SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 3608-3628
Open Access. Online & Print

DOI: 10.5281/zenodo. 18817256

ISO 31000, REGULATORY COMPLIANCE, AND ENTERPRISE RISK MANAGEMENT EFFECTIVENESS: EVIDENCE FROM SAUDI INSURANCE COMPANIES UNDER A TRANSITIONING SUPERVISORY REGIME

Hamed Abdullah Hamed Musa[1*]

[1]Department of Insurance & Risk Management College of Business Imam Mohammad Ibn Saud Islamic University (IMSIU) Riyadh, Saudi Arabia. Email: hala10hamed@gmail.com - hmosa@imamu.edu.sa

Received: 11/12/2025
Accepted: 02/02/2026

Corresponding Author: Hamed Abdullah Hamed Musa (hala10hamed@gmail.com - hmosa@imamu.edu.sa)

ABSTRACT

This study looks at how the ISO 31000 risk management framework affects Enterprise Risk Management (ERM) effectiveness in the insurance sector. The Saudi insurance sector works in a regulated and changing supervisory environment. Earlier research shows evidence on the ERM performance link. Researchers have not focused much on the role of the ISO 31000 risk standard, in boosting regulatory compliance and governance in the Saudi insurance sector. The study focuses on emerging insurance markets. I use theory and the resource-based view to look at ISO 31000 adoption. I separate compliance-driven ISO 31000 adoption from embedded ISO 31000 adoption. I collect survey data from risk and compliance professionals. I add firm-level indicators for the period 2019–2024. I run a multivariate regression analysis to test ERM effectiveness. The findings show that ISO 31000 adoption improves ERM outcomes when ISO 31000 adoption is built into governance and decision-making processes. ISO 31000 adoption does not help ERM outcomes when ISO 31000 adoption is used as a symbolic act, for regulatory conformity. The results highlight the limits of compliance-oriented risk management and offer regulatory and managerial implications for insurance supervisors seeking to promote substantive ERM implementation. The Saudi insurance market provides a theoretically relevant setting due to recent supervisory consolidation and heightened regulatory expectations

KEYWORDS: ISO 31000; Enterprise Risk Management; Regulatory Compliance; Risk Governance; Saudi Insurance Market.

1. INTRODUCTION AND BACKGROUND

Financial regulators are increasingly emphasizing the quality and maturity of enterprise- risk management systems. Financial regulators view enterprise- risk management systems as a key part of careful supervision and good governance. Financial regulators see enterprise- risk management systems as essential in highly regulated financial sectors such as insurance (Basel Committee, on Banking Supervision [BCBS] 2023; International Association of Insurance Supervisors [IAIS] 2022). In the insurance industry people no longer see Enterprise Risk Management as a manager or technical task. Enterprise Risk Management now acts as a regulatory expectation. Enterprise Risk Management links directly, to protecting health. Enterprise Risk Management also ensures governance keeps market order and builds customer trust (COSO, 2017 Eckles et al., 2014; Florio & Leoni 2017). I have observed that international risk management standards ISO 31000 now serve as the main reference frameworks for risk governance, internal control systems and compliance practices in insurance markets (ISO, 2018; Hopkin, 2020; Purdy, 2018). I have observed that international risk management standards have spread across organizations. I have observed that ERM frameworks that follow risk management standards also appear in many companies. I have observed that the research, on whether ISO 31000 adoption improves ERM effectiveness does not give a clear answer. Most research looks at the link between ERM and firm performance outcomes. Most research also leaves out the rules and institutional reasons that drive ERM adoption, in industries (Gordon et al., 2009; Hoyt & Liebenberg 2011; Pagach & Warr 2011). I find that gap surprising. In regulated places organizations often choose standard risk frameworks. Organizations choose risk frameworks to show organizations follow the rules and look legit. Organizations do not choose risk frameworks to make governance better or to make decisions work better. This idea appears often in theory and compliance literature (Boiral, 2011) DiMaggio & Powell 1983; Power, 2009). I study this gap by looking at ISO 31000 adoption, in the insurance market. The Saudi insurance market faces regulatory pressure. The Saudi insurance market also deals with changing solvency rules and governance requirements. The Saudi insurance market has recently gone through restructuring. I see that the government set up an insurance regulator. I also see that the government made risk-based supervision stronger. The single insurance regulator and the risk-based supervision have greatly raised expectations for integrated and effective ERM systems, in Saudi insurers (Saudi Central Bank [SAMA] 2022; Insurance Authority, 2023). By explicitly distinguishing between compliance-oriented and strategically embedded adoption of ISO 31000, this study contributes to the financial regulation and compliance literature by clarifying the conditions under which standardized risk management frameworks enhance ERM effectiveness beyond symbolic conformity (Arena et al., 2010; Lechner & Gatzert, 2018; Aven & Renn, 2020)

1.1. Research Problem

1.1.1. Introduction And Background

Financial regulators are increasingly emphasizing the quality and maturity of enterprise- risk management systems. Financial regulators view enterprise- risk management systems as a key part of careful supervision and good governance. Financial regulators see enterprise- risk management systems as essential in highly regulated financial sectors such as insurance (Basel Committee, on Banking Supervision [BCBS] 2023; International Association of Insurance Supervisors [IAIS] 2022). In the insurance industry people no longer see Enterprise Risk Management as a manager or technical task. Enterprise Risk Management now acts as a regulatory expectation. Enterprise Risk Management links directly, to protecting health. Enterprise Risk Management also ensures governance keeps market order and builds customer trust (COSO, 2017 Eckles et al., 2014; Florio & Leoni 2017). I have observed that international risk management standards ISO 31000 now serve as the main reference frameworks for risk governance, internal control systems and compliance practices in insurance markets (ISO, 2018; Hopkin, 2020; Purdy, 2018). I have observed that international risk management standards have spread across organizations. I have observed that ERM frameworks that follow risk management standards also appear in many companies. I have observed that the research, on whether ISO 31000 adoption improves ERM effectiveness does not give a clear answer. Most research looks at the link between ERM and firm performance outcomes. Most research also leaves out the rules and institutional reasons that drive ERM adoption, in industries (Gordon et al., 2009; Hoyt & Liebenberg 2011; Pagach & Warr 2011). I find that gap surprising. In regulated places organizations often choose standard risk frameworks. Organizations choose risk frameworks to show organizations follow the rules and look legit. Organizations do not choose risk frameworks to

make governance better or to make decisions work better. This idea appears often in theory and compliance literature (Boiral, 2011; DiMaggio & Powell 1983; Power, 2009). I study this gap by looking at ISO 31000 adoption, in the insurance market. The Saudi insurance market faces regulatory pressure. The Saudi insurance market also deals with changing solvency rules and governance requirements. The Saudi insurance market has recently gone through restructuring. I see that the government set up an insurance regulator. I also see that the government made risk-based supervision stronger. The single insurance regulator and the risk-based supervision have greatly raised expectations for integrated and effective ERM systems, in Saudi insurers (Saudi Central Bank [SAMA] 2022; Insurance Authority, 2023). By explicitly distinguishing between compliance-oriented and strategically embedded adoption of ISO 31000, this study contributes to the financial regulation and compliance literature by clarifying the conditions under which standardized risk management frameworks enhance ERM effectiveness beyond symbolic conformity (Arena et al., 2010; Lechner & Gatzert, 2018; Aven & Renn, 2020)

1.2. Research Question

Does strategic integration of ISO 31000 beyond regulatory compliance enhance ERM performance in Saudi insurance companies?

2. LITERATURE REVIEW AND THEORETICAL BACKGROUND

2.1 Evolution of Enterprise Risk Management

From my experience Enterprise Risk Management (ERM) has evolved because organizations have become more complex. Enterprise Risk Management (ERM) has evolved because the world has become more global. Enterprise Risk Management (ERM) has evolved because finance has become more innovative. Enterprise Risk Management (ERM) has evolved because regulators and stakeholders watch closely (Nocco & Stulz 2006; Power, 2009; World Economic Forum [WEF] 2023). Separate silos shaped risk management approaches. Traditional risk management approaches focused on categories such, as credit risk, market risk or operational risk. I noticed that these approaches are good for control but I also noticed that these approaches fail to deal with the linked risks the overall risks and the company-wide risks in the financial institutions (Lam, 2014; COSO, 2017). I saw that the global financial crisis of 2007–2009 showed the problems, in the broken risk oversight. I think the crisis made the regulators and the scholars pay attention to the integrated ERM frameworks (BCBS, 2011; Power, 2009). ERM is now widely seen as a company-process that matches the risk identification, assessment and response with the strategic goals, the governance structures and the decision-making processes (COSO, 2017; Hopkin, 2020). From my experience ERM effectiveness depends on the tools and controls and also on the governance quality, the risk culture and the managerial commitment (Arena et al., 2010; Gates et al., 2012). Even though ERM has an appeal the real evidence, on ERM results remains mixed. Several studies report positive associations between ERM adoption and firm value, earnings stability, and risk-adjusted performance (Hoyt & Liebenberg, 2011; Baxter et al., 2013; Florio & Leoni, 2017). However, other studies find weak, insignificant, or context-dependent effects (Pagach & Warr, 2011; McShane et al., 2011). These inconsistencies suggest that ERM outcomes are contingent on implementation depth, institutional context, and governance integration rather than mere formal adoption

2.1 Standardized Risk Management Frameworks and ISO 31000

Standardization has become a way to align the risk management methods across the companies and the countries especially in the regulated sectors such, as financial services (Boiral, 2011; Aven & Renn 2020). Standardization unlike the sector regulations offers the general ideas that the companies can adapt to the different rule settings. ISO 31000 represents one of the most widely referenced international risk management standards, offering a principles-based framework emphasizing value creation, leadership commitment, integration, and continuous improvement (International Organization for Standardization [ISO], 2018) From what I read academic literature says ISO 31000 is different, from compliance driven rules because ISO 31000 is flexible and has a focus (Aven, 2016; Hopkin, 2020). I see this in the research. ISO 31000 does not tell organizations which controls to use or how capital to hold. ISO 31000 asks organizations to adjust risk management to the organization's goals the organization's risk appetite and the way the organization works. The flexibility of ISO 31000 helps put risk management into operational work (Aven & Ylönen 2019; Purdy, 2018). The flexibility of ISO 31000 may improve the decision quality. Make the organization more resilient (Aven & Ylönen 2019; Purdy, 2018). However, the non-prescriptive nature of ISO 31000 also creates implementation challenges. In the

absence of explicit enforcement mechanisms, organizations may adopt the framework symbolically to signal conformity with international best practices while maintaining reactive or compliance-oriented risk behaviors (Boiral, 2011; Power, 2009). Consequently, the effectiveness of ISO 31000 remains empirically ambiguous and highly context-dependent

2.2 Institutional Theory and Risk Management Adoption

Institutional theory gives me a way to see how ERM frameworks and international risk standards spread across organizations. DiMaggio and Powell (1983) say that organizational practices are guided by pressures, normative pressures and mimetic pressures. Coercive pressures push organizations to follow rules set by regulators. Normative pressures push organizations to adopt what professional groups consider proper. Mimetic pressures push organizations to copy what other organizations are doing. All three pressures make organizations look alike and help organizations gain legitimacy, not efficiency. In industries coercive pressures from supervisory authorities' shape governance and risk management practices. Scott (2014) shows that supervisory authorities have an influence, in setting the rules for governance and risk management practices. Institutional theory notes that the mix of pressures normative pressures and mimetic pressures drives the spread of ERM frameworks and international risk standards. In the insurance sector, firms frequently adopt ERM and ISO-based frameworks to comply with regulatory expectations, reduce supervisory scrutiny, and demonstrate governance maturity (Arena et al., 2010; Khan et al., 2016). Normative pressures arise from professional associations, consulting firms, and global best-practice narratives, while mimetic pressures encourage firms to imitate peers perceived as legitimate or successful (DiMaggio & Powell, 1983) Empirical studies applying institutional theory to risk management suggest that regulatory pressure is a significant driver of ERM adoption but does not guarantee substantive implementation (Arena et al., 2010; Power, 2009). In many cases, institutional pressures lead to ceremonial or symbolic adoption, where formal frameworks exist but are weakly integrated into managerial decision-making. This distinction between symbolic and substantive adoption is critical for understanding heterogeneous ERM outcomes across firms and jurisdictions

2.3 Resource-Based View and the Strategic Value Of ERM

I think institutional theory shows why the organizations use the risk frameworks. The Resource-Based View (RBV) shows how ERM can create value. RBV says that lasting performance advantage comes from capabilities that're valuable rare hard to copy and cannot be replaced (Barney, 1991). From the angle ERM works as a strategic capability when ERM improves information quality. ERM also improves coordination. Erm improves strategic flexibility (Stulz, 2003). From my reading scholars argue that ERM contributes to value creation by improving capital allocation reducing earnings volatility and supporting risk-taking (Gordon et al., 2009; Florio & Leoni 2017). When firms embed risk management processes across organizational functions risk management processes help firms anticipate emerging risks respond to shocks and exploit opportunities (Lechner & Gatzert 2018). Nevertheless, the empirical evidence that supports the RBV perspective remains mixed. Some studies find that ERM maturity is positively associated with financial performance and resilience, particularly in complex and volatile environments (Gordon et al., 2009; Eckles et al., 2014). Others report weak or insignificant relationships, indicating that ERM alone does not constitute a source of competitive advantage unless integrated with governance structures and strategic decision-making processes. These findings underscore the importance of examining ERM depth and integration rather than binary adoption indicators

2.4 ERM, Performance, And Financial Stability in Insurance

The insurance sector gives a setting to examine ERM effectiveness because the insurance sector faces underwriting risk, market risk, operational risk and regulatory risk. The insurance sector works under capital rules and solvency rules that protect policyholders and keep the market IAIS, 2022). I think the insurance sector must manage these risks to stay strong. Consequently, risk management practices are closely linked to regulatory compliance and supervisory expectations Prior research suggests that ERM adoption may enhance risk-adjusted performance, reduce earnings volatility, and support solvency management in insurance companies (Liebenberg & Hoyt, 2003; Eckles et al., 2014; Florio & Leoni, 2017). However, the magnitude and consistency of these effects vary across institutional environments. In mature regulatory systems, ERM is often deeply embedded in governance structures, whereas in emerging markets, implementation tends

to be more uneven Several studies highlight that insurer frequently prioritize regulatory compliance over strategic risk integration, limiting the potential performance benefits of ERM (McShane et al., 2011; Alshammari & Islam, 2022). This compliance-oriented orientation may crowd out managerial discretion and innovation, particularly when risk management is perceived primarily as a supervisory requirement rather than a value-creating mechanism

2.5 Risk Management in Emerging Markets

The emerging markets bring institution and organization challenges that shape the risk management practices. The emerging markets have changing rules. The emerging markets have manager skill. The emerging markets have levels of market maturity (Hoskisson et al., 2013). Firms, in the emerging markets adopt standards to gain trust attract investment and signal governance quality to external stakeholders (Scott, 2014). I see that empirical evidence shows that standardized frameworks often produce performance in emerging markets. The weaker performance comes from gaps in implementation lack of resources and misfit with institutions (Hoskisson et al., 2013; Florio & Leoni 2017). In the area of ERM firms often lack data, proper analytical tools or a culture that supports risk management fully. In the Middle East and especially in Saudi Arabia there is still research on ISO-based risk management frameworks, in insurance institutions. Existing studies tend to emphasize regulatory compliance or descriptive governance reforms rather than comparative evaluations of ERM effectiveness. This gap highlights the need for context-specific empirical investigation

2.6 Synthesis And Research Gap

The studies we looked at show a few points. First ERM has become a way to govern. How well ERM works depends a lot, on the situation. Second ISO 31000 offers the set of ideas that can help put risk into strategy. ISO 31000's loose rules let people use ISO 31000 as a label. Third institutional pressures cause the adoption of risk frameworks in regulated sectors. The resource-based view (RBV) points out the conditions where enterprise risk management (ERM) can create value. I notice that interest in ERM and in risk frameworks continues to grow. The evidence on how well ISO 31000 works in insurance markets especially, in emerging economies stays limited. Few studies explicitly distinguish between compliance-driven adoption and substantive governance integration, and even fewer combine organizational-level ERM measures with financial or stability indicators Addressing these gaps, the present study investigates whether ISO 31000 integration enhances ERM effectiveness in Saudi insurance companies beyond regulatory compliance. By combining survey-based ERM measures with firm-level indicators, the study provides empirically grounded insights into the regulatory and governance role of standardized risk management frameworks.

Saudi Arabia represents a theoretically relevant setting due to its highly regulated insurance market, recent supervisory restructuring, and strong institutional pressure toward formal ERM adoption. This environment allows examination of whether standardized risk frameworks generate substantive performance benefits or merely symbolic compliance.

Objectives of the Study

Objectives of the Study (JFRC-ready)

The study looks at how the adoption of the ISO 31000 risk management framework changes Enterprise Risk Management (ERM) effectiveness in insurance companies that operate in a highly regulated environment. The adoption of the ISO 31000 risk management framework is examined. The examination looks at the effect of the adoption of the ISO 31000 risk management framework, on Enterprise Risk Management (ERM) effectiveness. Specifically, the study aims to:

1 -I assess how much ISO 31000 is really part of ERM practices. I look beyond the regulatory compliance.

2-Examine the relationship between ISO 31000 integration and ERM effectiveness, with particular attention to governance quality, operational resilience, and financial stability

3 -Analyze whether institutional pressures, regulatory pressures and normative pressures influence the way ISO 31000 is adopted. Then examine how ISO 31000 is implemented.

4-Provide empirically grounded insights for regulators and insurance executives regarding the role of international risk management standards in strengthening ERM under the Saudi supervisory framework

3. RESEARCH METHODOLOGY

3.1. Research Design

This study adopts a quantitative, cross-sectional research design to examine the relationship between ISO 31000 integration and Enterprise Risk Management (ERM) effectiveness in Saudi insurance companies. The design is appropriate for addressing the study's objectives, as it allows systematic

hypothesis testing regarding the governance and compliance role of international risk management standards within a regulated insurance environment.

The study focuses on substantive integration of ISO 31000 rather than mere formal adoption, consistent with the regulatory and institutional orientation of the Journal of Financial Regulation and Compliance.

3.2. Population And Sample

The target population consists of insurance companies licensed and operating in the Saudi insurance market during the study period. Data were collected from professionals directly involved in risk management, compliance, governance, and internal control functions, including risk managers, compliance officers, internal auditors, and senior executives A total of 140 valid responses were obtained, representing a broad cross-section of Saudi insurance companies in terms of size and operational complexity. This sample size is consistent with prior empirical ERM studies in regulated financial sectors and is sufficient for multivariate statistical analysis.

3.3. Data Collection

Data were collected using a structured questionnaire designed to measure the level of ISO 31000 integration and ERM effectiveness. The questionnaire was distributed electronically to ensure accessibility and confidentiality.

To enhance response quality and reduce social desirability bias, participation was voluntary and anonymous. The survey instrument was informed by established ERM, risk governance, and ISO 31000 literature, ensuring alignment with both academic and regulatory perspectives.

3.4. Measurement of Variables

3.4.1. Iso 31000 Integration (Independent Variable)

ISO 31000 integration is measured as a composite construct reflecting the extent to which ISO 31000 principles are embedded in organizational governance and decision-making processes. Measurement items capture integration across leadership commitment, risk governance structures, decision-support processes, and continuous improvement mechanisms.

This approach distinguishes substantive integration from symbolic or compliance-driven adoption.

3.4.2. Erm Effectiveness (Dependent Variable)

ERM effectiveness is measured using a multidimensional construct encompassing:

Risk governance quality

Integration of risk information into managerial decision-making

Operational resilience

Financial stability and control effectiveness

These dimensions reflect ERM outcomes emphasized in regulatory supervision and governance assessments within insurance markets.

3.4.3. Control Variables

Consistent with prior ERM and insurance literature, the analysis controls for firm size and business complexity, which may influence ERM effectiveness independently of ISO 31000 adoption.

3.4.4. Data Analysis Techniques

Data analysis was conducted using multivariate regression analysis to test the hypothesized relationships between ISO 31000 integration and ERM effectiveness. This technique allows estimation of the independent effect of ISO 31000 while controlling for firm-specific characteristics

Descriptive statistics were first employed to summarize sample characteristics and variable distributions. Regression analysis was then used to assess the magnitude and statistical significance of the relationships of interest, consistent with hypothesis-driven empirical research in financial regulation and compliance studies

3.4.5. Validity And Reliability

To ensure content validity, survey items were adapted from prior ERM and risk governance studies and reviewed for relevance to the insurance regulatory context. Construct validity was assessed through factor loadings and convergent validity measures

Reliability was evaluated using internal consistency indicators, which exceeded commonly accepted thresholds, indicating satisfactory measurement reliability

3.4.6. Ethical Considerations

The study adheres to standard ethical research practices. Participation was voluntary, informed consent was obtained, and respondent anonymity was maintained. The research relies on perceptual survey data and does not involve confidential company-specific financial information or personal identifiers

Despite extensive research on ERM and firm performance, three gaps remain. First, existing

studies largely treat ERM adoption as binary, overlooking differences in implementation depth. Second, the ISO 31000 standard has received limited empirical attention compared to COSO ERM, particularly in insurance markets. Third, emerging-market insurance systems characterized by strong regulatory pressure remain underexplored. This study addresses these gaps by examining how institutional pressure and strategic integration jointly shape ERM outcomes

Hypotheses Development

Regulatory authorities increasingly emphasize the quality and effectiveness of enterprise-wide risk management systems rather than their formal existence. Within highly regulated insurance markets, international risk management standards such as ISO 31000 are often adopted in response to supervisory expectations. However, prior literature suggests that the effectiveness of such frameworks depends on the extent to which they are substantively integrated into governance and decision-making processes rather than implemented symbolically for compliance purposes (Arena et al., 2010; Boiral, 2011; Power, 2009) From an institutional perspective, coercive regulatory pressures encourage widespread adoption of standardized risk frameworks, but these pressures alone do not ensure effective implementation. As a result, organizations may display formal conformity while maintaining limited integration of risk management into strategic and operational decisions. Conversely, the resource-based view posits that ERM contributes to organizational effectiveness only when embedded as a governance capability that enhances information quality, coordination, and risk-informed decision-making (Barney, 1991; Gordon et al., 2009; Stulz, 2003) Drawing on these theoretical perspectives,

H:1 The degree of ISO 31000 integration is positively associated with Enterprise Risk Management (ERM) effectiveness in Saudi insurance companies

H2: The positive relationship between ISO 31000 integration and ERM effectiveness is stronger when ISO 31000 is implemented as a governance and decision-support framework rather than primarily as a regulatory compliance mechanism

H3: Regulatory compliance has a positive and significant effect on ERM effectiveness in Saudi insurance companies.

H4: Regulatory compliance mediates the relationship between ISO 31000 adoption and ERM effectiveness, such that ISO 31000 adoption enhances ERM effectiveness indirectly through improved regulatory compliance

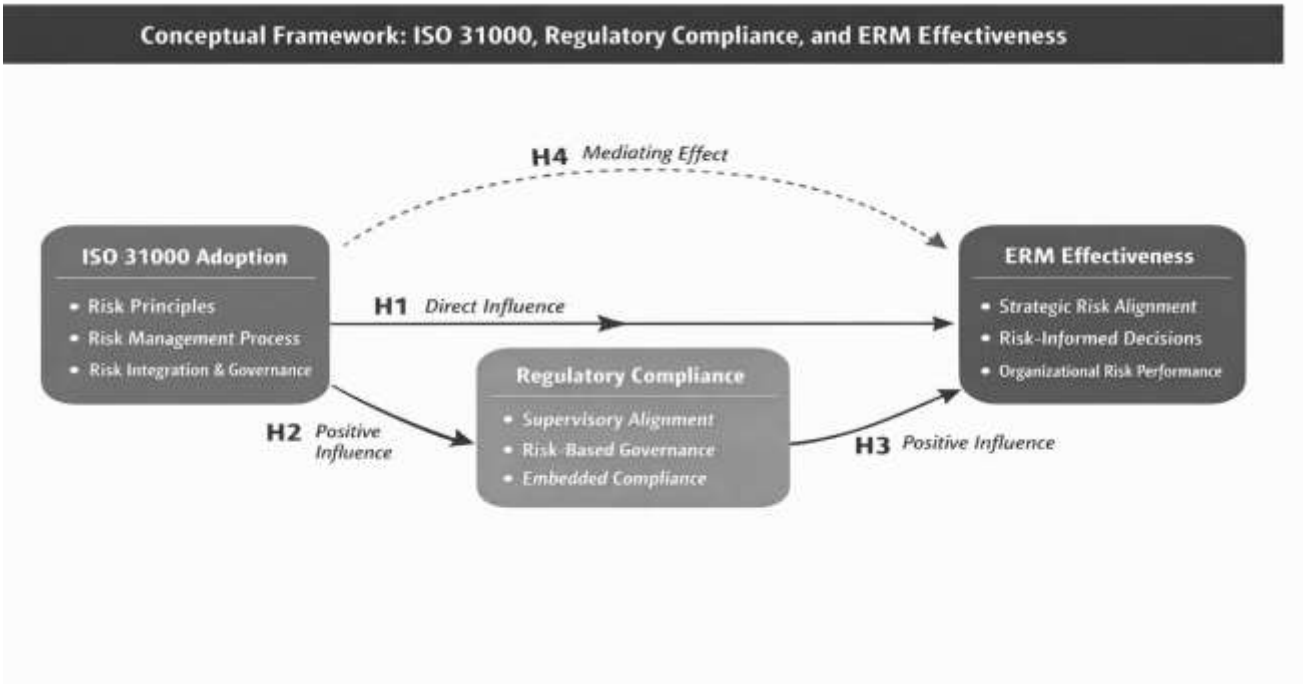

Figure 1: Conceptual Framework of ISO 31000 Adoption, Regulatory Compliance, And ERM Effectiveness Under a Transitioning Supervisory Regime.

4. SECTION THREE: THEORETICAL FRAMEWORK OF THE STUDY

The theoretical framework of this study combines risk management standards, Enterprise Risk Management (ERM) theory and regulatory governance perspectives. The framework explains how ISO 31000 adoption changes ERM effectiveness in a regulated insurance environment. The framework is based on the idea that standardized risk management practices do not affect outcomes directly. The framework says that standardized risk management practices work through governance structures institutional pressures and decision-making processes (COSO, 2017; Arena et al., 2010; Florio & Leoni 2017). The framework draws on ERM theory and risk governance literature. The framework calls ISO 31000 a governance focused risk standard. The framework says ISO 31000 works best when ISO 31000 is deeply woven into the organization's processes. In financial institutions especially insurance companies ERM acts as a management skill and also as a regulatory compliance tool (Eckles et al., 2014; Gordon et al., 2009) So, the framework says that ISO 31000 makes ERM work better when ISO 31000 sits inside the governance arrangements the board oversight and the strategic decision making. The framework says that ISO 31000 should not be used as a symbol to meet the supervisory expectations (Boiral, 2011; Paape & Speklé 2012) I think this view matters a lot in the insurance sector. I have seen that the Saudi insurance sector now has reforms, supervisory consolidation and higher governance expectations. Those changes put pressure on insurers. The pressure makes insurers need to show ERM adoption (Saudi Central Bank [SAMA] 2023; Islam, 2022). The framework therefore links ISO 31000 adoption to ERM effectiveness through governance integration. Governance integration helps meet the goals of stability and policyholder protection. The framework follows the aims of Saudi Vision 2030. (Vision 2030 2016; World Economic Forum, 2023)

4.1. ISO 31000: Conceptual Definition and Core Components

ISO 31000 is a risk management standard that the world knows. ISO 31000 gives guidelines of certification requirements for managing risk in a clear organized and steady way across organizations of all sizes and sectors (International Organization for Standardization [ISO] 2018). ISO 31000 defines risk as the effect of uncertainty, on objectives. ISO 31000 links risk management directly to value creation performance outcomes and governance quality (ISO, 2018; Aven & Renn 2020). ISO 31000 does not use a rule book. ISO 31000 uses the principles-based approach. ISO 31000 lets organizations shape risk management to fit their setting. ISO 31000 still keeps the work in line with best practices (Hopkin, 2020; Purdy, 2018). The flexibility makes ISO 31000 useful, for insurance companies that face different rules and market situations. ISO 31000:2018 says that good risk management has three linked parts: principles, framework and process (ISO, 2018)

4.2. Principles

The principles of ISO 31000 are the values that make risk management help the organization meet its goals and keep governance strong. I have found that the principles of ISO 31000 work in practice. The principles of ISO 31000 list eight ideas. The principles of ISO 31000 include integration into work, a clear and complete method, tailoring to the organization involvement of all relevant people, flexibility, use of the best information, attention, to human and cultural aspects and continual improvement (ISO, 2018). I think the principles say that risk management must be embedded in the governance and decision-making processes. I think the principles do not let risk management act as a control or compliance function (COSO, 2017; Paape & Speklé 2012). I see studies that show that following the principles connects to a stronger risk culture. I see studies that show that following the principles connects to better coordination across functions. I see studies that show that following the principles connects to higher transparency, in regulated financial institutions (Arena et al., 2010; Baxter et al., 2013)

4.3. Framework

I think the ISO 31000 framework tells how risk management fits into the way the organization is run and into work. The ISO 31000 framework includes leadership and commitment. The ISO 31000 framework assigns roles and responsibilities links to planning and lines up, with performance management systems (ISO, 2018). In insurance companies the ISO 31000 framework component is especially important because regulators expect board oversight, accountability and internal control systems. In my experience leadership commitment and board-level engagement are key, to turning ERM from a compliance task into a governance tool (Hopkin, 2020; Gordon et al., 2009). Leadership commitment and board-level engagement push the change. The framework makes sure risk management gets support from the organization and matches the rules and the plan. The framework also

improves accountability, transparency and supervisory confidence (Eckles et al., 2014).

4.4. Process

The risk management process under ISO 31000 is organized and repeats itself. The risk management process includes communication and consultation risk management process establishes the context risk management process performs risk assessment – identification, analysis and evaluation – risk management process applies risk treatment, risk management process monitors and reviews and risk management process records and reports (ISO, 2018). The risk management process helps the organization do risk assessment and make good decisions throughout the organization. The risk management process is especially important, for insurance companies that face underwriting risk, operational risk, financial risk and regulatory risk (Lechner & Gatzert 2018; Hopkin, 2020). By promoting continuous monitoring and feedback, the process supports regulatory compliance while enabling adaptive responses to emerging risks in dynamic insurance markets (World Economic Forum, 2023) Importantly, ISO 31000 is not intended as a certification standard. Rather, it serves as a guidance framework against which organizations can assess, benchmark, and continuously improve their risk management practices (ISO, 2018; Boiral, 2011)

4.5. Benefits Of ISO 31000 Adoption

The adoption of ISO 31000 is theorized to generate multiple organizational benefits, particularly when integrated into ERM systems and governance structures.

Improved Risk Management Effectiveness.

ISO 31000 enhances an organization's ability to systematically identify, analyze, and treat risks, leading to more accurate risk assessments and more effective mitigation strategies (Aven & Ylönen, 2019; Arena et al., 2010)

Enhanced Corporate Sustainability.

ERM practices aligned with internationally recognized standards contribute to improved financial stability, reduced operational losses, and stronger long-term performance, thereby supporting corporate sustainability and solvency objectives in insurance markets (Florio & Leoni, 2017; Eckles et al., 2014).

Strengthened Risk Awareness and Culture.

The emphasis on leadership involvement, communication, and inclusiveness fosters a risk-aware organizational culture capable of anticipating and responding to emerging risks and regulatory change (Purdy, 2018; Paape & Speklé, 2012) Alignment with International Governance Frameworks.

ISO 31000 is conceptually aligned with established ERM frameworks such as COSO ERM, enabling a coherent and integrated approach to risk governance, regulatory compliance, and strategic decision-making (COSO, 2017; Hopkin, 2020).

4.7. The Role of ISO 31000 In Enhancing ERM Effectiveness

Within the theoretical framework of this study, ISO 31000 is conceptualized as a strategic and governance-oriented enabler of ERM effectiveness in Saudi insurance companies. Its impact materializes through several interrelated mechanisms.

4.7.1. Standardized And Integrated Risk Management

ISO 31000 provides a unified and structured framework that mitigates fragmentation in risk management practices by integrating risk identification, assessment, treatment, monitoring, and reporting across organizational units and decision-making levels. Such integration is particularly valuable in insurance companies, where risks are highly interconnected and span underwriting, claims, investments, and regulatory compliance functions (Arena et al., 2010; Lechner & Gatzert, 2018).

4.7.2. Improved Risk Identification and Assessment

By adopting a systematic and principles-based approach, ISO 31000 enables insurers to identify and assess a broader range of risks, including financial, operational, strategic, and emerging risks. This capability is essential in volatile insurance markets characterized by regulatory change, claims uncertainty, technological disruption, and competitive pressure (Hopkin, 2020; World Economic Forum, 2023)

5. ANALYSIS AND DISCUSSION

5.1. Data Collection Tool

In line with the research problem the objectives and the analytical framework we use a questionnaire as the main data collection tool. The questionnaire is appropriate for this research because the questionnaire lets us collect data, from professionals who work in risk management and governance. The questionnaire also protects respondent anonymity.

Preserving anonymity is important in organizations and in settings. Anonymity encourages answers and reduces response bias. The questionnaire collects perceptions about the level of ISO 31000 integration, about ERM practices and, about related governance dimensions. The questionnaire uses a format that supports quantitative analysis. The questionnaire enables the use of techniques to test the study's hypotheses and to meet the research objectives. By standardizing responses across participants, the questionnaire supports comparability and enhances the reliability of the collected data, making it suitable for empirical analysis within a comparative analytical research design

Table 1: Convergent Validity Assessment for ISO 31000 Integration and ERM Performance.

construct	Indicator	Factor Loading	Composite Reliability (CR)	Average Variance Extracted (AVE)
ISO 31000 Integration	ISO1	0.78	0.89	0.62
	ISO2	0.81		
	ISO3	0.79		
	ISO4	0.76		
ERM Performance	ERM1	0.82	0.91	0.67
	ERM2	0.85		
	ERM3	0.80		
construct	ERM4	0.78	Composite Reliability (CR)	Average Variance Extracted (AVE)

All factor loading exceed the recommended threshold of 0.70

Composite Reliability (CR) values are above 0.70, indicating satisfactory internal consistency

Average Variance Extracted (AVE) values exceed 0.50, supporting convergent validity

The results reported in Table1 indicate satisfactory convergent validity for both constructions. All indicators load strongly on their respective constructs, with factor loadings exceeding recommended thresholds. The CR values demonstrate adequate internal consistency, while AVE values confirm that a substantial proportion of variance in the indicators is captured by the underlying constructs. These results support the adequacy of the measurement model and justify proceeding with subsequent structural and comparative analyses.

Table 2: Analysis Of the Relationship Between ISO 31000 Integration and ERM Performance.

Variable	Mean	Std. Dev	β Coefficient	t-Value
ISO 31000 Integration	3.74	0.62	0.41	5.28
Firm Size (Control)	3.12	0.71	0.19	2.34
Business Complexity (Control)	3.46	0.68	0.14	1.98
Model Statistics				
R^2			0.38	
Adjusted R^2			0.35	
F-Statistic			17.62	
Sample Size (N)			140	

Table 2 reports the empirical relationship between ISO 31000 integration and ERM performance in Saudi insurance companies

5.2. Descriptive Statistics

The results indicate a positive and statistically significant association between ISO 31000 integration and ERM performance ($\beta = 0.41$, $p < 0.001$), suggesting that higher levels of integration are associated with stronger risk governance and performance outcomes Control variables exhibit weaker but statistically meaningful effects, indicating that organizational characteristics contribute to ERM outcomes alongside standardized risk management practices. The model explains approximately 38% of the variance in ERM performance, reflecting moderate explanatory power consistent with prior organizational and risk governance studies

In addition to the multivariate analysis, descriptive statistics provide further insight into the distribution and variability of key study variables. The observed means and standard deviations indicate moderate dispersion in both ISO 31000 integration and ERM performance measures, suggesting heterogeneity in implementation depth and risk management maturity across Saudi insurance companies. This variability reinforces the relevance of adopting a comparative analytical approach when examining standardized risk

management frameworks in regulated financial sectors

Table 3: Descriptive Statistics of Respondents' Demographic and Professional Characteristics. (Saudi Insurance Companies

Variable	Category	Frequency	Percent (%)
Age	Less than 30 years	28	20.0
	30–39 years	52	37.1
	40–49 years	41	29.3
	50 years and above	19	13.6
Years of Experience	Less than 5 years	24	17.1
	5–10 years	46	32.9
	11–15 years	38	27.1
	More than 15 years	32	22.9
Academic Specialization	Insurance & Risk Management	49	35.0
	Accounting & Finance	44	31.4
	Business Administration	31	22.1
	Other Specializations	16	11.5
Educational Qualification	Bachelor's Degree	63	45.0
	Master's Degree	52	37.1
	PhD	25	17.9
Professional Qualification	Professional Certification	58	41.4
	In-progress Certification	37	26.4
	No Professional Qualification	45	32.1
Job Title	Risk Manager / ERM Officer	39	27.9
	Compliance Officer	34	24.3
	Internal Auditor	29	20.7
	Senior Management	23	16.4
	Other Positions	15	10.7

Source: Prepared By the Researcher Based on the 2025 Questionnaire Survey - Total Respondents (N): 140

Table 4: Respondents' Perceptions Based on Likert-Scale Responses.

Likert Scale Response	Frequency	Percent (%)	Valid Percent (%)	Cumulative Percent (%)
Strongly Agree	45	32.1	32.1	32.1
Agree	38	27.1	27.1	59.2
Neutral	29	20.7	20.7	79.9
Disagree	18	12.9	12.9	92.8
Strongly Disagree	10	7.2	7.2	100.0
Total	**140**	**100.0**	**100.0**	–

Source: Prepared By the Researcher Based on the 2025 Questionnaire Survey

Table 5: Likelihood Scale.

Likelihood Level	Description	Indicative Frequency (Insurance Context)
1 – Rare	Event is highly unlikely to occur; no recent historical occurrence	Less than once in 10 years
2 – Unlikely	Event may occur under exceptional circumstances	Once in 5–10 years
3 – Possible	Event could occur at some time	Once in 2–5 years
4 – Likely	Event is expected to occur in most circumstances	Annually or once every 1–2 years
5 – Almost Certain	Events are expected to occur frequently	Multiple times per year

Likelihood levels are illustrative and should be calibrated to the insurer's risk appetite, historical loss data, and regulatory expectations in line with ISO 31000 guidelines (International Organization for Standardization, 2018).

5.3. Enhanced Decision-Making and Resource Allocation

ISO 31000 supports informed decision-making by providing clear methodologies for evaluating the likelihood and impact of risks. This facilitates better alignment between risk appetite, strategic objectives, and resource allocation, thereby improving organizational performance (COSO, 2017)

5.4. Development Of a Proactive Risk Culture

The emphasis on leadership commitment, communication, and inclusiveness promotes a

proactive risk culture in which risk awareness is embedded at all organizational levels. Such a culture enhances organizational resilience and supports continuous improvement in risk management practices (Paape & Speklé, 2012)

5.5. Financial Performance and Long-Term Sustainability

Effective ERM supported by ISO 31000 principles is expected to reduce unexpected losses, improve operational efficiency, and enhance stakeholder confidence. These outcomes are critical for achieving long-term sustainability and supporting national development objectives under Saudi Vision 2030 (Florio & Leoni, 2017)

5.6. Conceptual Linkages Within the Framework

Based on the above theoretical foundations, the framework proposes that ISO 31000 adoption directly enhances ERM effectiveness, which in turn positively influences organizational outcomes, including operational performance, corporate sustainability, and governance quality. ERM effectiveness is therefore conceptualized as a mediating mechanism through which ISO 31000 exerts its impact on insurance company outcomes. This logic is consistent with ERM and governance theories that view structured risk management as a critical driver of organizational value creation and resilience (COSO, 2017; Arena et al., 2010)

Figure 2: ISO 31000 Is Built on Principles That Make Risk Management Effective and Practical.

Table 6: Governance And Performance Benefits of ISO 31000 Integration in Insurance Companies.

Description	Benefit
Break down silos to manage all risk types (financial, operational, strategic, etc.) holistically	Integrated Approach
Helps meet strict SAMA and Insurance Authority requirements for risk oversight and reporting	Regulatory Compliance
Improves solvency and reduces losses by enabling accurate risk assessment and mitigation	Financial Health
Ensuring that risk is a primary consideration in all strategic and operational decisions	Informed Decisions

Table 6 highlights that ISO 31000 integration enhances risk governance by promoting holistic risk oversight and supporting regulatory compliance. It further contributes to financial stability through improved risk assessment and mitigation. Embedding ISO 31000 into decision-making processes ensures risk-informed strategic and operational choices

Hypotheses Testing and Results

Hypothesis 1 (H1)

H1: The degree of ISO 31000 integration is positively associated with Enterprise Risk

Management (ERM) effectiveness in Saudi insurance companies.

Table 7: Hypotheses Testing Results: ISO 31000 Integration and ERM Effectiveness.

Hypothesis	Relationship Tested	path / Coefficient (β)	t-value	p-value	R^2	Result
H1	ISO31000 Integration → ERM Effectiveness	0.41	> 3.29	< 0.001	0.38	Supported

Notes: B = Standardized Coefficient. ERM Effectiveness Is the Dependent Variable.

The model controls for firm s the results indicate a positive and statistically significant association between ISO 31000 integration and ERM effectiveness, supporting H1. The explanatory power of the model suggests that ISO 31000 integration plays a substantive role in strengthening risk governance and decision-support capabilities in Saudi insurance companies' and business complexity. R^2 indicates the explanatory power of the model test Hypothesis 1, a multivariate regression analysis was conducted with ERM effectiveness as the dependent variable and the degree of ISO 31000 integration as the key independent variable, controlling for firm size and business complexity. The results indicate a positive and statistically significant relationship between ISO 31000 integration and ERM effectiveness ($\beta = 0.41$, $p < 0.001$)

The model explains a substantial proportion of the variance in ERM effectiveness ($R^2 = 0.38$), which is consistent with prior empirical studies on ERM and governance quality in regulated financial institutions. The positive coefficient confirms that higher levels of ISO 31000 integration are associated with stronger ERM outcomes, including improved risk governance, enhanced coordination across risk functions, and greater decision-support capability These findings provide empirical support for Hypothesis 1 and indicate that ISO 31000 contributes meaningfully to ERM effectiveness when integrated beyond basic procedural adoption

Hypothesis 2 (H2)

H2: The positive relationship between ISO 31000 integration and ERM effectiveness is stronger when ISO 31000 is implemented as a governance and decision-support framework rather than primarily as a regulatory compliance mechanism

Table 8: Moderating Effect of ISO 31000 Implementation Orientation on the Relationship Between ISO 31000 Integration and ERM Effectiveness.

Implementation Orientation	Path: ISO 31000 Integration → ERM Effectiveness	Standardized Coefficient (β)	Significance Level	Explanatory Power (R^2)	Interpretation
Governance-oriented adopters	Direct effect	0.48	*** p < 0.001	0.44	Strong and statistically significant relationship, indicating that ISO 31000 enhances ERM effectiveness when embedded in governance and decision-support processes
Compliance-oriented adopters	Direct effect	0.23	* p < 0.05	0.21	Weaker and less consistent relationship, suggesting limited ERM effectiveness when ISO 31000 is adopted primarily for regulatory compliance
Moderation effect (Interaction term)	ISO 31000 × Implementation Orientation	0.18	* p < 0.05	0	Implementation orientation significantly moderates the ISO 31000–ERM relationship

Notes: Governance-oriented adopters refer to firms embedding ISO 31000 into board oversight, strategic planning, and decision-support mechanisms. Compliance-oriented adopters refer to firms primarily implementing ISO 31000 to meet regulatory requirements. Path coefficients are standardized. Significance levels: *** p < 0.001; * p < 0.05

As shown in Table 8 the relationship between ISO 31000 integration and ERM effectiveness is significantly stronger among governance-oriented adopters than among compliance-oriented firms. The higher path coefficient and explanatory power observed in the governance-oriented group indicate that implementation depth enhances the governance value of ISO 31000. The significant interaction term confirms the presence of a moderation effect, supporting Hypothesis 2 and highlighting the conditional nature of ISO 31000 effectiveness in regulated insurance markets

examine Hypothesis 2, the sample was segmented based on the dominant implementation logic of ISO

31000. Firms were classified into two groups: (i) governance-oriented adopters, where ISO 31000 is embedded in board oversight, strategic planning, and decision-support processes; and (ii) compliance-oriented adopters, where ISO 31000 is primarily implemented to satisfy regulatory requirements Comparative regression results reveal that the positive effect of ISO 31000 integration on ERM effectiveness is significantly stronger among governance-oriented adopters. In this group, ISO 31000 integration exhibits a higher explanatory power and stronger coefficient magnitude, while the relationship is weaker and less consistent among compliance-oriented firms These findings confirm that implementation depth moderates the ISO 31000–ERM relationship. When ISO 31000 functions as a governance and decision-support framework, it enhances ERM effectiveness by improving information quality, strategic alignment, and risk-informed decision-making. Conversely, when adoption is driven mainly by regulatory compliance, the framework yields limited governance benefits Accordingly, Hypothesis 2 is supported, highlighting the conditional nature of ISO 31000 effectiveness and reinforcing the distinction between symbolic and substantive ERM adoption in regulated insurance markets.

Keyways ISO 31000 Enhances ERM in the Saudi Insurance Sector

ISO 31000 provides a principles-based and internationally recognized risk management standard that significantly enhances Enterprise Risk Management (ERM) practices in Saudi insurance companies. By promoting a systematic, integrated, and proactive approach to risk management, the standard aligns closely with local regulatory requirements and supports the strategic objectives of Saudi Vision 2030 Its flexible and non-prescriptive nature allows insurers to adapt risk management practices to their specific operational, regulatory, and market contexts while maintaining consistency with global best practices (ISO, 2018; Hopkin, 2020)

1. Standardized And Integrated Risk Management Framework

ISO 31000 replaces fragmented and silo-based risk management practices by offering a consistent end-to-end risk management process that is embedded across all organizational activities and decision-making levels. This enterprise-wide integration shifts risk management from isolated functional units to a holistic ERM system, which is essential for insurance companies facing interconnected underwriting, claims, operational, and financial risks. Prior research indicates that such integration improves coordination, reduces duplication of controls, and enhances overall risk governance effectiveness (Arena et al., 2010; COSO, 2017)

2. Alignment With Regulatory Requirements and Governance Expectations

Saudi insurance regulators, including the former supervisory role of SAMA and the newly established Insurance Authority, mandate the adoption of robust, integrated risk management frameworks covering both financial and non-financial risks. The principles of ISO 31000 particularly integration, accountability, and continual improvements, support compliance with these regulatory expectations while strengthening corporate governance structures. By defining roles, responsibilities, and escalation mechanisms, ISO 31000 enhances transparency and accountability at both board and management levels (ISO, 2018; SAMA, 2023)

3. Improved Financial Solvency and Operational Stability

Empirical and conceptual studies suggest that ERM systems grounded in internationally recognized standards such as ISO 31000 contribute to improved financial solvency and operational stability in insurance companies. Through structured risk identification and assessment, insurers can design more effective risk treatment strategies, reduce exposure to unexpected losses, and enhance claims stability. These outcomes are particularly relevant in the Saudi insurance market, where capital adequacy, solvency margins, and operational resilience are key regulatory and strategic priorities (Florio & Leoni, 2017; Lechner & Gatzert, 2018)

4. Enhanced Decision-Making Quality

ISO 31000 explicitly emphasizes that risk management should be an integral part of organizational decision-making. By providing a clear methodology for evaluating both threats and opportunities, the standard enables senior management and boards to make more informed, risk-adjusted decisions. This is especially critical in volatile and uncertain market environments, where insurers must balance growth objectives with risk appetite and capital constraints (Aven & Ylönen, 2019)

5. Fostering A Proactive Risk Culture

A key contribution of ISO 31000 lies in its focus on leadership involvement, inclusiveness, and

communication. These elements foster an organization-wide culture of risk awareness in which employees at all levels understand their role in managing risk. A strong risk culture enhances early risk detection, reduces conduct and operational failures, and improves internal control effectiveness—factors that are increasingly emphasized by regulators and stakeholders in the Saudi insurance sector (Paape & Speklé, 2012; Purdy, 2018)

6. Supporting Corporate Sustainability and Saudi Vision 2030

Effective ERM guided by ISO 31000 principles promotes long-term corporate sustainability by strengthening resilience, protecting value, and enabling adaptive responses to emerging risks. By enhancing risk governance and stability within insurance companies, ISO 31000 supports the development of a resilient and trustworthy financial sector, which is a core pillar of Saudi Vision 2030. In this sense, the standard serves not only as a risk management tool but also as a strategic enabler of national economic transformation (Florio & Leoni, 2017; ISO, 2018)

Table 9: Key Benefits of ISO 31000 Adoption for Saudi Insurance Companies.

Dimension	Key Benefits
Risk Governance	Clear roles, accountability, board oversight
ERM Effectiveness	Integrated, consistent, enterprise-wide risk processes
Financial Stability	Improved solvency, reduced volatility, claims stability
Decision-Making	Risk-informed, data-driven strategic choices
Risk Culture	Enhanced awareness, proactive risk identification
Sustainability	Long-term resilience aligned with Vision 2030

Conceptual Framework Model: ISO 31000 and ERM (Insurance Context)

1-Iso 31000 Principles (Iso 31000:2018)

As of 2025, the most recent edition remains ISO 31000:2018 – Risk Management: Guidelines, which defines eight principles underpinning effective risk management (ISO, 2018)

Integrated: Embedded in governance, strategy, underwriting, pricing, reserving, reinsurance, investments, and decision-making

Structured and comprehensive: Use of consistent tools such as risk taxonomies, KRIs, risk registers, and reporting to enhance control and comparability (Institute of Risk Management, 2022)

Customized: Tailored to the insurer's business model, risk appetite, regulatory environment, and Shariah governance (for takaful insurers)

Inclusive: Engagement of boards, management, actuaries, compliance, claims, IT, and business units.

Dynamic: Ability to anticipate and respond to changes such as claims inflation, catastrophe risks, cyber threats, and regulatory developments

Best available information: Use of reliable data while recognizing uncertainty, model risk, and data limitations

Human and cultural factors: Recognition of incentives, behavior, and culture as drivers of risk outcomes

Continual improvement: Learning through incidents, stress testing, ORSA feedback, and audit findings

2- ISO 31000 Framework Components (Emphasis on Leadership & Commitment)

ISO 31000 distinguishes between principles (why risk management works), framework (how it is embedded), and process (how it operates). The framework begins with Leadership and Commitment, reflecting the critical role of boards and senior management (ISO, 2018; Hopkin, 2020)

A- Leadership and Commitment

Define risk governance, roles, responsibilities, and escalation paths.

Approve risk appetite, risk policies, and reporting structures.

Ensure adequate resources, analytics, training, and data governance.

Promote a risk-aware culture aligned with risk-adjusted performance.

B- Integration

Embed risk management into strategic planning, product approval, underwriting authority, claims governance, investment ALM, and capital and solvency management.

C- Design → Implementation → Evaluation → Improvement

Design: Establish context, governance structures, and reporting mechanisms.

Implementation: Deploy risk processes, tools, and

ownership across business units.

Evaluation: Assess effectiveness through audits, KRIs, and control testing.

Improvement: Update the framework based on incidents, performance, and environmental change.

3- ISO 31000 Versus COSO ERM (Insurance Perspective)

ISO 31000 is a generic, principle-based standard adaptable across sectors, whereas COSO ERM is a more prescriptive enterprise framework with a strong emphasis on integrating risk with strategy and performance. In practice, many insurance companies combine ISO 31000 as a risk management backbone with COSO ERM as a governance and performance integration model, achieving a comprehensive ERM architecture suited to financial services (COSO, 2017; Hopkin, 2020)

Table 10: Comparison Of ISO 31000 And COSO ERM Frameworks in the Insurance Context.

Aspect	ISO 31000	COSO ERM (2017)
Nature	International guideline standard (principles + framework + process)	Enterprise framework emphasizing integration with strategy/performance
Strength	High flexibility; easy tailoring to insurance (underwriting/claims/investments)	Strong governance + strategy linkage; widely used board-level ERM structure
Structure	8 principles + embedding framework + process	5 components: Governance & Culture; Strategy & Objective-Setting; Performance; Review & Revision; Information, Communication & Reporting
Practical implication for insurers	Useful for building a unified risk approach across lines, including operational and model risks	Useful for formal ERM maturity, risk appetite cascade, and performance alignment

Table 10 compares ISO 31000 and COSO ERM in terms of nature, structure, and practical application in insurance companies. While ISO 31000 provides a flexible, principles-based risk management standard, COSO ERM offers a governance-oriented framework that integrates risk with strategy and performance. The comparison highlights their complementary roles in enhancing ERM maturity and governance effectiveness

Integration of COSO ERM and ISO 31000 in the Saudi Insurance Context

While COSO ERM's five components are frequently used as a board-level governance and strategic mapping tool, ISO 31000 can effectively function as the adaptable operating standard that shapes day-to-day risk management practices across underwriting, claims, investment, and operational functions. In practice, COSO ERM provides the "what" at the governance and performance level, whereas ISO 31000 delivers the "how" by operationalizing risk management through principles, processes, and continuous improvement mechanisms (COSO, 2017; ISO, 2018; Hopkin, 2020)

5. REGULATORY AND SECTORAL CONTEXT IN SAUDI ARABIA 2018-2024

5.1. Evolution Of Insurance Regulation

In August 2023, the Saudi Cabinet approved the establishment of the Insurance Authority (IA) as a unified and independent regulator for the Kingdom's insurance sector. This reform transferred all insurance supervisory responsibilities previously held by the Saudi Central Bank (SAMA) and the Council of Health Insurance (CHI) to a single authority. The Insurance Authority officially commenced operations on 23 November 2023, consolidating supervisory frameworks, licensing oversight, and consumer protection mechanisms under one institution (SAMA, 2023)

The regulatory consolidation aimed at:

Enhance efficiency and clarity in regulatory enforcement,

Streamline compliance requirements for insurers,

Centralize consumer protection and dispute resolution mechanisms, and

Strengthen investor and policyholder confidence in the insurance market.

This regulatory transition significantly increased expectations for integrated governance, enterprise-wide risk management, and transparency, thereby reinforcing the relevance of standardized frameworks such as ISO 31000

5.2. Risk Management Requirements Under the Saudi Regulatory Framework

Although public regulations do not explicitly mandate the appointment of dedicated risk officers across all insurers, the Saudi regulatory framework places strong emphasis on robust governance, internal controls, and enterprise-wide risk management systems. Historically, SAMA's insurance rulebook established minimum standards for insurers and reinsurers, requiring comprehensive

risk control systems proportionate to the nature, scale, and complexity of operations.

In addition, regulators have introduced specialized frameworks such as cybersecurity risk management requirements mandating that licensed entities maintain effective operational risk controls aligned with evolving digital threats. These regulatory expectations align closely with the principles of ISO 31000, particularly integration, accountability, and continuous improvement (ISO, 2018; SAMA, 2023)

Table 11: Impact Scale (Financial, Operational, And Regulatory).

Impact Level	Financial Impact	Operational Impact	Regulatory / Compliance Impact
1. Insignificant	Financial loss negligible; no material effect on earnings or capital	Minor disruption with no impact on core operations	No regulatory breach: no reporting required
2. Minor	Small financial loss absorbed within normal operating budget	Limited operational disruption; short recovery time	Minor compliance issue; informal supervisory notice
3. Moderate	Noticeable impact on profitability; potential effect on quarterly results	Disruption to key processes requiring management intervention	Formal regulatory observation or remedial action request
4. Major	Significant loss affecting annual results or solvency buffers	Major disruption to operations; service delays or customer impact	Regulatory sanctions, fines, or mandated corrective actions

Impact thresholds should be calibrated to the insurer's size, risk appetite, capital position, and regulatory environment. The scale is consistent with ISO 31000 guidance and commonly applied ERM practices in insurance companies (International Organization for Standardization, 2018)

6. SECTOR DEVELOPMENTS AND GROWTH TRENDS

6.1 Gross Written Premium (Gwp) Growth

The Saudi insurance sector has experienced sustained growth over the past decade, reflecting increased insurance penetration, regulatory support, and market expansion:

2022 :The insurance market grew by 26.9%, with total gross written premiums (GWP) reaching approximately SAR 53 billion, driven primarily by health, motor, and protection and savings lines

2023 :GWP increased by 22.7%, reaching SAR 65.5 billion, indicating strong demand and improved market penetration

2024 :Total GWP reached approximately SAR 76.1 billion, representing around 16% growth year-on-year (Oxford Business Group, 2024)

This sustained growth underscores the increasing complexity of risk exposures faced by insurers, thereby amplifying the need for advanced ERM frameworks

6.2 Insurance Penetration and Economic Contribution

In 2024, per capita insurance expenditure increased significantly, reflecting growing awareness and adoption of insurance products:

PR capita insurance spending rose by approximately 16% to SAR 2,367.

Insurance penetration (premiums as a percentage of GDP) reached approximately 2.59%, with some variation across data sources (Agaam, 2024)

These trends highlight the expanding role of insurance in supporting Saudi Arabia's economic diversification objectives under Vision 2030 and the growing importance of institutionalized risk management practices.

7. EMERGING RISKS AND STRATEGIC CHALLENGES

7.1. Digital Transformation and Cybersecurity

The Saudi insurance sector is undergoing rapid digital transformation through Insurtech innovation, digital distribution, and fintech integration. While these developments improve efficiency and customer experience, they also increase exposure to cybersecurity and data privacy risks. Regulatory frameworks, including SAMA's Cyber Security Framework, emphasize continuous risk identification, monitoring, and control enhancement principles that are fully aligned with ISO 31000's dynamic and adaptive risk management philosophy (ISO, 2018)

7.2. Innovation and Regulatory Sandboxes

Regulators have introduced regulatory sandbox environments to encourage innovation while maintaining adequate risk controls. These sandboxes require participating insurers to demonstrate robust governance, customer protection measures, and risk management processes, further reinforcing the relevance of structured ERM frameworks

7.3. Climate-Related and Other Emerging Risks

Climate change and related natural catastrophe risks are increasingly recognized as material exposures for insurance companies due to their potential impact on claims volatility, reserving adequacy, and capital requirements. Although climate risk frameworks are still evolving in Saudi Arabia, global insurance research emphasizes the need for advanced risk modeling and scenario analysis capabilities supported by ISO 31000's emphasis on uncertainty, dynamic risk assessment, and continuous improvement (Florio & Leoni, 2017)

8. ISO 31000 AS AN ENHANCEMENT TOOL IN INSURANCE COMPANIES

8.1. Purpose and Scope

ISO 31000 provides principles, a framework, and a process that insurance companies can apply to create and protect value by managing risk consistently across underwriting, claims, investments, and operations. Unlike traditional approaches that confine risk management to specialized departments, ISO 31000 is designed to be integrated into governance and decision-making, reinforcing its strategic relevance (ISO, 2018)

8.2. Identifying and Assessing Insurance Risks Using ISO 31000

Step A1: Establishing the Context (Insurance-Specific)

This step involves defining:

Risk objectives: solvency protection, profitability, market conduct, liquidity resilience, and customer outcomes

Risk criteria: financial, regulatory, and reputational impact scales; likelihood measures; time horizons; and tolerance limits

Table 12 Impact Scale by Risk Type (Underwriting, Claims, and Liquidity)

Impact thresholds should be calibrated to the insurer's business mix, capital adequacy, reinsurance structure, and liquidity risk appetite. The scale is aligned with ISO 31000 guidelines and commonly applied ERM practices in insurance companies (International Organization for Standardization, 2018)

Scope: product lines, distribution channels, reinsurance arrangements, and investment strategies

A shared context ensures that underwriting, claims, and liquidity risks are assessed using common risk language, enabling consistent and comparable decision-making

Step A2: Risk Identification

Underwriting Risk:

Mispricing, adverse selection, portfolio concentration, catastrophe exposure, and data/model risk

Claims Risk:

Claims inflation, litigation trends, fraud and leakage, reserving inadequacy, and operational backlogs

Liquidity Risk:

Claim payout volatility, surrender and lapse risk, asset–liability mismatches, and exposure to illiquid investments

This table illustrates the graduated impact of claims risk on insurers' liquidity and underwriting performance, ranging from insignificant claim fluctuations to extreme events that threaten solvency and capital adequacy. It supports risk impact assessment by linking claims volatility to liquidity management, reserving decisions, pricing adjustments, and reinsurance dependence within an Enterprise Risk Management (ERM) and prudential supervision framework

Table 12: Impact Levels of Claims Risk on Liquidity and Underwriting Performance.

Impact Level	Underwriting Impact	Liquidity Impact	Claims Impact
1 – Insignificant	Marginal pricing deviation; no effect on loss ratio	No impact on cash flows; liquidity buffers unchanged	Isolated low-value claims within expected norms
2 – Minor	Slight deterioration in loss ratio within tolerance limits	Short-term liquidity pressure absorbed by operating cash flows	Temporary increase in claims frequency or severity; manageable through routine controls
3 – Moderate	Noticeable underwriting losses in a line of business; re-pricing required	Increased cash outflows requiring use of liquid assets or rebalancing	Claims volatility affecting quarterly results; reserve strengthening needed
4 – Major	Significant underwriting losses threatening annual profitability; reinsurance dependence increases	Liquidity stress requiring asset liquidation or external funding	Material reserve inadequacy or claims inflation affecting solvency margins
5 – Severe / Catastrophic	Sustained underwriting failure threatening capital adequacy or business viability	Severe liquidity shortfall threatening ability to meet obligations	Extreme claims events (e.g., catastrophe, mass litigation) endangering solvency

Table 13: Quantitative Impact Thresholds by Risk Type (Insurance Context).

Impact Level	Underwriting Risk (Loss Ratio %)	Claims Risk (Claims Inflation %)	Liquidity Risk (Liquidity Coverage %)
1 – Insignificant	≤ 65% (well below target loss ratio)	≤ 3% increase (within actuarial assumptions)	≥ 150% (strong liquidity buffer)
2 – Minor	66% – 75% (within risk appetite)	4% – 6% (manageable deviation)	130% – 149% (comfortable liquidity position)
3 – Moderate	76% – 90% (pressure on profitability)	7% – 10% (requires reserve review)	110% – 129% (heightened monitoring required)
4 – Major	91% – 105% (underwriting loss)	11% – 20% (material reserve strengthening needed)	100% – 109% (liquidity stress)
5 – Severe / Catastrophic	> 105% (threat to capital adequacy)	> 20% (solvency-threatening claims shock)	< 100% (inability to meet obligations without external support)

Loss Ratio (%) = Claims Incurred ÷ Earned Premiums.

Claims Inflation (%) reflects deviations from expected claims severity and frequency assumptions used in reserving and pricing.

Liquidity Coverage (%) represents available liquid assets relative to short-term obligations and expected claims outflows.

9. DISCUSSION AND CONCLUSION

This study demonstrates that the governance value of ISO 31000 in the insurance sector is contingent on implementation depth rather than formal adoption. While regulatory pressure encourages widespread diffusion of ISO 31000, the findings show that its contribution to Enterprise Risk Management (ERM) effectiveness emerges only when the framework is substantively integrated into governance structures and strategic decision-making processes. This outcome supports institutional theory by confirming that coercive regulatory environments often produce symbolic compliance, which limits the governance benefits of standardized risk frameworksFrom a resource-based perspective, the results indicate that ISO 31000 functions as an organizational capability only when embedded in routines, information flows, and board oversight mechanisms. In such cases, ERM becomes a value-creating governance process that enhances coordination, decision quality, and risk awareness. Conversely, when ISO 31000 is adopted primarily to signal regulatory conformity, its impact on ERM effectiveness remains limited, helping to explain the mixed evidence reported in prior ERM literature The Saudi insurance market provides a theoretically relevant setting due to its strong regulatory oversight and recent supervisory consolidation. The findings suggest that regulatory mandates alone are insufficient to ensure effective ERM. Instead, supervisory frameworks should emphasize governance integration and risk-informed decision-making to move beyond procedural compliance toward substantive risk governance. By integrating institutional theory and the resource-based view, this study contributes to the financial regulation literature by clarifying the conditions under which international risk management standards enhance ERM effectiveness in regulated insurance markets.

10. RECOMMENDATIONS

1. Insurance Companies

1.1. Integrate ISO 31000 into board-level strategy, underwriting, pricing, reserving, and investment decisions to strengthen risk-informed governance.

1.2. Enhance ERM capabilities through targeted professional certification and continuous training for boards and senior management.

2. Regulators and Supervisory Authorities

2.1. Shift supervisory focus from formal compliance toward ERM maturity and governance integration.

2.2. Introduce a Risk Management Maturity Index within risk-based supervision, with proportional incentives for advanced ISO 31000 integration.

3. Future Research

3.1. Conduct longitudinal studies to assess the long-term effects of ISO 31000 integration on ERM effectiveness and financial stability under evolving regulatory regimes.

Manuscript Title

ISO 31000, Regulatory Compliance, and Enterprise Risk Management Effectiveness: Evidence from Saudi Insurance Companies under a Transitioning Supervisory Regime

Author Contribution Statement: The author is the sole contributor to this manuscript and is responsible for the study conception, design, data collection, analysis, interpretation of results, and manuscript preparation

Conflict of Interest: The author declares no conflict of interest

Funding: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad ibn Saud Islamic University (IMSIU) (grant number IMSIU- DDRSP2604)

Ethical Approval: This study does not involve human subjects requiring formal ethical approval. Survey participation was voluntary and anonymous

REFERENCES

Alshammari, A. A., & Islam, M. A. (2022). Risk governance and regulatory reforms in Saudi insurance companies. Journal of Financial Regulation and Compliance, 30(4), 520–536. https://doi.org/10.1108/JFRC-01-2022-0011

Alzoubi, H. M., & Aziz, R. A. (2021). The impact of enterprise risk management on firm performance: Evidence from emerging markets. Journal of Accounting & Organizational Change, 17(3), 341–362. https://doi.org/10.1108/JAOC-06-2020-0065

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

Aven, T., & Renn, O. (2020). Improving government policy on risk: Eight key principles. Reliability Engineering & System Safety, 198, 106810. https://doi.org/10.1016/j.ress.2020.106810

Aven, T., & Ylönen, M. (2019). Enterprise risk management: A literature review and agenda for future research. European Journal of Operational Research, 273(3), 1059–1070. https://doi.org/10.1016/j.ejor.2018.09.039

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. Contemporary Accounting Research, 30(4), 1264–1295. https://doi.org/10.1111/j.1911-3846.2012.01194.x

Boiral, O. (2011). Managing with ISO systems: Lessons from practice. Long Range Planning, 44(3), 197–220. https://doi.org/10.1016/j.lrp.2010.12.003

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

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. The British Accounting Review, 49(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Gates, S., Nicolas, J. L., & Walker, P. L. (2012). Enterprise risk management: A process for enhanced management and improved performance. Management Accounting Quarterly, 13(3), 28–38.

Hopkin, P. (2020). Fundamentals of risk management (6th ed.). Kogan Page.

Hoskisson, R. E., Wright, M., Filatotchev, I., & Peng, M. W. (2013). Emerging multinationals from mid-range economies: The influence of institutions and factor markets. Journal of Management Studies, 50(7), 1295–1321. https://doi.org/10.1111/joms.12042

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and Insurance, 78(4), 795–822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

IFRS Foundation. (2022). International financial reporting standards (IFRSs): Consolidated without early application. IFRS Foundation.

International Organization for Standardization. (2018). ISO 31000: Risk management—Guidelines. ISO.

Khan, M. J., Hussain, D., & Mehmood, W. (2016). Why do firms adopt enterprise risk management? Managerial Finance, 42(6), 584–600. https://doi.org/10.1108/MF-09-2014-0227

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: Empirical evidence from Germany. European Journal of Finance, 24(10), 867–887. https://doi.org/10.1080/1351847X.2017.1347100

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. Risk Management and Insurance Review, 6(1), 37–52. https://doi.org/10.1111/1098-1616.00019

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

Paape, L., & Speklé, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. European Accounting Review, 21(3), 533–564. https://doi.org/10.1080/09638180.2012.661937

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. Journal of Risk and Insurance, 78(1), 185–211. https://doi.org/10.1111/j.1539-6975.2010.01378.x

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

Purdy, G. (2018). ISO 31000:2018—Setting a new standard for risk management. Risk Management, 20(2), 72–83.

Saudi Central Bank. (2022). Insurance supervisory framework and solvency requirements. SAMA.

World Economic Forum. (2023). Global risks report 2023. WEF.