American Journal of Economics and Business Innovation (AJEBI)

ISSN: 2831-5588 (ONLINE), 2832-4862 (PRINT)

VOLUME 5 ISSUE 3 (2026)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Economics and Business Innovation (AJEBI)

Volume 5 Issue 3, Year 2026
ISSN: 2831-5588 (Online), 2832-4862 (Print)
DOI: https://doi.org/10.54536/ajebi.v5i3.8563
https://journals.e-palli.com/home/index.php/ajebi

Enterprise Risk Management in Saudi Arabia: Aligning COSO, ISO 31000, and National Regulatory Frameworks with Vision 2030

Mohamed Abdelhalim Soliman[1*]

Article Information

Received: June 25, 2026

Accepted: September 10, 2026

Published: November 14, 2026

Keywords

CMA, Corporate, COSO ERM, Enterprise Risk Management, ISO 31000, SAMA, Saudi Arabia, Vision 2030

ABSTRACT

Enterprise Risk Management (ERM) has become a key tool of corporate governance and strategy management; however, there is a great diversity in the application of ERM among industries and jurisdictions. An interesting institutional context is represented by the Kingdom of Saudi Arabia (KSA), where the banking sector operates within the regulations of the Saudi Arabian Monetary Authority (SAMA) according to the Basel standards of prudential regulation; the stock market operates under the CMA corporate governance code; and the vision of state transformation named Vision 2030, which radically alters the structure of the state apparatus, financial sector and private businesses of the country. The paper provides an extensive examination of Enterprise Risk Management (ERM) frameworks such as the COSO Enterprise Risk Management Integrating with Strategy and Performance (2017) and ISO 31000:2018 standards. This shows how they fit into the risk management standards of SAMA and CMA. Drawing on a systematic qualitative content analysis of roughly 45 documents retrieved from Google Scholar, Scopus, Web of Science, ProQuest, and SSRN, the literature review integrates theoretical discussion and empirical research related to ERM value creation with special emphasis on ERM-related research on Saudi and GCC companies. According to the results of the analysis, Saudi companies function within a fragmented risk governance regime where the integration of prudential, market conduct, and strategic risk management needs is not achieved. As a result, the paper formulates an integrated Saudi ERM model combining the process-driven approach of ISO 31000 with the components of COSO and SAMA/CMA regulations and connecting risk appetite with Vision 2030 goals. The model serves as the major theoretical contribution of the paper; its practical contribution is a phased plan for the implementation of the proposed model by Saudi banks, listed corporations, and governmental institutions. The paper effectively distinguishes between findings of the analysis, conclusions reached by the authors, and recommendations, and ends with implications for policy and future research directions.

INTRODUCTION

One of the most important economic transitions in the twenty-first century takes place within the Kingdom of Saudi Arabia. Introduced in 2016, the Vision 2030 aims to diversify the economy which was previously dependent on oil resources; increase the contribution of the private sector, and improve the development of the financial market of the country (Vision 2030, 2016). The Financial Sector Development Program (FSDP) is one of those realization programs of the Vision and focuses on the development of the banking, insurance, equity, and debt markets, financial inclusion, and regulation (Vision 2030, n.d.). In this context, enterprise risk management has stopped being merely a compliance requirement and has become a strategic goal for each company private, listed, or governmental that operates in the Kingdom of Saudi Arabia. However, the risk management structure of institutions in Saudi Arabia is very fragmented. The SAMA regulates the banks on the basis of a prudential system that is in compliance with the Basel requirements, and risk management rules for banks have been framed (Saudi Central Bank [SAMA], 2023b). With regard to the listed joint stock companies, the risk and internal control are managed by the CMA under the Corporate Governance Regulations (Capital Market Authority [CMA], 2017). There is no special regulatory regime with regard to the risk management in the public sector institutions, such as sovereign wealth funds and giga projects associated with the vision 2030, who mostly draw their ideas for risk management from the international standard of COSO enterprise risk management (2017) and ISO 31000:2018 (International Organization for Standardization [ISO], 2018). In consequence, there is an overlap and conflict of the following: an organization may be faced with the prudential risk management regulations by SAMA, corporate governance risk disclosure by CMA, and risk from strategic perspective due to vision 2030 objectives.

The division is not merely bureaucratic in nature. From an international research perspective, ERM brings about an increase in risk-adjusted performance only when the concept is effectively combined with strategy and decision-making processes (Gordon *et al.*, 2009; Hoyt & Liebenberg, 2011; Florio & Leoni, 2017); otherwise, when ERM is implemented formally, it becomes costly and provides no benefits to the company (Bromiley *et al.*, 2015; Power, 2009). Consequently, whether Saudi organizations benefit from ERM is determined by whether they implement ERM frameworks that are

[1] International Business Academy of Switzerland (IBAS), Switzerland
[*] Corresponding author's e-mail: mohamed.abdelhalimsoliman@researchpublication.co

coherent and appropriate for their specific situation. SAMA manages the banks through a holistic prudential framework. The literature about ERM in Saudi Arabia is very new and fragmented in the sense that researchers are dealing with the topics such as risk disclosures and performance (Al-Dubai & Abdelhalim, 2021), features of board of directors and audit committees (Al-Matari, 2022; Algrady *et al.*, 2025), risk management in Saudi banks (Al-Zeer & Al-Saber, 2020), and risk governance in GCC financial institutions (Al-Hadi *et al.*, 2016, 2019). As far as the author is aware of, there is no study that compares the international ERM frameworks with the Saudi regulations. This paper will try to bridge this gap in three ways. First, the paper aims at providing a systematically reviewed major ERM frameworks which include the frameworks like COSO (2017) and ISO 31000:2018 with SAMA and CMA risk management regulations in the context of Vision 2030. The second task involves synthesizing the existing empirical literature on ERM value creation, particularly with regard to the experiences of Saudi and GCC companies, so as to establish what is well-established and what is not. Finally, this paper makes an attempt to propose an integrative ERM framework for Saudi Arabia that would incorporate ISO 31000 process orientation and COSO component model along with SAMA and CMA mandatory stipulations and the risk appetite of enterprises vis-à-vis Vision 2030 goals.

The contribution is thus two-fold. First, theoretically, the paper provides an understanding of framework integration into a national strategic aim Vision 2030 and goes beyond the theoretical discussion of best practices and answers the call for contextualized ERM research (Mikes & Kaplan, 2015; Bromiley *et al.*, 2015). Second, practically, it provides the Saudi board members, chief risk officers, regulators, and policy makers a roadmap for implementing ERM which would satisfy all regulators without duplication of cost. Throughout the paper, evidence (in Section 2), author analysis (in Sections 4 and 5), and author's recommendations (in Section 6) are separated. The rest of the paper is organized as follows. Section 2 provides a review of the existing literature related to the concepts of ERM, COSO and ISO frameworks, the empirical findings relating to the ERM-firm performance nexus, and the existing research regarding ERM in the GCC and Saudi Arabia. Section 3 outlines the methodology used in this study, comprising the search process, inclusion/exclusion criteria, and analytical approach. Section 4 highlights the results of the analysis: the Saudi regulatory environment, the comparative assessment of the four reference frameworks, and the review of the empirical evidence. Section 5 deals with the integration of the frameworks and the contribution of the study both theoretically and practically.

LITERATURE REVIEW

Enterprise Risk Management: Concept and Evolution

ERM refers to the integrated approach used by firms to manage all types of risks associated with the operations of the business. The fact remains that the concept came about due to the necessity of coming up with something to replace the then existing approach of silo risk management whereby risks such as credit risk, market risks, operational risks and strategic risks among others were separately managed (Nocco & Stulz, 2006). In fact, the first description of ERM on a global level came from COSO in their report "Enterprise Risk Management – Integrated Framework" published in 2004 where ERM was described 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 exposures within its risk appetite".

Agency and stakeholder theories represent the main theoretical underpinning for enterprise risk management. According to agency theory, risk management is a means of control used by board members to control the risk-taking behavior of self-serving managers and get their actions aligned with the interests of the stockholders (Bhimani, 2009); ERM decreases information asymmetry in relation to the company's overall risk level. On the other hand, stakeholder theory calls attention to the need to take responsibility for creditors, employees, governmental agencies, and society because risk-taking creates externalities for all of these stakeholders (Amico, 2014). Both theories are relevant to the case of Saudi Arabia.

There were two milestones that turned ERM into a strategically driven concept. First, the financial crisis that began in 2007 revealed the insufficiency of isolated risks management practices and led to the necessity for regulators, including the Basel Committee on Banking Supervision (2015), to make the Board responsible for risks. Second, the 2017 update of the COSO framework has moved risk management from the back office into the strategy room making strategy and performance the core concepts of the discipline (COSO, 2017). These facts define the approach of this paper to ERM as governance competency developed by organizations at any stage of maturity (Beasley *et al.*, 2015).

The COSO ERM Framework (2017)

The COSO 2017 Enterprise Risk Management—Integrating with Strategy and Performance Framework has replaced the previous 2004 version and is the most widely used ERM framework worldwide (COSO, 2017). The framework posits that ERM builds and sustains value through linkage of risk to strategy and performance. This framework divides the 20 principles of ERM into five interdependent components, namely (a) governance and culture, whereby the board is involved in oversight and creation of structure and culture, and defining values; (b) strategy and objective setting, whereby risk considerations are integrated into strategy development process and determination of risk appetite and evaluation of strategies; (c) performance, whereby identification, assessment, prioritization, and response to risks that may

impact on the strategy and objectives is done; (d) review and revision, whereby ERM is assessed in case of any substantial change; and (e) information, communication, and reporting, whereby information about risk for governing the entity is acquired and communicated (COSO, 2017).

There are three aspects of the 2017 framework which are highly relevant to the Saudi case. First, risk has a dual-valence quality in that it incorporates both threats and opportunities, and the framework considers the risk that the strategy does not match the mission, vision, and values. Second, risk appetite and risk tolerance are highlighted as strategic tools whose setting is done by the board and implementation by management. Third, ERM has to be used not only for implementation but in the process of strategy formulation as well. This makes the COSO framework (2017) a very good choice to be the architecture of the Saudi framework as it links governance of the board (CMA) with risk appetite (SAMA) and strategic objectives of the nation (Vision 2030).

The criticism raised against COSO (2017) includes the point that it is expensive and difficult to implement fully, that it needs considerable interpretation due to its principle-based approach, and that it is not generally implemented in its entirety in small to medium-sized firms outside of financial organizations and multinational corporations (Bromiley *et al.*, 2015; Gjerdrum & Peter, 2010). This line of reasoning becomes especially pertinent in emerging economies, where there is a competition between formal guidelines and small talent pool and immature internal control system; evidence of incomplete implementation suggests that ceremonial implementation does not add much value (Power, 2009; Arena *et al.*, 2010).

The ISO 31000:2018 Standard

ISO 31000:2018, Risk Management Guidelines, is the second pillar of the international risk management framework (ISO, 2018). The standard provides principles, framework, and process of managing risk, which an organization may adapt regardless of its size, activities, and sectors. ISO 31000:2018 has been developed with consideration to eight principles: risk management is an integrated, structured, and comprehensive approach, tailor-made, inclusive, dynamic, and improving, and creates and retains value and responds to uncertainty. The framework of the standard consists of five elements: leadership and commitment, integration, design, implementation, and evaluation and improvement, thus making the risk management an essential component of governance and management system of the organization. The process of ISO 31000:2018 is presented in the cycle structure: communication and consultation; scope, context, and criteria; risk assessment (identification, analysis, and evaluation); risk treatment; monitoring and review; and documentation and reporting (ISO, 2018).

The relative strengths of COSO (2017) and ISO 31000:2018 have been extensively discussed before (Gjerdrum & Peter, 2010; Mikes & Kaplan, 2015). The strength of COSO is its governance orientation: specifying accountability, linking risk to strategy and performance and matching the governance requirements of internal controls and audits. On the other hand, ISO 31000 is process oriented, simpler, industry agnostic and more clear-cut in emphasizing that risk management is continuous and iterative, while staying purposefully vague on questions of governance and risk appetite. In the context of Saudi organizations, the two standards are complementary as opposed to being competitors. An institution that adopts ISO 31000 in terms of process discipline requires COSO to satisfy the risk governance requirements of SAMA; an organization adopting COSO requires the process approach of ISO 31000 for operational risk assessment. This complementarity forms the basis of the integrated framework discussed in Section 5.

ERM and Firm Performance: Empirical Evidence

There is a rich literature on ERM value creation, albeit with some disagreement. Cross-sectional studies from the US insurance industry revealed a positive link between ERM implementation and firm value (Hoyt & Liebenberg, 2011); moreover, contingency studies have shown that the performance consequences of ERM depend on whether ERM fits with other firm-specific and environmental factors (Gordon *et al.*, 2009). The European evidence supports this; indeed, Florio and Leoni (2017) found in their study of Italian publicly-listed firms that greater implementation of ERM is linked with better performance, especially when ERM goes beyond mere adoption and includes a chief risk officer and risk committees. Nocco and Stulz (2006) offer the standard theoretical explanation of how ERM creates value through decreasing lower tail events, better capital allocation, and risk profile understanding of investors. There is sector-specific support for both drivers of ERM implementation; thus, in the insurance industry, ERM is implemented due to regulation, and due to perceived business value as well (Jabbour & Abdel-Kader, 2016).

A counter literature runs parallel to these arguments. According to Bromiley *et al.* (2015), a significant amount of research on ERM is flawed in terms of ambiguous constructs and poor identification while benefits of ERM are often claimed rather than demonstrated. In the same line of thought, Power (2009) states that risk management can be ritualistic – "risk management of nothing" – in which organizations focus on managing the impression of risk rather than the risk itself. Arena *et al.* (2010) state that ERM systems are influenced by organizational politics and are likely to not influence decision making in any way. Mikes and Kaplan (2015) claim that ERM practices may differ from organization to organization and there cannot be a universal model applicable to all organizations because every organization's strategies will be different – an important point considering the case of Saudi Arabia where even banks, listed companies, and public sector organizations are worlds apart.

ERM in the Gulf Cooperation Council and Saudi Arabia

Research into ERM in the GCC region and Saudi Arabia has been increasing at a fast pace since 2017 in conjunction with an increase in regulatory scrutiny. With regard to risk governance, studies by Al-Hadi *et al.* (2016) confirm that risk committee presence and diligence help in disclosing market risk for financial institutions in the GCC region. However, studies by Al-Yahyaee and Al-Hadi (2016) find that when the risk committee members have too many commitments, it can undermine the effect of monitoring. Studies by Al-Hadi *et al.* (2019) further expand on the topic by analyzing the relationship between risk management and governance for banks in the GCC region. For Saudi banks, the studies by Al-Zeer and Al-Saber (2020) analyze the use of ERM in the sector and find that its application is inconsistent, with credit risks being prevalent compared to strategic and operational risks.

At the corporate governance level, Boshnak (2021) observes increased board governance for the Saudi listed firms since the introduction of CMA regulations in 2017, building on the previous studies by Al-Matari & Fadzil (2011) regarding Saudi board and audit committeesAl-Matari (2022) states that corporate governance and top management team diversity affect financial performance of Saudi companies operating in the financial sector. Moreover, Algrady *et al.* (2025) find that audit committee features positively affect the quality of financial information in Saudi and UAE companies. Alsaadi *et al.* (2021) observe that corporate governance practices are connected with high financial reporting quality of the listed Saudi firms. Moreover, Tawfik *et al.* (2022), analyzing the GCC stock markets, conclude that the relationship between the company's performance and the governance practices with regards to ownership by the royal family is essential for understanding the ownership role in Saudi Arabia, while Al-Matari (2025) also proves the link between board diversity and environmental sustainability and performance in the Saudi environment.

In regard to risk disclosure and management, Al-Dubai and Abdelhalim (2021) show that risk disclosure is positively related to the performance of listed Saudi companies, emphasizing the significance of risk disclosure to the market; Alzeban and Gwilliam (2014) provide determinants of the efficiency of internal auditing in Saudi public sector companies; and Alhamami and Alruwaili (2025) emphasize that governance, risk management, and compliance are now crucial to the performance of investments as Saudi organizations go digital. Comparative and crisis-based studies are also relevant in this regard: Shatnawi and Eldaia (2020) establish that there is a connection between ERM practices and performance of firms in Jordanian and Malaysian settings, while Grewal *et al.* (2022) argue that the coronavirus outbreak has highlighted the shortcomings of ERM frameworks across countries, including the MENA region.

There are two recent doctoral works providing the most extensive synthesis of literature. Almodawi (2024) explores the effect of audit committee attributes on ERM, internal audit, and performance in Saudi Arabia, while Al-Tayan (2022) focuses on ERM and firm value in Middle Eastern countries, finding out that adoption of ERM is correlated with firm value and that its rates are still low compared to the international level. Al-Zaimoor and Desoky (2024) and Mrabet *et al.* (2024) also contribute more GCC evidence on audit committee characteristics, board diversity, and firm risk. In general, the literature suggests three important conclusions forming the basis for the current research. First, good risk governance, including risk committees, diligent board and competent audit committee, is positively correlated with quality of disclosures and reporting and performance of firms in Saudi and GCC countries. Second, the banking industry, influenced by prudential regulations of SAMA, is the most advanced one in terms of ERM implementation, while listed nonfinancial firms and governmental entities are behind. Third, there has been no research attempting to integrate international frameworks into the Saudi regulatory framework within Vision 2030.

MATERIALS AND METHODS

Research Design and Analytical Approach

This study uses the method of qualitative content analysis (QCA), which is appropriate for the synthesis of heterogeneous documentary material (framework documents, regulations, and empirical studies) into an analytical narrative (Elo & Kyngäs, 2008). Reporting is based on the guidelines of PRISMA 2020 statement for systematic reviews, modified for qualitative, document-oriented reviews (Page *et al.*, 2021). The protocol of the review was predetermined and included the research questions, search strategy, criteria for inclusion/exclusion, and coding frame.

Search Strategy

A search was conducted from January to March 2026 using five electronic databases: Google Scholar, Scopus, Web of Science, ProQuest, and SSRN. The search involved keyword blocks relating to (a) the concept, (b) frameworks, (c) regulatory environment, and (d) geographical scope. The main search terms included "enterprise risk management Saudi Arabia," "COSO ERM," "ISO 31000," "SAMA risk management," and "CMA corporate governance," combined using Boolean operators and adapted for each specific database. The time span of the search was narrowed to publications in the period between 2017 and 2025 since the adoption of the COSO (2017) framework and the CMA (2017) regulations; literature that predates 2017 but is essential (such as COSO, 2004; Hoyt & Liebenberg, 2011; Nocco & Stulz, 2006) was identified using snowballing techniques. The full search strategy is included in Appendix A.

Inclusion and Exclusion Criteria

The documents that have been considered for review met all the following conditions: (a) They were peer-

reviewed journals, regulations or framework documents and doctoral dissertations; (b) They had content about enterprise risk management, risk governance or corporate governance with the element of risk; (c) The topics of the papers related to Saudi Arabia, the GCC, or the international frameworks (COSO, ISO) concerning the Kingdom; and (d) These were written in English. There were two exceptions made regarding the language criteria, which were as follows: official documents published in Arabic by SAMA and CMA, since they are primary sources of law and regulation. The excluded documents were non-academic and non-official sources (such as blogs or consultancy papers written by practitioners), documents not written in English (excluding official Saudi documents), and those unrelated to ERM, risk governance or corporate governance even if they mentioned risk.

Screening, Data Extraction, and Synthesis

The searches in the databases resulted in 212 hits. Exclusion of 96 duplicate papers left 116 hits which were reviewed using the titles and abstracts, excluding 71 articles that were not relevant to the research. Finally, 45 papers were reviewed in their entirety, satisfying the inclusion criteria and forming the corpus for the literature review. These 45 papers include 42 academic papers and dissertations, and three regulatory documents from Saudi Arabia (SAMA, 2023a, 2023b; CMA, 2017). In addition, seven more anchor papers were obtained directly from their sources to facilitate the framework comparison (COSO, 2017; ISO, 2018; Basel Committee, 2015; Vision 2030, 2016 and n.d.; SAMA, 2024; Page *et al.*, 2021). Thus, a total of 52 papers were used as a basis for the literature review. The screening log can be found in Appendix C.

Data coding followed a framework based on five main dimensions: (a) governance anchor (boards and committees for risk); (b) risk identification, assessment, and mitigation process; (c) strategy and risk appetite linkage; (d) reporting, disclosure and communications; and (e) contextual and institutional elements (ownership, regulations, and culture). Appendix B contains a list of the codes used in the analysis. The synthesis consisted of two main parts: thematic synthesis of the empirical literature (sections 2 and 4.3) and structured comparison of the four frameworks (section 4.2). The findings in sections 4 and 5 constitute the interpretation and synthesis of the author. Quality assessment was criterion-based: regulatory documents were seen as primary law; peer-reviewed publications were weighted depending on their method (panel studies spanning several years were valued over cross-sectional studies); and framework documents were viewed as definitive sources of the standards they articulated.

There are three limitations to the approach that must be recognized. Firstly, this is a qualitative review and no effect size is given; the significance of any ERM effects described comes from the primary study itself. Secondly, despite adjustments made for government documents written in Arabic in Saudi Arabia, there is a limitation to the use of only English literature. Finally, the time frame of the review, 2017-2025, means that anything after 2025 is not covered.

RESULTS AND DISCUSSION

The Saudi Regulatory Context

The risk regulation system in Saudi Arabia includes two major regulators with differing purposes. SAMA was created in this capacity through the Central Bank Law (M/36 of 1442H). It oversees banks, insurance firms, financial institutions, and operates a prudential regime consistent with international standards. The risk management guidelines for banks issued by SAMA require that the board of directors takes responsibility for risk management within the bank, create risk management functions and committees, risk appetite approach, stress testing, and capital planning in the internal capital adequacy assessment process (ICAP) (SAMA, 2023b). As per the Financial Stability Report (2023a) of SAMA, the Saudi financial sector proved itself resilient with high capital adequacy ratios and increased provision levels, while concentration risks and interest rate risks were among the major vulnerabilities of the system. In its Annual Report (SAMA, 2024), SAMA points at the further development of the regulatory framework, including digital financial infrastructure and supervisory technology.

The CMA is responsible for overseeing the capital market of Saudi Arabia through the Capital Market Law. According to the Corporate Governance Regulations of the CMA (2017), which apply to listed joint stock companies, the board is required to approve and oversee the company's risk management policies, establish an audit committee and, in most cases, a risk management committee, and make disclosure in respect of related party transactions, material risks, and board structures. There are several regulations that are comply-or-explain regulations—an approach that favors substance over form but provides room for different interpretations (Boshnak, 2021; Alsaadi *et al.*, 2021).

Over this framework of regulators comes Vision 2030 (2016) and its implementation programs. The Financial Sector Development Program (Vision 2030, n.d.) is focused on financial market development and diversification, while the sovereign wealth funds and giga projects that are a part of the Vision are risk bearing organizations themselves, and whose governance, audit, and risk management are required to be up to international standards (Alhamami & Alruwaili, 2025). The OECD evaluation of corporate governance enforcement in the MENA region (Amico, 2014) is highly relevant, enforcement capacity lags behind the formal adoption of the rules, and this can be seen in the Saudi case in the mismatch between SAMA banking rules and less prescriptive governance system for non-financial firms.

Comparative Analysis of ERM Frameworks

Table 1 presents a comparative evaluation of the four

Table 1: Comparative Analysis of COSO (2017), ISO 31000:2018, SAMA, CMA, and the Proposed Integrated Saudi ERM Model

Dimension	COSO ERM (2017)	ISO 31000:2018	SAMA (2023) Banking Guidelines	CMA (2017) Governance Regulations	Proposed Integrated Saudi ERM Model
Core orientation	Value creation through integration of ERM with strategy and performance; enterprise-wide and culture-based.	Generic guidelines for any organization; principles, framework, and process; value creation and protection.	Bank prudential supervision: capital adequacy, credit, market, liquidity, and operational risk management; Basel-related recovery planning.	Maintaining market integrity and investor protection: board supervision; audit and risk committees; listing company disclosures.	Creation of value through a strategy consistent ERM approach, tailored to Saudi regulatory and conduct-of-business standards and Vision 2030.
Governance anchor	Board and senior management set risk appetite and oversee governance and culture; board-level risk oversight.	Leadership and commitment; risk management integrated into governance; accountability assigned.	Board accountable for risk governance; mandatory risk committee; independent chief risk officer reporting to the board.	Board responsible for oversight of risk and internal control; audit committee; risk committee required for listed companies.	Board-level risk committee with a clear charter; CRO reporting directly to the board; coordinated audit and risk committee mandates.
Risk definition and appetite	Risk as the possibility that events affect strategy and objectives; upside and downside; formal risk appetite and tolerance statements.	Risk as the effect of uncertainty on objectives; positive and negative deviations.	Prudential risk taxonomy (credit, market, liquidity, operational, reputational, Shariah/ compliance); formal risk appetite framework required.	Prudent risk oversight implicit in board duties; risk policies to be established and disclosed.	Dual-valence risk definition; risk appetite statement linked to Vision 2030 objectives and reviewed annually.
Process structure	Five components, 20 principles: governance and culture; strategy and objective-setting; performance; review and revision; information, communication, and reporting.	Closed-loop process: communication and consultation; scope, context, and criteria; risk assessment (identification, analysis, evaluation); treatment; monitoring and review; recording and reporting.	Structured prudential cycle: ICAAP, stress testing, capital and liquidity planning, risk measurement and mitigation, monitoring, internal controls, recovery planning.	Internal control framework; audit oversight; board evaluation of internal control effectiveness.	Layered process: ISO 31000 process engine operating within the COSO component architecture; SAMA and CMA reporting requirements overlaid.
Strategy integration	ERM explicitly applied in strategy setting; evaluation of strategy alternatives; risk appetite informs strategy.	Risk criteria derived from organizational objectives; risk management integrated into all activities and decision making.	Risk appetite linked to capital planning and business strategy; strategy review embedded in ICAAP.	Board approves strategy; risk considerations inform strategic decisions and major transactions.	Strategic risk appetite statement aligned to Vision 2030 sector objectives; ERM applied at strategy formulation, not only execution.

Documentation and reporting	Information, communication, and reporting component; entity-level portfolio view reported to the board.	Recording and reporting of process outputs; continual improvement of the framework.	Regular risk reports to the board and board committees; Pillar 3 disclosure; data quality governance.	Periodic disclosure to the market: annual reports, governance report, related-party transactions, material risk information.	Unified risk reporting: annual ERM statement in the governance report (CMA), Pillar 3 disclosures (SAMA), and an integrated management risk dashboard.
Applicability in Saudi Arabia	Voluntary best practice; increasingly expected for listed and financial firms; adaptable to Vision 2030 objectives.	Voluntary and sector-neutral; applies to banks, listed firms, public sector, and giga-projects.	Mandatory for licensed banks and insurance companies supervised by SAMA.	Mandatory for listed joint-stock companies; comply-or-explain elements.	Tiered mandate: banks follow SAMA-plus-Basel; listed firms follow CMA-plus-COSO; public sector follows ISO-plus-Vision 2030.
Strengths and limitations	Strong strategy-performance linkage; comprehensive but complex and resource-intensive.	Simplicity and cross-sector validity; less prescriptive on governance structures and risk appetite.	Rigorous and prudentially calibrated; banking-specific and not directly generalizable.	Establishes board accountability and transparency; governance-centric with limited risk-process detail.	Contextualized and coherent; reduces duplication and compliance cost; requires implementation capacity and skilled risk talent.

models, which include COSO (2017), ISO 31000:2018, SAMA Banking Guidelines (2023b), and CMA Corporate Governance Regulations (2017), as well as the proposed Saudi Arabia ERM model, based on eight parameters. This is the author's evaluation of the cited models in Sections 2 and 4.1.

There are three findings. Firstly, there is complementarity in terms of orientations among these four frameworks. While COSO framework provides the governance and strategic orientation, ISO provides the sector-independent process engine, SAMA provides prudence within the context of financial sector and CMA provides market accountability for companies listed on the stock exchange. Secondly, there is no coherence in terms of language and time horizons among these four frameworks. That is, if a Saudi business is subject to more than one framework, then there is repetition rather than synergy among these four frameworks. Lastly, these four frameworks do not provide the mechanism of bridging between enterprise risks and national development goals.

Analysis: Synthesis of Empirical Evidence

There are three findings. Firstly, there is complementarity in terms of orientations among these four frameworks. While COSO framework provides the governance and strategic orientation, ISO provides the sector-independent process engine, SAMA provides prudence within the context of financial sector and CMA provides market accountability for companies listed on the stock exchange. Secondly, there is no coherence in terms of language and time horizons among these four frameworks. That is, if a Saudi business is subject to more than one framework, then there is repetition rather than synergy among these four frameworks. Lastly, these four frameworks do not provide the mechanism of bridging between enterprise risks and national development goals.

Pattern 2: Governance structure is more significant than formal adoption. In all GCC-based studies, the formation and effectiveness of risk management committees and audit committees are found to be significantly related to risk disclosures, high-quality reporting, and good performance (Al-Hadi *et al.*, 2016, 2019; Algrady *et al.*, 2025; Al-Zaimoor & Desoky, 2024; Alsaadi *et al.*, 2021). This is in line with the international observation that implementation intensity, not adoption, determines the value of ERM systems (Florio & Leoni, 2017; Beasley *et al.*, 2015). It means that in Saudi Arabia, regulators and corporate boards need to focus on the functioning of risk governance committees rather than on the quantity of risk-related documentation.

Pattern 3: Ownership affects the incentive structure for ERM. The ownership structure in Saudi Arabia, which includes ownership by the government and the royal family, determines the demand and supply of risk information (Tawfik *et al.*, 2022; Alqarni, 2021). In situations where there are dominant owners who have access to information privately, risk disclosure may not be as robust and market enforcement may be lacking. On

the other hand, internationalization in the Saudi market, including foreign investments and giga-projects and ESG issues, raises the importance of risk governance (Mrabet *et al.*, 2024; Al-Matari, 2025). This is one reason why the purely voluntary approach may not be sufficient.

Discussion

Toward an Integrated ERM Framework for Saudi Arabia

From the analysis presented in Section 4 emerges the main contribution of this paper, which is an integrated Saudi ERM framework that integrates the four aforementioned frameworks into one layered, goal-directed structure. The proposed framework is comprised of three layers. On the lowest layer, the process defined by the ISO 31000:2018 (communication and consultation; scope, context, and criteria; risk assessment; treatment; monitoring and review; recording and reporting) provides the engine for managing risks of all organizations (ISO, 2018). On the layer above, the component architecture of COSO (2017), which consists of the following elements: governance and culture, strategy and objective setting, performance, review and revision, and information, communication, and reporting, provides the governance skeleton including board oversight, risk appetite, and reporting (COSO, 2017). The highest layer is comprised of national goals coming from Vision 2030 and its programs (Vision 2030, 2016, n.d.). To each layer, there is added an overlay specific for regulators, which is SAMA prudential requirements for financial institutions (SAMA, 2023b) and CMA requirements for corporate governance and disclosure for listed companies (CMA, 2017).

The integrated approach avoids duplication rather than creating a fifth model, whose premise is mapping rather than inventing. The risk appetite principle in SAMA maps onto the strategy and objective-setting aspect of COSO; the risk committee provision in CMA maps onto the governance and culture aspect of COSO; and the SAMA Pillar 3 disclosures and annual disclosures by CMA companies merge into one enterprise risk report. The tiered mandate (Table 1, rightmost column) takes into account that a blanket mandate would be inappropriate: the banks need the SAMA level of prescriptiveness; the publicly held companies need the CMA level of accountability with COSO-style practices; while public organizations and giga projects need process discipline based on ISO under the national purpose layer.

Theoretical Contribution

This study has three theoretical implications. First, the paper adds to the body of knowledge concerning international ERM by examining a non-western, resource-endowed, and institutionally influenced country, addressing the call to conduct ERM research within the context (Bromiley *et al.*, 2015; Mikes & Kaplan, 2015). The example from Saudi Arabia demonstrates that frameworks for ERM are not institutionally neutral in nature since their effectiveness is contingent on the nature of ownership structures, regulatory power, and national strategic purpose. Secondly, the paper draws a connection between ERM theories and national development strategy by introducing the concept of purpose layer which implies the anchoring of enterprise risk appetite in national purposes. It expands agency and stakeholder theories of ERM (Bhimani, 2009; Amico, 2014) by introducing the state as a stakeholder whose strategic goals limit enterprise risk taking. Thirdly, the paper introduces an analysis template for fragmented risk-regulation architecture through comparing four frameworks (COSO, ISO 31000, SAMA, and CMA).

Practical Contribution: Implementation Roadmap

The practical contribution consists of a staged road map for Saudi organizations to adopt the integrated framework. The road map is the proposed recommendation by the author based on the evidence collected in Sections 2 and 4 in five stages aligned with the maturity level of the organization.

Stage 1 (diagnosis and commitment, months 1-3): the board approves the adoption of the integrated framework; a gap analysis evaluates the current risk management practices with respect to the five COSO components and the ISO process steps and identifies the corresponding regulations of SAMA and CMA. Stage 2 (governance structure, months 4-6): the board establishes a risk committee with well-defined responsibilities and appoints a chief risk officer who reports directly to the board along with aligning the mandates of the audit and risk committees—as per evidence from literature (Al-Hadi *et al.*, 2016; Algrady *et al.*, 2025). Stage 3 (alignment of risk appetite with strategy, months 7-9): management prepares a risk appetite statement in both financial and non-financial terms with reference to the regulatory capital and in alignment with Vision 2030 objectives and the board approves it.

Phase 4 (process implementation and reporting, months 10-18): the ISO 31000 process gets implemented throughout business units; a comprehensive risk report is developed to comply with SAMA Pillar 3, CMA governance disclosure, and internal board reporting using one source of information. Phase 5 (evaluation and institutionalization, months 19-24): the board conducts annual assessment of ERM effectiveness by means of the COSO review and revision element, and the internal audit verifies ERM implementation to make ERM capability out of a project (Beasley *et al.*, 2015; Florio & Leoni, 2017). For banks, the ERM roadmap becomes an integral part of the ICAAP cycle; for listed firms, it becomes an integral part of the CMA governance cycle; and for public organizations, it becomes an integral part of the Vision 2030 delivery cycle.

CONCLUSION

This review examined integrating COSO ERM (2017), ISO 31000:2018, SAMA, and CMA requirements in Saudi Arabia. Evidence indicates fragmented risk

governance: although the frameworks complement one another, differing language, horizons, and mandates can cause duplication and weaken links between enterprise risks and Vision 2030. The proposed model layers ISO's risk process within COSO's governance and strategy components, applies SAMA and CMA requirements by sector, and links risk appetite to national priorities. It remains empirically unvalidated.

SAMA and CMA should develop a shared risk taxonomy and reporting format and strengthen ERM disclosure for listed nonfinancial firms. Boards should treat risk committees as strategic bodies, give the chief risk officer direct board access, set measurable risk appetite linked to capital and strategy, and review ERM effectiveness annually. Public organizations, sovereign wealth funds, and giga-projects should adopt ISO 31000, establish board-level oversight, and improve comparable disclosures. Researchers should test the model across GCC sectors and examine ERM maturity, implementation costs, ownership, Shariah governance, and disclosure.

The review is limited by its qualitative design, English-language scope, and 2017–2025 search window; the framework remains untested. Future research should validate its comparison dimensions, assess pilot implementation costs, and study digitalization and artificial intelligence in risk identification and reporting. The priority is not only adopting ERM but building governance capacity to use risk information in decisions and align enterprise resilience with Saudi Arabia's development goals.

REFERENCES

Al-Dubai, S. A. A., & Abdelhalim, A. M. M. (2021). The relationship between risk disclosure and firm performance: Empirical evidence from Saudi Arabia. *Journal of Accounting, Finance, Economics and Business, 8*(2).

Algrady, S. M., Huang, R., & Al-Matari, E. M. (2025). How do audit committee characteristics affect the quality of financial information? Evidence from Saudi Arabia and United Arab Emirates companies. *SAGE Open, 15*(2). https://doi.org/10.1177/21582440251317803

Al-Hadi, A., & colleagues. (2019). *Risk management in GCC banks.* [Bibliographic details to be verified by the author against the original publication.]

Al-Hadi, A., Hasan, M. M., & Habib, A. (2016). Risk committee, firm life cycle, and market risk disclosures. *Corporate Governance: An International Review, 24*(2), 145–170.

Alhamami, M., & Alruwaili, W. S. (2025). Investigating the role of governance, risk, and compliance (GRC) in investment outcomes through digital transformation in Saudi context. *European Journal of Sustainable Development, 14*(2).

Al-Matari, E. M. (2022). Do corporate governance and top management team diversity have a financial impact among financial sector? A further analysis. *Cogent Business & Management, 9*(1), Article 2141093. https://doi.org/10.1080/23311975.2022.2141093

Al-Matari, E. M. (2025). Do corporate environmental sustainability affect corporate performance? The role of board diversity: Evidence from Saudi Arabia stock market. *Contaduría y Administración, 70*(3), Article e507.

Al-Matari, Y. A., & Fadzil, F. H. (2011). Corporate governance (board of directors and audit committee characteristics) and firm performance. *Global Business and Management Research, 3*(3), 63–75.

Almodawi, A. (2024). I*mpact of the audit committee's characteristics on enterprise risk management, internal audit, external audit and firm performance in Saudi Arabia* [Doctoral dissertation, RMIT University]. RMIT Research Repository.

Alqarni, A. A. M. (2021). *The impact of corporate governance on major shareholdings: The case of Saudi Arabia* [Doctoral dissertation, Newcastle University].

Alsaadi, M. A., Tijjani, B., & Falgi, K. I. (2021). *Corporate governance and quality of financial reporting of listed firms: Evidence from Saudi Arabia.* Corporate Governance: The International Journal of Business in Society.

Al-Tayan, R. (2022). *Empirical analysis of enterprise risk management in Middle East countries* [Doctoral dissertation, Loughborough University]. Loughborough University Repository.

Al-Yahyaee, K., & Al-Hadi, A. (2016). Ineffective corporate governance: Busyness of internal board monitoring committees. *Corporate Ownership and Control, 14*(1), 130–143.

Al-Zaimoor, N., & Desoky, A. (2024). The impact of audit committee features on firm performance—Empirical evidence from GCC countries. *Polish Journal of Management Studies, 30(*1).

Alzeban, A., & Gwilliam, D. (2014). Factors affecting the internal audit effectiveness: A survey of the Saudi public sector. *International Journal of Auditing, 18*(2), 142–157. https://doi.org/10.1111/ijau.12016

Al-Zeer, M., & Al-Saber, S. (2020). *Enterprise risk management practices in Saudi Arabian banks.* [Bibliographic details to be verified by the author against the original publication.]

Amico, A. (2014). *Corporate governance enforcement in the Middle East and North Africa: Evidence and priorities* (OECD Corporate Governance Working Papers No. 15). OECD Publishing. https://doi.org/10.1787/5jxws6scxg7c-en

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society, 35*(7), 659–675.

Basel Committee on Banking Supervision. (2015). *Corporate governance principles for banks. Bank for International Settlements.*

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2015). *Report on the current state of enterprise risk management: Enterprise risk management is not yet the standard of practice.* AICPA & COSO.

Bhimani, A. (2009). Risk management, corporate

governance and management accounting: Emerging interdependencies. *Management Accounting Research, 20*(1), 2–5.

Boshnak, H. A. (2021). Corporate governance mechanisms and firm performance in Saudi Arabia. *International Journal of Financial Research, 12*(3), 107–123.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276.

Capital Market Authority. (2017). *Corporate governance regulations*. https://cma.gov.sa/en/RulesRegulations/Regulations/Pages/details.aspx?code=2

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management—Integrated framework*. AICPA.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. https://www.coso.org

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review, 49*(1), 56–74.

Gjerdrum, D., & Peter, M. (2010). *The new international standard on the practice of risk management—A comparison of ISO 31000:2009 and the COSO ERM framework*. Risk & Insurance Management Society.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301–327.

Grewal, J., Habahbeh, L., Acharyya, M., & Aravind, R. (2022). COVID-19 and the effectiveness of ERM frameworks. *British Actuarial Journal, 27*, Article e8.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance, 78*(4), 795–822.

International Organization for Standardization. (2018). *Risk management—Guidelines (ISO 31000:2018)*. https://www.iso.org/standard/65694.html

Jabbour, M., & Abdel-Kader, M. (2016). ERM adoption in the insurance sector: Is it a regulatory imperative or business value driven? *Qualitative Research in Accounting & Management, 13*(4), 472–510.

Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance, 27*(1), 37–40.

Mrabet, Z., Arouri, H., & Mnasri, A. (2024). *The impact of board characteristics, gender diversity and ESG performance on firm systematic risk: Evidence from GCC countries*. SSRN. https://ssrn.com/abstract=5040813

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance, 18*(4), 8–20.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6–7), 849–855.

Saudi Central Bank. (2023a). *Financial stability report 2023*. https://www.sama.gov.sa/en-US/Publications/FinanceReports/pages/financialstability.aspx

Saudi Central Bank. (2023b). *Risk management guidelines for banks*. SAMA Rulebook. https://rulebook.sama.gov.sa/en/risk-management

Saudi Central Bank. (2024). *Annual report 2023*. https://www.sama.gov.sa/en-US/Publications/EconomicReports/pages/annualreport.aspx

Shatnawi, S. A., & Eldaia, D. M. (2020). *The factors influencing the enterprise risk management practices and firm performance in Jordan and Malaysia*. SSRN. https://ssrn.com/abstract=3568299

Tawfik, O. I., Alsmady, A. A., Rahman, R. A., & Alsayegh, M. F. (2022). Corporate governance mechanisms, royal family ownership and corporate performance: Evidence in Gulf Cooperation Council (GCC) market. *Heliyon, 8*(12), Article e12624.

Vision 2030. (n.d.). *Financial Sector Development Program*. Retrieved March 15, 2026, from https://www.vision2030.gov.sa/en/explore/programs/financial-sector-development-program

Vision 2030. (2016). *Saudi Vision 2030*. https://www.vision2030.gov.sa

Appendix A: Search Strategy

Databases searched: Google Scholar; Scopus; Web of Science; ProQuest (ABI/INFORM and Dissertations & Theses); SSRN. Search period: 2017–2025 (supplemented by snowballed seminal works published before 2017). Language filters: English (with the exception of official Arabic-language documents of SAMA and the CMA).

Principal search strings (adapted to each database): "enterprise risk management Saudi Arabia"; "COSO ERM"; "ISO 31000"; "SAMA risk management"; "CMA corporate governance"; "ERM firm performance GCC"; "risk committee Saudi Arabia"; "risk disclosure Saudi listed companies"; "Vision 2030 financial sector risk."

Boolean operators (AND/OR) combined concept blocks: (enterprise risk management OR ERM OR risk governance) AND (Saudi Arabia OR GCC OR Gulf) AND (COSO OR ISO 31000 OR SAMA OR CMA OR Basel).

Supplemental sources: reference lists of retained studies (backward snowballing); citations of retained studies (forward snowballing); official websites of SAMA, the CMA, the ISO, and COSO for primary framework and regulatory texts.

Appendix B: Coding Framework

Documents were coded along five dimensions derived from the COSO (2017) and ISO 31000:2018 architectures and from prior review frameworks: (a) governance anchor—board oversight, risk committee existence and charter, chief risk officer role, audit committee interface; (b) risk process—identification, assessment (likelihood/impact, qualitative and quantitative), treatment (avoid, accept, reduce, share), monitoring and review, escalation; (c) strategy and appetite—risk appetite statement, tolerance limits, linkage to strategy formulation and capital planning; (d) reporting and disclosure—internal risk reporting, external disclosure (annual report, Pillar 3, governance report), data governance; (e) institutional context—ownership structure, regulator(s) applicable, sector, Shariah governance, Vision 2030 relevance.

Coding was performed by the author against the primary source documents; ambiguous assignments were resolved by reference to the framework documents (COSO, 2017; ISO, 2018).

Appendix C: Document Screening Log

Records identified through database searching: 212. Records after duplicate removal: 116. Records excluded at title/abstract screening (out of scope, non-ERM): 71. Full-text documents reviewed: 45 (the review corpus; all met the inclusion criteria). Composition of the review corpus: 42 scholarly studies and dissertations; 3 official Saudi regulatory documents (SAMA, 2023a, 2023b; CMA, 2017). Primary anchor documents retrieved directly from official sources for the framework comparison: 7 (COSO, 2017; ISO, 2018; Basel Committee, 2015; Vision 2030, 2016 and n.d.; SAMA, 2024; Page *et al.*, 2021). Total distinct documents informing the analysis: 52.