs and KPIs to risk owners
ADOPTION	Support	Support from stakeholders to implement HERM
ASSURANCE	Optimize	Corporate risk appetite with risk capacity through HERM governance framework
ANTICIPATION	Monitor and control	Using the risk assessment matrix

- Awareness ensures that leaders and employees understand the systemic nature of risk.
- Alignment maps risk policies to strategic objectives and operational realities.
- Action assigns KRIs and KPIs to accountable risk owners.
- Adoption secures stakeholder buy-in, particularly from boards, regulators, and senior management.
- Assurance balances risk appetite with risk capacity through governance oversight.
- Anticipation emphasizes proactive monitoring using risk assessment matrices rather than reactive crisis management.

This change model highlights that HERM is as much a cultural transformation as it is a technical reform. This model integrates risk and performance management into a single framework.

4.5. The Five Whys and the Strategic Rationale for HERM (Table 3)

The paper strengthens the conceptual foundation of HERM using the five Whys of design thinking (Table 3). This approach justifies HERM at multiple levels:

Table 3. The five Whys of holistic enterprise risk management.

5 Whys	Questions on 5 Whys	Outcome
1) Why Nation?	Why is HERM vital to African nations for attracting foreign investment?	To manage the balance of payments, GDP growth, fiscal and monetary policy
2) Why Industry?	Why is HERM imperative to African banking industry sustainability?	To Grow, Globe and Glow its industry, infrastructure, and incentives
3) Why Bank?	Why is HERM crucial to the survival of an African bank?	To balance risk appetite (*strategic plan*) with risk capacity (*financial budget*) to prevent financial crisis
4) Why Government?	Why is HERM important to every African nation?	To attract foreign direct investments (*FDIs*) and safeguard foreign reserves for stability in government policy
5) Why Global Institution?	Why is HERM of paramount importance to global banking institutions?	To control the pace of economic growth, to prevent overheating, and control bad debts

- At the national level, HERM supports macroeconomic stability and foreign direct investment.
- At the industry level, it enhances banking sustainability and competitiveness.
- At the firm level, it balances risk appetite with financial capacity to prevent crises.
- At the government level, it safeguards national financial stability.
- At the global level, it mitigates systemic risks such as asset bubbles and financial contagion.

This multi-level justification positions HERM not merely as a firm-level tool but as a governance mechanism with broader economic implications.

4.6. From Procedural ERM to Transformational HERM

The conceptual distinction between ERM and HERM lies in their underlying philosophies. ERM remains predominantly procedural, emphasizing documentation, reporting, and compliance checklists. HERM, by contrast, is transformational: it seeks to change how organizations think about risk, how leaders behave under uncertainty, and how technology supports decision-making. Where ERM treats risk as something to be minimized, HERM views risk as an inherent feature of strategic action that must be intelligently managed rather than avoided. This shift aligns with contemporary perspectives in strategy and innovation, which argue that risk-taking is essential for growth and competitiveness. In sum, HERM represents a significant theoretical advancement in risk management by integrating strategy, governance, culture, and technology into a unified framework. It builds on existing standards (COSO, ISO, Basel) but transcends their limitations by embedding risk into the fabric of organizational life. By linking corporate vision, risk culture, digital infrastructure, and performance management through a coherent architecture, HERM offers a more resilient and adaptive model for banks operating in a VUCA world. This conceptual foundation sets the stage for the empirical and ap-

plied analyses that follow in subsequent sections of the paper.

Risk Capacity: Risk capacity refers to the maximum level of risk a bank can absorb without breaching regulatory capital, liquidity, or solvency constraints. In practice, risk capacity is assessed primarily through quantitative indicators, including capital adequacy ratios, liquidity coverage ratios, stress-testing outcomes, and regulatory capital buffers.

Risk Culture: Risk culture describes the collective values, norms, and behaviors that shape how employees perceive and respond to risk within an organization. It is assessed using qualitative mechanisms, including governance reviews, board oversight evaluations, leadership behaviors, and internal audit assessments of accountability structures.

Strategy-Execution Gap: The strategy-execution gap refers to the disconnect between strategic objectives defined at the corporate level and their effective implementation across operational units. In banking organizations, this gap can be assessed through both quantitative and qualitative indicators, such as misaligned performance incentives, delayed implementation of risk controls, operational losses, and governance failures. Within the HERM framework, these constructs are measured through a combination of financial indicators (KPIs), risk indicators (KRIs), and governance assessments embedded in the HERM Balanced Scorecard (Goh, 2018).

5. The HERM Framework: Core Components

5.1. The Input-Process-Output-Control (IPOC) Model

The Holistic Enterprise Risk Management (HERM) framework is conceptualized as a closed-loop, dynamic system rather than a static compliance mechanism. Consistent with systems-thinking perspectives in risk governance, the Input-Process-Output-Control (IPOC) structure ensures continuous alignment between corporate strategy, risk governance, and operational execution in a VUCA environment (Brown, 2008; Sinha & Arena, 2018). At the Input stage, risk management begins with strategic intent rather than control activities. Corporate strategy must be explicitly aligned with risk appetite and risk capacity, reflecting COSO's (2017) emphasis on integrating risk with strategy and performance. Senior leadership defines acceptable risk levels in pursuit of growth while considering capital constraints, regulatory expectations, and stakeholder tolerance (BIS, 2010). Simultaneously, organizations must systematically assess VUCA risks—volatility, uncertainty, complexity, and ambiguity—particularly in banking, where systemic interdependencies amplify risk exposure (Goh, 2018). This assessment informs the identification of Key Risk Areas (KRAs) that are most critical to organizational resilience and value creation.

The Process stage translates strategic intent into coordinated action. In line with Basel's principles for effective risk data aggregation and reporting, robust digital infrastructure is essential for real-time risk monitoring and decision support (BIS, 2012). Unlike traditional ERM, where risk responsibilities often remain centralized,

HERM distributes accountability across the organization by assigning KRIs and KPIs to specific process owners at corporate, business, and operational levels (Moeller, 2011). At the Output stage, success is evaluated through both financial and risk performance. Effective HERM implementation should improve liquidity management, profitability, and organizational stability while reducing fraud, operational failures, and regulatory breaches (BIS, 2010). This reframes risk management as a value-creating capability rather than a compliance cost. Finally, the Control stage ensures continuous learning and adaptation. Risk performance is monitored through KRIs and KPIs embedded within an executive risk dashboard, enabling early warning and board oversight. This closed-loop learning cycle aligns with design-thinking principles of iterative improvement rather than one-time compliance (Brown, 2008).

5.2. Theoretical Contributions

This paper advances risk management theory in three interrelated ways by reconceptualizing Enterprise Risk Management through the lens of Holistic Enterprise Risk Management (HERM). Rather than treating risk as a technical or compliance function, the study positions risk as an integrated organizational capability embedded in strategy, systems, and culture (Goh, 2018). While COSO (2017), ISO 31000 (ISO, 2018), and Basel III provide important guidance on risk governance, HERM introduces three key innovations:

Framework	Focus	Limitation	HERM Contribution
COSO ERM	Integration of risk with strategy	Largely governance-focused	Adds operational cascade via KRAs/KRIs/KPIs
ISO 31000	Principles-based risk management	Limited guidance on execution	Embeds risk into organizational processes
Basel III	Capital and liquidity regulation	Primarily regulatory	Integrates strategy, culture, technology

The principal novelty of HERM lies in translating strategic risk governance into operational decision-making through a closed-loop system linking strategy, execution, and control.

First, the paper advances the integration of strategy and risk. Traditional ERM frameworks—while valuable—have tended to separate strategic planning from risk oversight, often relegating risk to back-office functions (Moeller, 2011). By contrast, HERM reframes risk as a core strategic resource rather than a constraint. Building on COSO's (2017) call for closer alignment between risk and performance, HERM embeds risk appetite directly into corporate strategy formulation and execution. The Input-Process-Output-Control (IPOC) model illustrates how strategic intent, risk assessment, and operational execution can be integrated within a continuous feedback loop. This contributes theoretically by shifting the focus from risk mitigation to risk-informed value creation, particularly in volatile environments (Sinha

& Arena, 2018).

Second, the study contributes a system-based risk architecture. Drawing on systems thinking, HERM connects corporate, business, and operational levels within a unified governance framework. Unlike fragmented ERM approaches that operate in silos, HERM establishes vertical and horizontal coherence through KRAs, KRIs, and KPIs cascading across organizational layers. This extends emphasis on integrated risk data aggregation by embedding analytics within decision-making processes rather than treating them as reporting tools. The HERM Balanced Scorecard further bridges strategy and execution by linking risk performance with organizational learning, customer trust, internal process integrity, and financial stability (COSO, 2017). Theoretically, this advances risk scholarship by demonstrating how multi-level alignment can reduce the persistent strategy-execution gap in banking (Sinha & Arena, 2018).

Third, the paper foregrounds a behavioral and cultural lens on risk. Much of traditional ERM literature privileges technical controls over human factors. HERM, however, recognizes leadership behavior and organizational culture as primary determinants of risk outcomes. The 6As Change Model highlights how awareness, alignment, and adoption shape collective risk consciousness, while assurance and anticipation institutionalize proactive governance (Goh, 2018). This aligns with behavioral insights from Kahneman and Tversky (1979), suggesting that risk decisions are shaped as much by cognition and culture as by formal models. By integrating ethical governance, accountability, and learning into risk management, HERM advances a socio-technical understanding of risk that moves beyond mechanistic control systems.

Collectively, these contributions reposition risk management as a dynamic capability rather than a static compliance apparatus. HERM integrates regulatory standards (Basel III; BIS, 2010), managerial frameworks (COSO, 2017), and design thinking principles (Brown, 2008) into a coherent theoretical model suited to VUCA conditions. This synthesis extends the boundaries of ERM scholarship by demonstrating how strategy, systems, and culture can be mutually reinforcing rather than fragmented domains of governance.

6. Managerial Implications

The HERM framework offers several practical implications for bank executives, boards, and regulators seeking to strengthen resilience in an increasingly uncertain financial landscape. Risks in banking organizations frequently emerge during the implementation of strategic initiatives, where incentives, processes, and technology interact with organizational behavior. Poorly designed incentive structures can create conduct risks, as illustrated by the Wells Fargo scandal, where aggressive cross-selling targets led employees to open unauthorized accounts. Similarly, weak product rollout governance in digital banking may expose institutions to cybersecurity or regulatory risks when fintech products are introduced without sufficient compliance oversight. In addition, inadequate IT change control during

technology upgrades can disrupt payment systems or compromise data security. These mechanisms illustrate that risks often arise from internal strategic execution rather than external shocks alone (Goh, 2018).

First, boards must actively own risk strategy. Traditional governance often delegates risk oversight to specialized committees or compliance teams, which can create accountability gaps (Moeller, 2011). HERM argues that boards should treat risk as a strategic agenda item rather than a technical compliance issue. This requires directors to engage directly with risk appetite statements, scenario planning, and VUCA assessments rather than relying solely on risk dashboards. Consistent with Basel III principles, board-level engagement enhances liquidity planning, capital adequacy, and long-term stability (BIS, 2010).

Second, risk should be embedded in performance incentives. Many banking scandals—including Wells Fargo and Commonwealth Bank—stemmed from misaligned incentives that prioritized growth over governance (Bloomberg, 2016, 2017). HERM recommends integrating KRIs alongside KPIs in managerial evaluation systems so that executives are rewarded not only for profitability but also for risk integrity. The HERM Balanced Scorecard operationalizes this by linking financial performance to customer trust, process resilience, and learning capability (COSO, 2017).

Third, digital risk analytics should complement human judgment. Modern banking risks—cybersecurity, algorithmic trading, and cross-border transactions—require sophisticated data infrastructure. In line with Basel's risk data principles, banks should invest in RegTech and RiskTech platforms that enable real-time monitoring and predictive analytics (BIS, 2012). However, HERM cautions against overreliance on algorithms; expert judgment, ethical reasoning, and contextual understanding remain essential to avoid model risk and cognitive blind spots (Brown, 2008).

Fourth, regulators should assess risk culture, not just compliance metrics. Traditional supervision emphasizes capital ratios, stress tests, and control checklists. HERM suggests that regulators should also evaluate organizational culture, leadership behavior, and accountability structures, as these often predict risk failures more reliably than technical indicators. This aligns with post-crisis regulatory trends emphasizing conduct risk and governance quality alongside prudential measures (BIS, 2010).

More broadly, HERM encourages a shift from reactive crisis management to proactive resilience-building. By integrating strategy, culture, and technology, banks can better anticipate shocks, adapt to digital disruption, and maintain stakeholder trust. For emerging-market banks, where institutional volatility is high, HERM offers a particularly valuable governance blueprint for sustainable growth.

7. Limitations and Future Research

This study is primarily conceptual and exploratory, drawing on three illustrative African banking cases rather than large-scale quantitative analysis. While the cases

provide rich practical insights, they do not allow for statistical generalization across all banking contexts (Goh, 2018). Future research should therefore subject the HERM framework to rigorous empirical testing.

First, scholars could conduct multi-country quantitative studies comparing banks that have adopted HERM-like practices with those using traditional ERM. Structural equation modeling or panel regression could assess whether HERM implementation correlates with improved liquidity, reduced compliance breaches, or enhanced profitability (BIS, 2010).

Second, comparative research should examine performance differences between HERM and conventional ERM systems over time. Longitudinal studies could track how risk culture, board engagement, and digital analytics capabilities influence crisis resilience and recovery speed (COSO, 2017).

Third, cross-country regulatory differences warrant further investigation. Emerging markets face distinct institutional risks compared with developed economies; thus, HERM's applicability may vary depending on legal frameworks, supervisory regimes, and market maturity (Sinha & Arena, 2018).

Finally, future work could explore how artificial intelligence, machine learning, and blockchain technologies interact with HERM governance structures. As digital finance evolves, new risks and opportunities will emerge that require continuous theoretical refinement.

Despite these limitations, this paper offers a robust conceptual foundation for rethinking enterprise risk governance in banking.

8. Discussion and Conclusion

In an increasingly VUCA world, fragmented and compliance-driven ERM frameworks are insufficient for ensuring banking stability and organizational resilience. Major financial scandals have demonstrated that technical controls alone cannot prevent systemic failures rooted in misaligned strategy, weak governance, and problematic organizational culture (Bloomberg, 2016, 2017). The HERM framework links corporate strategy with risk governance through cascading alignment between risk appetite, KRAs, KRIs, and KPIs. For example, a bank seeking to expand its SME lending portfolio by 20% within three years may establish a risk appetite threshold requiring the Liquidity Coverage Ratio (LCR) to remain above 110%. Liquidity risk becomes the primary Key Risk Area (KRA), monitored through Key Risk Indicators (KRIs) such as LCR, Net Stable Funding Ratio (NSFR), and wholesale funding dependency. At the operational level, Key Performance Indicators (KPIs) measure SME loan growth and profitability. If LCR falls below the threshold, lending approvals trigger enhanced treasury review and board oversight.

This paper proposes Holistic Enterprise Risk Management (HERM) as a strategy-centered, systems-based, and culture-aware alternative to traditional ERM. By integrating corporate vision, risk culture, digital infrastructure, and performance management within a closed-loop IPOC model, HERM bridges the persistent gap between strategy formulation and execution (Sinha & Arena, 2018).

The framework's 6As Change Model highlights that effective risk governance requires behavioral transformation, not merely procedural compliance (Goh, 2018). Meanwhile, the HERM Balanced Scorecard embeds risk directly into organizational performance, aligning financial success with ethical conduct, operational resilience, and stakeholder trust (COSO, 2017).

The application of HERM in three African banks illustrates its practical relevance in high-risk institutional environments, where volatility, regulatory uncertainty, and digital disruption are pervasive. By strengthening board oversight, enhancing data governance, and aligning incentives with risk integrity, HERM offers a pathway toward sustainable banking stability (BIS, 2012).

The HERM framework operates within a three-lines-of-defense governance model. The Board of Directors provides strategic oversight by approving risk appetite and monitoring enterprise risk exposure. Senior management implements HERM policies and assigns KRAs, KRIs, and KPIs across business units to ensure operational alignment. Risk owners and operational managers manage day-to-day risks and escalate emerging issues when thresholds are approached. Independent oversight is provided by risk management, compliance, and internal audit functions, while regulators assess capital adequacy and governance standards. When conflicts arise between profitability objectives (KPIs) and risk indicators (KRIs), escalation protocols within the HERM dashboard ensure that risk committees or the board review decisions before strategic initiatives proceed.

Ultimately, HERM reframes risk not as a threat to be minimized but as an inherent dimension of strategic action that must be intelligently managed. As financial systems become more interconnected and technologically complex, holistic approaches such as HERM will be essential for building resilient, trustworthy, and adaptive banking institutions—particularly in emerging markets.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Agarwal, R., & Ansell, J. (2016). Strategic Change in Enterprise Risk Management. *Strategic Change, 25,* 427-439. https://doi.org/10.1002/jsc.2072

Andersen, T. J., & Young, P. C. (2023). Enhancing Public Sector Enterprise Risk Management through Interactive Information Processing. *Frontiers in Research Metrics and Analytics, 8,* Article 1239447. https://doi.org/10.3389/frma.2023.1239447

Bank for International Settlements (BIS) (2010). *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems.* BIS.

Bank for International Settlements (BIS) (2012). *Principles for Effective Risk Data Aggregation and Risk Reporting.* BIS.

BCBS (2010). *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems.* https://www.bis.org/publ/bcbs189_dec2010.htm

Black, F., & Scholes, M. (1973). The Pricing of Options and Corporate Liabilities. *Journal of Political Economy, 81,* 637-654. https://doi.org/10.1086/260062

Blaskovich, J., & Taylor, E. Z. (2011). By the Numbers: Individual Bias and Enterprise Risk Management. *Journal of Behavioral and Applied Management, 13,* 5-23. https://doi.org/10.21818/001c.17867

Bloomberg (2016). *Wells Fargo Cross-Selling Scandal.* Bloomberg News.

Bloomberg (2017). *Commonwealth Bank Anti-Money Laundering Breaches.* Bloomberg News.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2014). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48,* 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

Brown, I., Steen, A., & Foreman, J. (2009). Risk Management in Corporate Governance: A Review and Proposal. *Corporate Governance: An International Review, 17,* 546-558. https://doi.org/10.1111/j.1467-8683.2009.00763.x

Brown, T. (2008). Design Thinking. *Harvard Business Review, 86,* 84-92.

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

D'Arcy, S. (1999). *Enterprise Risk Management.* Wiley.

Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review, 16,* 147-166. https://doi.org/10.1111/rmir.12016

Dürst, N., & Kunz, J. (2025). Embedding Risk Culture in a Financial Institution: An Action Research Perspective. *Review of Managerial Science*. https://doi.org/10.1007/s11846-025-00946-2

Gleißner, W., & Berger, T. B. (2024). Enterprise Risk Management: Improving Embedded Risk Management and Risk Governance. *Risks, 12,* Article 196. https://doi.org/10.3390/risks12120196

Goh, C. (2018). *Design Thinking for Enterprise Risk Management: A Holistic Action Research Approach Using Three African Banks as Case Studies.* Ph.D. Thesis, University of Information Technology and Management.

Grunewald, D., Feis, G. D., & Atallo, D. (2017). When Cross-Selling Crosses the Line: Wells Fargo and Unintended Consequences. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921039

International Organization for Standardization (ISO) (2018). *ISO 31000: Risk Management-Guidelines.* ISO.

Jedynak, P., & Bąk, S. (2021). *Risk Management in Crisis.* Routledge. https://doi.org/10.4324/9781003131366

Jengwa, E., & Pellissier, R. (2022). An Operational Excellence Strategy Implementation Model for Growth in a Volatile, Uncertain, Complex, and Ambiguous Environment. *Acta Commercii, 22,* a960. https://doi.org/10.4102/ac.v22i1.960

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47,* 263-291. https://doi.org/10.2307/1914185

Koldovskiy, A. (2024). Strategic Infrastructure Transformation: Revolutionizing Financial Sector Management for Enhanced Success. *Acta Academiae Beregsasiensis. Economics, 5,* 323-332. https://doi.org/10.58423/2786-6742/2024-5-323-332

Kunz, J., & Heitz, M. (2021). Banks' Risk Culture and Management Control Systems: A Systematic Literature Review. *Journal of Management Control, 32,* 439-493. https://doi.org/10.1007/s00187-021-00325-4

Lelissa, T. B. (2014). Factors Influencing the Level of Credit Risk in Ethiopian Commercial Banks. *European Journal of Business and Management, 6,* 139-150.

Markowitz, H. (1952). Portfolio Selection. *The Journal of Finance, 7,* 77-91. https://doi.org/10.2307/2975974

Mathrani, S., & Mathrani, A. (2013). Utilizing Enterprise Systems for Managing Enterprise Risks. *Computers in Industry, 64,* 476-483. https://doi.org/10.1016/j.compind.2013.02.002

Merton, R. C. (1989). On the Application of the Continuous-Time Theory of Finance to Financial Intermediation and Insurance. *The Geneva Papers on Risk and Insurance—Issues and Practice, 14,* 225-261. https://doi.org/10.1057/gpp.1989.21

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A Framework for Enterprise Risk Identification and Management: The Resource-Based View. *Managerial Auditing Journal, 34,* 162-188. https://doi.org/10.1108/maj-12-2017-1751

Moeller, R. R. (2011). *COSO Enterprise Risk Management: Understanding the New Integrated Framework.* Wiley. https://doi.org/10.1002/9781118269145

Monazzam, A., & Crawford, J. (2024). The Role of Enterprise Risk Management in Enabling Organisational Resilience: A Case Study of the Swedish Mining Industry. *Journal of Management Control, 35,* 59-108. https://doi.org/10.1007/s00187-024-00370-9

Nuhić-Mešković, M., & Mešković, A. (2023). Risk Management Culture, Structure, and Process—Theoretical Insights and Empirical Evidence. *International Business Research, 16,* 10-24. https://doi.org/10.5539/ibr.v16n10p10

Oluloni, T. M. (2024). ERM Strategies for Navigating Financial Stress: Lessons from US Commercial Banks. *Finance & Accounting Research Journal, 6,* 1861-1880. https://doi.org/10.51594/farj.v6i10.1634

Przetacznik, S. (2022). The Evolution of Risk Management. *Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie, 53,* Article 95107. https://doi.org/10.25944/znmwse.2022.01-2.95107

Samad, S. A. (2025). Strengthening ERM Independence: A Conceptual Governance and Oversight Framework. *International Journal of Financial Research, 16,* 63-74. https://doi.org/10.5430/ijfr.v16n3p63

Sax, J., & Andersen, T. J. (2018). Making Risk Management Strategic: Integrating Enterprise Risk Management with Strategic Planning. *European Management Review, 16,* 719-740. https://doi.org/10.1111/emre.12185

Sinha, V. K., & Arena, M. (2018). Manifold Conceptions of the Internal Auditing of Risk Culture in the Financial Sector. *Journal of Business Ethics, 162,* 81-102. https://doi.org/10.1007/s10551-018-3969-0

Tziakou, E., Fragkaki, A. G., & Platis, A. N. (2023). Identifying Risk Management Challenges in Laboratories. *Accreditation and Quality Assurance, 28,* 167-179. https://doi.org/10.1007/s00769-023-01540-3

Viscelli, T. R., Hermanson, D. R., & Beasley, M. S. (2017). The Integration of ERM and Strategy: Implications for Corporate Governance. *Accounting Horizons, 31,* 69-82. https://doi.org/10.2308/acch-51692

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling Effective Operational Risk Management in a Financial Institution: An Action Research Study. *Journal of Management Information Systems, 34,* 727-753. https://doi.org/10.1080/07421222.2017.1373006