ResearchLEAP

Journal of International Business Research and Marketing
Volume 8, Issue 1, 2023
journal homepage: www.researchleap.com

Enterprise Risk Management Practices in Kenya

Stanley Chege, Gregory Wanyembi, Constantine Nyamboga
Enterprise Computing, Mount Kenya University Computing and Informatics, Thika, Kenya

DOI: *10.18775/jibrm.1849-8558.2015.81.3002*
URL: *https://doi.org/10.18775/jibrm.1849-8558.2015.81.3002*

Keywords:
Enterprise Risk Management, ERM, ISO 31000, NIST RMF, COSO ERM, Resilience, Sustainability, Corporate Governance.

ABSTRACT

Enterprise Risk Management (ERM) is a structured and coordinated approach for identifying, assessing, and managing risks faced by an organization. Implementing ERM standards and frameworks has several benefits, including improving focus and perspective on risk. ERM aids in developing leading indicators to detect potential risk events and provide early warning signals. ERM also incorporates key metrics and measurements of risk to improve reporting value and analysis and monitor possible changes in risk vulnerabilities or likelihood. An ERM facilitates an efficient risk management (RM) process, allowing businesses to manage risks efficiently across various departments through a robust risk management framework. This framework includes the related department's team, working rules, and operational tools, covering all types of risks, including financial, strategic, operational, and accidental losses. The primary advantage of ERM is its ability to create a systematic and intentional process for identifying and addressing risks, treating risk management as a structured exercise where liabilities are addressed as part of a comprehensive framework rather than ad-hoc problem-solving. ISO 31000, NIST risk management framework, and COSO ERM framework are widely used frameworks for managing enterprise risks. Implementing a robust enterprise risk management standard has a positive relationship with business performance.

1. Introduction

ERM standards and frameworks provide guidance and best practices for managing risk in organizations (Bromiley and Rau, 2014). Organizations can choose the framework that best suits their needs and implement it to improve their risk management practices (Bromiley, McShane, Nair and Rustambekov, 2015). There are several risk management standards and frameworks available that organizations can use to manage risks effectively (Hutchins, 2018).

ISO 31000:2018 is an international standard for risk management that provides a comprehensive framework for risk management, including principles, guidelines, and a process for managing risk. ISO 31000 is a flexible standard that can be applied to any organization, regardless of size, industry, or sector (Simona and Cristian, 2018).

The COSO ERM is a framework for enterprise risk management that helps companies manage risks and achieve their strategic objectives. The framework includes five components: governance and culture, strategy and objective setting, performance, review and revision, and information, communication, and reporting (Moeller, 2007).

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a widely used framework for managing cybersecurity risk, which includes six steps: categorize, select, implement, assess, authorize, and monitor (Maclean, 2017).

The Silicon Valley Bank (SVB) recently experienced a significant collapse attributed to problems with risk management practices, which has been described as a colossal failure in asset-liability risk management (Oxford Analytica, 2023a). The bank failed to adequately manage its risks related to interest rate changes, leading to significant dislocation that triggered a mass withdrawal of deposits by startup clients. This, in turn, led to a liquidity crisis that ultimately caused the bank to collapse. The collapse of SVB has had significant repercussions for both depositors and borrowers, many of whom are startup companies and venture capitalists (Oxford Analytica, 2023b).

The Enron scandal was a sequence of events that resulted in the bankruptcy of Enron Corporation and the dissolution of Arthur Andersen LLP, one of the world's largest auditing and accounting companies. The collapse of Enron, which held assets worth more than $60 billion, resulted in one of the largest bankruptcy filings in history (Petrick and Scherer, 2003).

Enron's collapse also highlighted the inadequacy of its risk management practices. The company used complex and opaque accounting methods to conceal its actual financial position, preventing stakeholders from evaluating the risks associated with investing in the company. Enron's risk management framework was also found to be inadequate and unable to identify and manage the risks associated with the company's business operations. The Enron scandal serves as a warning about the importance of effective risk management practices and transparency in financial reporting (Nelson, Price and Rountree, 2008).

The 2008 financial crisis was a catastrophic event that had a negative impact on the economy. One of the major contributors to the crisis was the failure of risk management practices. Liquidity risk management weaknesses, as well as other areas of risk management, such as market, credit, and operational risks, were significant contributors to the crisis (Erkens, Hung and Matos, 2012).

The crisis exposed the limitations of banks' risk management, despite the use of complex models and algorithms to manage risks. Failures in corporate governance and risk management at many systemically important financial institutions were the primary causes of the crisis (Spiegel, 2011). The 2008 financial crisis revealed significant deficiencies in risk management practices in the financial industry, including inadequate attention to liquidity risk, poor risk modeling, and failures of corporate governance (Luchtenberg and Vu, 2015).

2. Problem Statement

The absence of effective risk management systems in organizations has resulted in the downfall of corporate giants. As a consequence, investor confidence has been weakened (Simona and Cristian, 2018). To re-establish investor confidence and guarantee business resilience and sustainability, organizations must establish sturdy ERM systems. However, the primary issue is that organizations do not have a strategy to implement resilient ERM systems (Tahir and Razali, 2011). Furthermore, some organizations in Kenya encounter the particular problem of not having effective ERM systems, standards, and frameworks.

3. Literature Review

3.1. ISO 31000:2018

ISO 31000:2018 is a set of guidelines for managing risk faced by organizations. The standard includes eight principles for effective risk management that aim to create and protect value, improve performance, encourage innovation, and support the achievement of objectives (Tranchard, 2018).

One strength of ISO 31000:2018 is its flexibility. The guidelines can be customized to any organization and its context, allowing for a tailored approach to risk management. Another strength is that the use of simplified language and purpose statements in the standard can make it easier for organizations to understand and implement (Wicaksono, 2020). One limitation is that the standard is too general and lacks specific guidance on how to implement risk management practices. Another limitation is that the standard is voluntary and not legally binding, which may limit its effectiveness. The standard is a flexible set of guidelines for managing risk that can be tailored to any organization and its context. The standard includes principles for effective risk management but may lack specific guidelines and is not legally binding (Parviainen, Goerlandt, Helle, Haapasaari, and Kuikka, 2021).

ISO 31000:2018 includes the following clauses: The Scope clause defines the scope of the standard and provides an overview of the guidelines it contains. The Normative clause references list the references used in the standard. The Terms and Definitions clause provides definitions for key terms used throughout the standard. The Principles clause identifies eight principles for effective risk management (Syahputri, and Kitri, 2020). These principles aim to create and protect value, improve performance, encourage innovation, and support the achievement of objectives. The Framework clause describes the risk management framework, including its components and how they are integrated. The Process clause outlines the risk management process, which includes establishing the context, assessing risk, treating risk, and monitoring and reviewing risk (Rampini, Takia, and Berssaneti, 2019). The Monitoring and review clause describes the monitoring and review process, including how to evaluate the effectiveness of risk management and make improvements as needed. The Communication and consultation clause emphasizes the importance of communication and consultation throughout the risk management process. The standard has annexes namely: Annex A provides additional guidance on establishing the context for risk management. Annex B provides additional guidance on assessing risk. Annex C provides additional guidance on treating risk. Annex D provides additional guidance on monitoring and reviewing risk (Qinthara, Sutari and Salma, 2021).

ISO 31000:2018 includes eight principles for effective risk management. The standard outlines a risk management framework and process, as well as guidance on monitoring and review, communication and consultation, and additional guidance in four annexes (Alijoyo, 2022).

ISO 31000:2018 Clause 4 deals with Principles. The eight principles are: Risk management (RM) creates and protects

value; RM integrates into organizational processes; RM is part of decision-making; RM explicitly addresses uncertainty; RM is systematic, structured, and timely; RM is based on the best available information; RM is tailored to the organization; RM takes human and cultural factors into account (Hutchins, 2018). ISO 31000:2018 underscores the wisdom of infusing RM into all organizational activities, processes, and decision-making. Organizations should implement the ISO 31000 principles and components that are best suited to their specific circumstances and modify other principles and components (Simona and Cristian, 2018).

ISO 31000:2018 Clause 4 of the standard focuses on the risk management framework. The risk management framework consists of three key elements: risk management principles, the risk management framework itself, and the risk management process. The principles include concepts such as risk ownership, risk communication, and continuous improvement. The framework sets out the overall approach to managing risk, including the establishment of objectives, the identification of risks, and the development of risk treatment plans. The risk management process involves a cyclical series of steps, including risk identification, analysis, evaluation, treatment, and monitoring and review. Clause 4 of ISO 31000:2018 provides a comprehensive overview of the risk management framework and its key components (Tranchard, 2018).

The ISO 31000:2018 Clause 5 focuses on the principles of RM. Risk management should be infused into all processes and cultures. The clause highlights the importance of evaluating the external and internal context of an organization, including the identification of stakeholders and their requirements, in the risk management process. The clause also emphasizes the need to establish clear and concise risk management objectives and to take a proactive approach. ISO 31000:2018 puts a greater emphasis on integrating risk management into all organizational activities, processes, and decision-making, as opposed to being a separate, departmentalized activity (Wicaksono, 2020).

ISO 31000:2018 Clause 6 outlines the RM process. The clause highlights the vitality of a structured approach to risk assessment and treatment, which may involve selecting and applying risk evaluation techniques, developing, and implementing risk treatment plans, and evaluating the effectiveness of risk management actions. The clause concludes by stressing the need for ongoing monitoring and review of the risk management process to ensure its continuing effectiveness and relevance (Parviainen, Goerlandt, Helle, Haapasaari, and Kuikka, 2021).

ISO 31000:2018 Clause 7 deals with monitoring and reviewing the risk management framework, criteria, analysis, and treatment to ensure that they remain relevant and effective. Monitoring and review are essential components of a successful risk management strategy that follows the ISO 31000 framework. Continuous evaluation is necessary as the organization evolves, and reviews could be conducted on a monthly, weekly, or annual basis (Syahputri and Kitri, 2020).

The ISO 31000:2018 Clause 8 deals with the communication and consultation aspect of risk management. The clause emphasizes the importance of clear and effective communication throughout the entire risk management process, including identifying, assessing, treating, monitoring, and reviewing risks. The standard recommends that organizations establish communication protocols that ensure all relevant stakeholders are kept informed about risks and risk management decisions. This includes both internal stakeholders, such as employees and management, and external stakeholders, such as customers, suppliers, and regulators. The clause also highlights the importance of consultation with stakeholders, particularly in the risk assessment and treatment phases, to ensure that all perspectives and concerns are considered (Rampini, Takia and Berssaneti, 2019).

The standard may be summarized as follows: Principles: This clause outlines the fundamental principles of risk management, including the need for a structured approach and the importance of considering the internal and external context. Framework: This clause outlines the overall framework for managing risk, including the establishment of a risk management policy and the identification of risk criteria (Alijoyo, 2022). Process: This clause describes the risk management process, including the steps of risk identification, analysis, evaluation, treatment, monitoring, and review. Monitoring and review: This clause outlines the ongoing monitoring and review of the risk management process to ensure its continued effectiveness. Communication and continual improvement: The clause emphasizes the importance of continually improving the risk management process through evaluation and feedback (Qinthara, Sutari, and Salma, 2021).

3.2. NIST Risk Management Framework (RMF)

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a comprehensive, flexible, risk-based approach that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The RMF provides a process for organizations to manage their risk in a structured, consistent, and repeatable manner (Maclean, 2017).

One strength of the RMF is its ability to complement an organization's existing cybersecurity program and risk management processes. Through the creation of profiles, organizations can identify areas where existing processes may be strengthened or new processes can be implemented (Rose, 2022). The RMF offers a wide range of controls and control types that can be implemented through policies, plans, and operational procedures, as well as through the configuration of

operating systems and applications (McCarthy and Harnett, 2014).

One limitation of the RMF is that it can be complex and time-consuming to implement. The RMF requires a significant amount of documentation and coordination between multiple stakeholders, which can make it difficult to manage and maintain over time. The RMF may not be suitable for all organizations, as it is primarily designed for federal agencies and other large organizations with complex systems and extensive security requirements (Patel, 2011).

The NIST RMF provides a comprehensive, flexible, risk-based approach to managing an organization's security, privacy, and cyber supply chain risk management activities. While the RMF has strengths in its ability to complement existing cybersecurity programs and provide a wide range of controls, it may be complex and time-consuming to implement, and may not be suitable for all organizations (Rose, 2021).

3.3. COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework is a widely accepted framework that defines internal control as a process designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance (Anderson, 2017). The framework is designed to improve the corporate governance function within organizations and monitor security, risk, and compliance programs to ensure adherence to policies, goals, and laws (Gjerdrum and Peter, 2011).

One strength of the COSO ERM framework is its widespread acceptance in the accounting literature and by entities. The framework is designed to improve risk assessments within organizations and encourage a more proactive approach to risk management (Williamson, 2007).

One limitation is that the COSO ERM may not be suitable for all organizations, as it is primarily designed for large public companies and government entities (Scott, 2004). The framework may not be sufficiently comprehensive in addressing all aspects of risk management, such as emerging technology risks and strategic risks (dan Perbankan, 2021).

The COSO ERM framework is widely accepted in the accounting industry and by entities and is designed to improve risk assessments and corporate governance within organizations. The framework may not be suitable for all organizations and may not sufficiently address all aspects of risk management (Williamson, 2007).

3.4. Organizational Resilience

Organizational resilience is a critical factor for businesses to survive and thrive in uncertain times. Businesses can develop resilience by implementing scripted routines, simple rules, and the ability to improvise. Organizations can build resilience across six crucial dimensions: financial, operational, technological, organizational, reputational, and business model resilience (Fiksel, 2015).

Building resilient teams is crucial for organizational resilience. Resilient teams build caring and supportive relationships with each other, which is the basis of their productivity. Succession planning has several benefits for organizational resilience. The planning can protect the business from sudden unexpected changes by ensuring that there is a plan in place to handle such events. The planning can help to retain talent by providing employees with a clear direction for career advancement and making them feel valued. The planning can contribute to the development of a diverse and inclusive leadership team and organizational culture. The planning can facilitate effective onboarding and communication between employees and their superiors, leading to a better-functioning organization (Dalziell, and McManus, 2004).

The best practices for organizational resilience include developing scripted routines, implementing simple rules, and improvisation, building resilience across six crucial dimensions, and fostering supportive relationships within teams. By adopting these practices, businesses can better cope with and thrive in uncertain times. There is a relationship between good practices in enterprise risk management and organizational resilience (Burnard and Bhamra, 2011).

Organizational resilience is the ability of an organization to anticipate, prepare for, respond to, and recover from disruptions in a way that enables it to continue its operations, grow and evolve. Resilient organizations can become more adaptable and agile, and better equipped to face the challenges of the modern world (Erol, Sauser and Mansouri, 2010).

3.5. Corporate Governance

Corporate governance refers to the set of practices and policies that ensure that a company is directed and managed effectively. Some of the good practices of corporate governance are clearly defining the roles and responsibilities of the board of directors, management, and other stakeholders is essential for effective corporate governance (Fung, 2014).

Companies should maintain transparency in their operations, financial reporting, and decision-making processes. This helps build trust among stakeholders and reduces the risk of fraud and corruption. Companies should establish mechanisms to hold directors, management, and other stakeholders accountable for their actions. This includes setting performance targets, conducting regular performance evaluations, and implementing consequences for non-compliance (Davies, 2012).

Organizations should foster a culture of ethics and integrity. A strong ethical culture is essential for effective corporate governance. Companies should establish a code of conduct and ensure that it is communicated and enforced throughout the organization. Companies should identify and manage risks to the business, including financial, legal, and reputational risks. This includes establishing risk management policies and procedures and conducting regular risk assessments (Sarbah and Xiao, 2015).

Companies should maintain strong relationships with stakeholders, including shareholders, employees, customers, and suppliers. This helps build trust and ensures that the company's decisions are aligned with stakeholder interests. Organizations need to ensure continuous monitoring and evaluation. Companies should regularly review their governance practices and policies and make necessary improvements to ensure their effectiveness. Companies should ensure effective corporate governance, build trust among stakeholders, and create long-term value for shareholders (Shanikat and Abbadi, 2011).

3.6. The World Economic Forum (WEF) Global Risks Report

The WEF published the Global Risks Report 2023. This report explores the severe risks that may arise over the next decade, such as climate change, geopolitical instability, and cyber threats (WEF, 2023).

The report highlights that the short-term risk landscape is dominated by energy, food, debt, and natural disasters. The most vulnerable demographics and regions are already suffering. The report warns that tougher trade-offs risk eroding climate action, human development, and future resilience (WEF, 2023).

The report includes a ranking of the top 10 risks based on their likelihood and potential impact, with the top five risks being extreme weather, infectious diseases, biodiversity loss, cyber-attacks, and the failure of national governance systems. The WEF Global Risks Report 2023 provides a comprehensive analysis of the most severe risks that may impact the world over the next decade and offers insights and strategies to mitigate them (WEF, 2023).

3.7. COBIT

The COBIT (Control Objectives for Information and Related Technology) framework is a comprehensive set of globally accepted practices, analytical tools, and models designed for the governance and management of enterprise IT. COBIT can be used as a benchmark to map current policies and procedures. COBIT can define or refine a process or identify areas of improvement in the implementation of IT governance (De Haes, Van Grembergen and Debreceny, 2013).

COBIT 2019 is an umbrella framework that references several standards, including the ISO/IEC 27000 series, ITIL, and NIST, and provides a holistic and integrated approach to enterprise IT governance and risk management (Năstase, Năstase and Ionescu, 2009).

COBIT is not a standalone framework for risk management. COBIT is a set of practices and processes for IT governance and management, which includes risk management as one of its components. Organizations should complement COBIT with other frameworks or standards, such as ISO/IEC 31000 or COSO ERM, to ensure a comprehensive and effective risk management process (Zhang, le Fever and le Zhang, 2013).

4. Methodology

The study employed the qualitative case study design. The qualitative case study design is a research method that involves an in-depth exploration of a particular phenomenon or case through detailed analysis of various sources of data (Baxter and Jack, 2008).

The qualitative case study design offers researchers the ability to gather detailed information and analyze data in-depth. The limitations of the design include the potential for bias, limited generalization, and time-consuming data collection and analysis (Stake, 2008).

5. Case Studies

5.1. Safaricom Kenya

Safaricom Kenya is a telecommunications company that provides mobile phone, broadband, and digital services. The company has a comprehensive approach to risk management, which involves identifying, assessing, and mitigating potential risks (Safaricom, 2023a).

One of the key topics covered in their sustainability reports is governance, risk management, and compliance. Safaricom has implemented a GRC system that enables them to manage regulations, and compliance, and track risks and related controls across the enterprise. This system has allowed for the easy integration of governance, risk, and compliance activities into existing processes (Safaricom, 2023b).

Safaricom Kenya has a comprehensive approach to risk management that involves identifying, assessing, and mitigating potential risks across its operations. The company's risk management practices include ERM, risk assessment, operational risk management, business continuity planning, and compliance management (Otera, 2020).

5.2. Equity Bank Holdings Kenya

Equity Bank Holdings Kenya is a financial services company that provides banking and financial solutions. The company has a robust approach to risk management that ensures that

potential risks are identified, assessed, and mitigated to protect the business and its customers.

Equity Bank is committed to complying with all applicable regulations. The company has a compliance management framework that ensures it meets all regulatory requirements and industry best practices. Equity Bank Holdings Kenya has a robust approach to risk management that involves identifying, assessing, and mitigating potential risks across its operations. The company's risk management practices include ERM, risk assessment, credit risk management, operational risk management, and compliance management (Kariuki, 2020).

5.3. KCB Bank Group

KCB Bank Group provides banking and financial services in Kenya. The bank has implemented several risk management practices to ensure that potential risks are identified, assessed, and mitigated effectively.

KCB Bank Group has a robust approach to risk management that involves identifying, assessing, and mitigating potential risks across its operations. The bank's risk management practices include ERM, risk assessment, credit risk management, operational risk management, compliance management, disaster recovery, and business continuity planning (Wanjohi, 2013).

5.4. Co-operative Bank of Kenya

Co-operative Bank of Kenya is a financial institution that provides banking and financial services in Kenya. The bank has implemented several risk management practices to ensure that potential risks are identified, assessed, and mitigated effectively.

The Co-operative Bank of Kenya has a robust approach to risk management that involves identifying, assessing, and mitigating potential risks across its operations. The bank's risk management practices include ERM, risk assessment, credit risk management, operational risk management, compliance management, disaster recovery, and business continuity planning (Gweyi, 2013).

5.5. Stanbic Bank of Kenya

Stanbic Bank provides banking and financial services in Kenya. The bank has implemented several risk management practices to ensure that potential risks are identified, assessed, and mitigated effectively.

The Stanbic Bank of Kenya has a robust approach to risk management. The bank released a risk and capital management report. The report provides insight into the risk management practices of the Standard Bank Group and the measures taken to mitigate potential risks. (Stanbicbank, 2023).

5.6. ICEA LION Kenya

ICEA LION has competent staff with professional experience in risk management, internal controls, and corporate governance. The organization values the expertise of professionals in enterprise risk management and has adopted the Kenyan insurance industry-specific guidelines for robust risk management.

ICEA LION is committed to sustainability and risk management practices. The company has adopted best-practice corporate governance practices, and long-term sustainability is a key pillar in its operations. ICEA LION's commitment to sustainability is demonstrated by its projects and impact stories, which show how the company protects companies and consumers from environmental, social, and governance risks, contributing to a more sustainable future (Icealion, 2023).

5.7. CIC group

CIC Group is one of the leading insurance companies in Kenya and has experienced exponential growth over the years. CIC adopted a framework to assess ERM practices, which includes five dimensions: insights and transparency, natural ownership, risk appetite, and strategy, risk-related decisions and processes, risk organization and governance, and risk culture and performance transformation (cicinsurancegroup, 2023).

5.8. BRITAM

Britam is a financial services company in Kenya, offering a wide range of products and services in insurance and asset management. The company ensures that all risks are identified, analyzed, and evaluated regularly while identifying, defining, and describing the broad risk group. The company has competent personnel who provide oversight and direction for the management of all risks across the group and is responsible for the identification, assessment, and management of all risks associated with both new and existing business (Britam, 2023).

6. Conclusion

There are several recent trends in enterprise risk management. One trend is the recognition that the risk landscape is changing rapidly, and new risks and response strategies are emerging all the time. Due to the long-term repercussions of the COVID-19 pandemic and the possibility of a recession, companies are realizing the need for stronger Enterprise Risk Management (ERM) programs to compete in the new era (Amankwah-Amoah, Khan, Wood and Knight, 2021).

More enterprises are adopting risk maturity frameworks to consolidate workflows and establish a consistent risk management process across the organization. These frameworks provide a structured approach to risk management, enabling organizations to measure, track, and report their risk maturity levels (Ershadi, Jefferies, Davis, and Mojtahedi, 2020).

Environmental, social, and governance (ESG) risks are gaining prominence as investors, customers, and regulators are increasingly prioritizing sustainability and ethical business practices. Organizations are expanding their risk management frameworks to include ESG risks and disclosing their ESG performance to stakeholders (de Silva Lokuwaduge and de Silva, 2020).

As organizations become more reliant on technology to drive their business, technology risks such as cyber threats, data breaches, and system failures are increasing. Organizations are investing in advanced technologies such as artificial intelligence (AI) and machine learning (ML) to mitigate these risks. Cyber risk needs to be quantified in terms of monetary value via an exhaustive risk assessment process (Galaz, Centeno, Callahan, Causevic, Patterson, Brass and Levy, 2021). With an ever-changing regulatory landscape, organizations are facing increased regulatory scrutiny and penalties. Organizations are adopting a proactive approach to regulatory compliance by leveraging risk management tools and frameworks to identify and mitigate compliance risks (Anagnostopoulos, 2018).

The COVID-19 pandemic illuminated the need for business continuity planning (BCP). Organizations are reviewing their BCPs to ensure they are effective in responding to unexpected disruptions and building resilience to future crises (Schmid, Raju and Jensen, 2021).

Various risk management teams need to work closely with business units to identify and manage risks. This will reduce siloed risk management functions and improve collaboration. This approach enables organizations to take a holistic view of their risk landscape and develop a coordinated response to mitigate risks. There is a need for organizations to enhance and contextualize risk monitoring according to the roles and profiles in the organization (Hasham, Joshi and Mikkelsen, 2019).
The practices of enterprise risk management (ERM) have evolved beyond traditional financial governance to include security, IT, third-party relationships, and GRC. The complexity in organizations, particularly due to data silos and operating environments, is causing enterprises to adopt integrated governance, risk, and compliance (IGRC) programs to simplify their risk management activities (Caldwell, Eid and Casper, 2008).

Many companies consider risk management as a strategy to improve business performance and gain a competitive advantage instead of just avoiding negative situations (Nocco and Stulz, 2006). Improving communication with employees, investors, and regulators in risk management is essential. While some risks are necessary for revenue expansion, a program must be in place to take decisive action if too many customers default (Gontarek and Bender, 2019).

Internal and external risk-sensing tools can generate risk intelligence, which helps identify trending and emerging risks, and improvements in all business units are necessary (Tounsi and Rais, 2018). The impact and frequency of extreme weather risk are growing, and CEOs and boards must implement risk management strategies to mitigate the effects on employees and assets (Sadgrove, 2016).

The top trends in enterprise risk management are the adoption of risk maturity frameworks, a new approach to the changing risk landscape, increased focus on ESG risks, technology risks, regulatory compliance risks, business continuity planning, and increased collaboration between risk management and business units (Lipton, Neff, Brownstein, Rosenblum, Emmerich, and Fain, 2011).

Robust enterprise risk management is associated with improved business performance. As businesses face more complex and varied risks, ERM becomes increasingly important (McShane, Nair and Rustambekov, 2011). Implementing a comprehensive ERM strategy can enhance business performance by identifying and addressing interruption risks, protecting against cyber threats, and promoting a risk-aware culture. By integrating ERM into strategic planning, organizations can achieve both their value creation and protection objectives. Appropriately addressing interruption risks can provide confidence and enable organizations to pursue business objectives more effectively (Arena, Arnaboldi and Azzone, 2010). As the volume and complexity of risks increase, organizations should focus on developing a strong ERM strategy to mitigate these risks and improve business performance (Hoyt a d Liebenberg, 2011).

Collaboration between business and IT units can improve risk management. IT can identify potential risks and vulnerabilities in the technology infrastructure, while business units can provide context and input on business risks and priorities (Gates, Nicolas and Walker, 2012).

References

- Agustina, L., & Baroroh, N. (2016). The relationship between Enterprise Risk Management (ERM) and firm value is mediated through financial performance. Review of Integrative Business and Economics Research, 5(1), 128.
- Ahmad, S., Ng, C., & McManus, L. A. (2014). Enterprise risk management (ERM) implementation: Some empirical evidence from large Australian companies. Procedia-Social and Behavioral Sciences, 164, 541-547. *CrossRef*
- Alijoyo, F. A. (2022). The use ISO 31000: 2018 in Indonesian Fintech Lending Companies: What Can We Learn? Journal of Business and Management Studies, 4(1), 16-22. *CrossRef*

- Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. Journal of Business Research, 136, 602-611.
- Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business, 100, 7-25. CrossRef
- Anderson, D. (2017). COSO ERM: Getting risk management right: Strategy and organizational performance are the heart of the updated framework. Internal Auditor, 74(5), 38-43.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. Accounting, Organizations and Society, 35(7), 659-675
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), 544-559.
- Britam. (2023). Investor relations. Retrieved from https://ke.britam.com/
- Bromiley, P., & Rau, D. (2014). Towards a practice-based view of strategy. Strategic Management Journal, 35(8), 1249-1256. CrossRef
- Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long range planning, 48(4), 265-276.
- Burnard, K., & Bhamra, R. (2011). Organizational resilience: development of a conceptual framework for organizational responses. International Journal of Production Research, 49(18), 5581-5599. CrossRef
- Caldwell, F., Eid, T., & Casper, C. (2008). Magic quadrant for enterprise governance, risk, and compliance platforms. Gartner Research G, 158295.
- Cicinsurancegroup. (2023). Investor Relations. Retrieved from https://www.cicinsurancegroup.com/
- Dalziell, E. P., & McManus, S. T. (2004). Resilience, vulnerability, and adaptive capacity: implications for system performance.
- dan Perbankan, J. K. (2021). COSO ERM Framework as the Basis of Strategic Planning in Islamic Banking. Jurnal Keuangan Dan Perbankan, 25(1), 21-35.
- Daud, W. N. W. D., Yazid, A. S., & Hussin, M. R. (2010). The effect of chief risk officer (CRO) on enterprise risk management (ERM) practices: Evidence from Malaysia. International Business & Economics Research Journal (IBER), 9(11). CrossRef
- Davies, M. A. (2012). Best practice in corporate governance: Building reputation and sustainable success. Gower Publishing, Ltd.
- De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. Journal of Information Systems, 27(1), 307-324.
- de Silva Lokuwaduge, C. S., & de Silva, K. (2020). Emerging corporate disclosure of environmental social and governance (ESG) risks: An Australian study. Australasian Accounting, Business and Finance Journal, 14(2), 35-50.
- Erkens, D. H., Hung, M., & Matos, P. (2012). Corporate governance in the 2007–2008 financial crisis: Evidence from financial institutions worldwide. Journal of corporate finance, 18(2), 389-411. CrossRef
- Erol, O., Sauser, B. J., & Mansouri, M. (2010). A framework for an investigation into extended enterprise resilience. Enterprise Information Systems, 4(2), 111-136.
- Ershadi, M., Jefferies, M., Davis, P., & Mojtahedi, M. (2020). Towards successful establishment of a project portfolio management system: business process management approach. The Journal of Modern Project Management, 8(1).
- Fiksel, J. (2015). Resilient by design: Creating businesses that adapt and flourish in a changing world. Island Press.
- Fung, B. (2014). The demand and need for transparency and disclosure in corporate governance. Universal Journal of Management, 2(2), 72-80. CrossRef
- Galaz, V., Centeno, M. A., Callahan, P. W., Causevic, A., Patterson, T., Brass, I., ... & Levy, K. (2021). Artificial intelligence, systemic risks, and sustainability. Technology in Society, 67, 101741.
- 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.
- Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework. Risk management, 31(21), 8-12.
- Gontarek, W., & Bender, R. (2019). Examining risk governance practices in global financial institutions: the adoption of risk appetite statements. Journal of Banking Regulation, 20, 74-85. CrossRef
- Gweyi, M. O. (2013). Credit risk mitigation strategies adopted by Commercial Banks in Kenya. International Journal of Business and Social Science, 4(6), 71-87.
- Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. McKinsey & Company, 2019.
- Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and insurance, 78(4), 795-822.
- Hutchins, G. (2018). ISO 31000: 2018 enterprise risk management. Greg Hutchins.
- ICEA Lion. (2023). Sustainability shared value. Retrieved from https://icealion.co.ke/
- Jiang, E. X., Matvos, G., Piskorski, T., & Seru, A. (2023). Monetary Tightening and US Bank Fragility in 2023: Mark-to-Market Losses and Uninsured Depositor Runs? Available at SSRN. CrossRef

- Kariuki, F. (2020). Sustainability in the financial sector in Kenya. Available at SSRN 3646976.
- Khan, M. J., Hussain, D., & Mehmood, W. (2016). Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. Management Decision.
- Lipton, M., Neff, D. A., Brownstein, A. R., Rosenblum, S. A., Emmerich, A. O., & Fain, S. L. (2011). Risk management and the board of directors. Bank and Corporate Governance Law Reporter, 45(6), 793-799.
- Luchtenberg, K. F., & Vu, Q. V. (2015). The 2008 financial crisis: Stock market contagion and its determinants. Research in International Business and Finance, 33, 178-203. *CrossRef*
- Maclean, D. (2017). The NIST risk management framework: Problems and recommendations. Cyber Security: A Peer-Reviewed Journal, 1(3), 207-217.
- McCarthy, C., & Harnett, K. (2014). National Institute of standards and Technology (NIST) cybersecurity risk management framework applied to modern vehicles (No. DOT HS 812 073). United States. National Highway Traffic Safety Administration.
- McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? Journal of Accounting, Auditing & Finance, 26(4), 641-658. *CrossRef*
- Moeller, R. R. (2007). COSO enterprise risk management: understanding the new integrated ERM framework. John Wiley & Sons.
- Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3, and ISO/IEC 27002 in enterprises. Economic computation & economic cybernetics studies & research, 43(3), 1-16.
- Nelson, K. K., Price, R. A., & Rountree, B. R. (2008). The market reaction to Arthur Andersen's role in the Enron scandal: Loss of reputation or confounding effects? Journal of Accounting and Economics, 46(2-3), 279-293.
- Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. Journal of applied corporate finance, 18(4), 8-20. *CrossRef*
- Otera, G. L. (2020). Evaluation of the impact of corporate governance practices on procurement compliance; case of Safaricom PLC (Doctoral dissertation, Strathmore University).
- Oxford Analytica. (2023a). SVB failure spells contagion but not systemic risk. Emerald Expert Briefings, (oxan-db).
- Oxford Analytica. (2023b). Banking overtakes jobs in importance to US rate moves. Emerald Expert Briefings, (oxides).
- Parviainen, T., Goerlandt, F., Helle, I., Haapasaari, P., & Kuikka, S. (2021). Implementing Bayesian networks for ISO 31000: 2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. Journal of Environmental Management, 278, 111520. *CrossRef*
- Patel, A. (2011). Baseline security controls for HIA-compliant EMR systems using a tailored NIST RMF approach.
- Petrick, J. A., & Scherer, R. F. (2003). The Enron scandal and the neglect of management integrity capacity. American Journal of Business, 18(1), 37-50.
- Power, M. (2009). The risk management of nothing. Accounting, organizations and Society, 34(6-7), 849-855. *CrossRef*
- Qinthara, H., Sutari, W., & Salma, S. A. (2021). Design of Risk Management System on Material Handling Services to Fulfill ISO 9001: 2015 Requirements Clause 6.1 Based on ISO 31000: 2018. JKIE (Journal Knowledge Industrial Engineering), 8(3), 154-166.
- Rampini, G. H. S., Takia, H., & Berssaneti, F. T. (2019). Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyses. Procedia Manufacturing, 39, 894-903. *CrossRef*
- Razali, A. R., & Tahir, I. M. (2011). Review of the literature on enterprise risk management. Business management dynamics, 1(5), 8.
- Razali, A. R., & Tahir, I. M. (2011). The determinants of enterprise risk management (ERM) practices in Malaysian public listed companies. Journal of Social and Development Sciences, 1(5), 202-207.
- Rochette, M. (2009). From risk management to ERM. Journal of Risk Management in Financial Institutions, 2(4), 394-408.
- Rose, S. (2021). Planning for a Zero Trust Architecture: A Starting Guide for Administrators (Draft) (pp. 16-16). National Institute of Standards and Technology.
- Rose, S. (2022). Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators (No. NIST CSWP 20, pp. 18-18). National Institute of Standards and Technology. *CrossRef*
- Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system: how a framework for IT governance supports ERM. Corporate Governance.
- Sadgrove, K. (2016). The complete guide to business risk management. Routledge.
- Safaricom. (2023a). Annual reports. Retrieved from https://www.safaricom.co.ke/
- Safaricom. (2023b). Sustainability Report. Retrieved from https://www.safaricom.co.ke/
- Sarbah, A., & Xiao, W. (2015). Good corporate governance structures: A must for family businesses. Open Journal of Business and Management, 3(01), 40. *CrossRef*
- Schmid, B., Raju, E., & Jensen, P. K. M. (2021). COVID-19 and business continuity-learning from the private sector and humanitarian actors in Kenya. Progress in Disaster Science, 11, 100181.

- Scott, A. (2004). COSO ERM framework released. Internal Auditor, 61(5), 17-19.
- Shanikat, M., & Abbadi, S. S. (2011). Assessment of corporate governance in Jordan: An empirical study. Australasian Accounting, Business and Finance Journal, 5(3), 93-106.
- Simona, D. A., & Cristian, D. (2018). Enterprise risk management–Benefits of ISO 31000: 2018. Revista OEconomica, (03-4).
- Spiegel, M. (2011). The academic analysis of the 2008 financial crisis: Round 1. The Review of Financial Studies, 24(6), 1773-1781. *CrossRef*
- Stake, R. E. (2008). Qualitative case studies.
- Stanbic bank. (2023). Investor relations. Retrieved from https://www.stanbicbank.co.ke/
- Syahputri, H. Y., & Kitri, M. L. (2020). Enterprise risk management analysis of group XYZ based on ISO 31000: 2018 framework. Asian Journal of Accounting and Finance, 2(3), 1-12.
- Tahir, I. M., & Razali, A. R. (2011). The relationship between enterprise risk management (ERM) and firm value: Evidence from Malaysian public listed companies. International Journal of economics and management sciences, 1(2), 32-41.
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212-233. *CrossRef*
- Tranchard, S. (2018). Risk management: The new ISO 31000 keeps risk management simple. Governance Directions, 70(4), 180-182.
- Wanjohi, J. G. (2013). The effect of financial risk management on the financial performance of commercial banks in Kenya (Doctoral dissertation, University of Nairobi).
- WEF. (2023). Global Risks Report 2023. Retrieved from https://www.weforum.org/
- Wicaksono, A. Y. (2020). Applying ISO: 31000: 2018 as a risk management strategy in the heavy machinery vehicle division. Journal homepage: https://journal. trunojoyo. ac. id/ijseit, 4(02). *CrossRef*
- Williamson, D. (2007). The COSO ERM framework: a critique from systems theory of management control. International Journal of Risk Assessment and Management, 7(8), 1089-1119. *CrossRef*
- Zhang, S., le Fever, H. T., & Le Zhang S, F. H. (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. Journal of Economics, Business, and Management, 1(4), 391-395.