Journal of Governance Risk Management Compliance and Sustainability https://doi.org/10.31098/jgrcs.v5i1.2665

Research Paper

Navigating Operational Risk: Developing Criteria for Operational Risk Management Maturity in the Wake of COVID-19

[1]Erika van der Westhuizen
[1] University of South Africa, South Africa

Received: April 19, 2024	Revised: December 19, 2024	Accepted: March 18, 2025	Online: March 30, 2025

Abstract

The COVID-19 pandemic has caused many organizations to suffer losses and even close due to being unprepared to manage the effects of such a deadly disease. This pandemic can be regarded as an external event that is an underlying risk factor for operational risk. Therefore, it is apparent that the losses and disruptions caused by COVID-19 can be directly linked to operational risk, meaning that any loss and damage can be attributed to a shortcoming in adequate operational risk control measures. Although many organizations were prepared in one way or another, it seemed uncertain at what level of risk maturity an organization would have adequate control measures in place for operational risk exposures. The research aimed to establish criteria for operational risk management maturity. The research followed a non-systematic literature review to evaluate various criteria within the framework of risk management. The literature review identified 30 criteria that can help organizations assess, develop, and benchmark their operational risk maturity. The concept of risk maturity can help organizations determine their level of risk resilience to cope with major operational risk events. Future research can be conducted to confirm the criteria and assess their applicability in various organizations.

Keywords: *operational risk; operational risk management framework; risk governance; risk culture; risk management process; risk management strategy*

INTRODUCTION

The global COVID-19 pandemic negatively influenced numerous organizations, causing some to permanently close their doors and others to take drastic measures to stay in business. On the other hand, many organizations proved to be resilient and could cope with the influences of the disaster. However, the pandemic mainly caused uncertainty and hightened reliance on technology, thereby increasing exposure to operational risks. According to the Basel Committee on Banking Supervision (BCBS) (2020), cyber threats spiked during the pandemic. Due to a greater reliance on virtual working environments, they increased the potential for operational risk events caused by people and failed processes and systems. Valsamakis et al. (2023) noted that the BCBS has proposed a globally accepted definition of operational risk as the risk of loss due to inadequate or failed internal processes, people, systems, or external events. Weeserik and Spruit (2018) defined operational risk as the ongoing management of risks arising from human actions, internal processes, systems, and external events. When analyzing this definition, it is apparent that although the COVID-19 pandemic is an external operational risk factor, it affects all factors, such as people, processes, and systems (technology). Since most organizations accept this definition of operational risk, managing the risk in terms of the underlying risk factors is important.

However, not all organizations operate at the same level of risk maturity, which could have influenced their preparedness to, for example, effectively deal with an event such as the COVID-19 pandemic, an external operational risk factor. In addition, Rasmussen (2020a) mentioned that organizations must go beyond the misleading concepts of risk and determine whether technology can meet the demands of their risk management maturity path. Organizations must clearly understand their current risk management and the levels that they want to achieve or maintain.

Corresponding author's email: bothae2@unisa.ac.za

Although various research on risk maturity models in enterprise and project management exists, organizations have no set criteria for measuring operational risk management maturity. This study aims to add value to an organization's risk management status by posing the following question: What are the criteria for operational risk management that can be used to determine its risk maturity and prepare an organization to be resilient during operational risk events?

In response to this question, this paper aims to find out the criteria required for an operational risk management maturity model that can be used to determine risk resilience in various organizations. However, as a starting point, it is essential to clarify the components of an operational risk management framework, which will serve as the basis for identifying the criteria for sound operational risk management. According to Coetzee and Lubbe (2013), a risk management framework concerns the totality of structures, processes, systems, people, and methodologies an organization can use for risk management. Triphathi (2013) posited that an operational risk management framework should be established in line with business processes and should reflect the fundamental operational complexities and overall operational risk profile. Blunden and Thirlwell (2013) stated that a risk framework could provide a structure for embedding operational risk management, while according to Naude and Chiweshe (2017), it can be regarded as a tool for providing the underlying components for an organization's risk management, including risk identification, assessment, mitigation and overall monitoring. A risk management framework forms the basis for risk management; however, it is important to establish the components of such a framework. As such, this research uses the components of a typical operational risk management framework as a platform to determine the criteria for operational risk management maturity. Therefore, the purpose of this article is to identify criteria for effective operational risk management that can serve as an indicator of risk maturity in managing operational risks.

The paper is organized as follows: following the introduction, the second part clarifies the operational risk management framework's conceptual framework. The third part outlines the methods used in this paper, followed by the results and discussion section. Finally, the paper reflects on the topics raised in the conclusion and provides suggestions for future research.

LITERATURE REVIEW

According to Weeserik and Spruit (2018), every organizational activity includes operational risk, and significant losses can result if these risks are not managed appropriately. IOR Webinar Videos (2018) noted that an effective framework needs to incorporate diverse components such as processes, communication, structure, culture, strategy, and human factors. Chapman (2011) inferred that a risk management framework should help organizations integrate risk management into their procedures to provide enough risk data to act as a basis for making decisions. Based on this view and the emphasis on decision-making, risk governance should form an operational risk management framework component. Young (2022) provided an overview of the typical components of an operational risk management framework, including risk management culture, strategy, structures, and risk management process. Moreover, Nuhić-Mešković (2023) posited that risk management must be a fundamental component of all organizational operations through an integrated risk management framework. Therefore, for this review, the components of a typical operational risk management framework include risk management culture, risk management strategy, risk governance structures and a risk management process.

Organizations, however, need a tool like the risk maturity model to identify and measure progress in these risk management improvements (Karunarathne & Kim, 2021; Hoseini et al., 2021). According to Hoseini et al. (2021), risk maturity means 'an evolution toward the full development of risk management processes' and provides the degree to which the process is

formalized and applied within various risk management activities. de Souza Feitos et al. (2021) posited that maturity models can guide organizations' improvement plans. Roghabadi and Moselhi (2020) further stated that risk maturity can assist organizations in identifying their strengths and weaknesses within the risk management process and taking the necessary steps for improvement. There are various risk maturity models, as highlighted by Hoseini et al. (2021). However, this research does not examine the maturity level of organizations in terms of these models. Instead, it provides a list of criteria organizations can use to measure their operational risk maturity. Future research could link the criteria to various risk maturity levels for organizations and industries.

RESEARCH METHOD

The article employed a literature review approach to examine operational risk maturity in South Africa. According to Kraus et al. (2022), a non-systematic literature review employs a deductive reasoning strategy in which the researcher first identifies a set of areas related to a topic and then consults the relevant literature to clarify and support scholarly findings in each area. A review of secondary sources, including academic articles, books, media articles, and other documents such as reports, policies and discussion papers, was conducted to establish the criteria required for operational risk management maturity. The study was supported by policies and reports from both national and international organizations on operational risk maturity. This method was chosen to analyze and synthesize primary research findings and provide additional insights, classifications, and frameworks on specific topics. The search used electronic databases such as Google Scholar, Scopus, and ResearchGate, which are among the most relevant information platforms for accessing significant publications on various aspects of operational risk management related to risk maturity. Thereafter, policy documents related to risk management were consulted, including King IV, ISO 31000, BCBS, COSO, and BIS.

According to a Scopus search of the criteria/terms ‘operational risk maturity’, no documents match these search terms. A Google Scholar search of these terms yielded 10 results, of which two were books. Most of the Google Scholar results were for the period 2011 to 2018. For this reason, the author used a range of documents published by academics and private organizations to avoid confining the investigation to some research articles. With various technological changes and external factors that influence operational risk maturity, organizations must have a set of guideline criteria to evaluate their operational risk maturity and be more prepared for future events. The components of the operational risk management framework served as a platform to determine the criteria for operational risk maturity, which included risk culture, risk strategy, risk governance structures and a risk management process.

FINDINGS AND DISCUSSION

There is a lack of clearly defined and agreed-upon criteria for organizations to measure their operational risk maturity. However, various studies have been conducted on the risk management framework and its importance for organizations. The framework forms an important starting point for establishing the criteria necessary for operational risk maturity. The components evaluated included risk culture, risk strategy, risk governance structures, and risk management process.

Risk Management Culture

Hillson (2013) stated that an organization requires a fully mature risk-awareness culture at all levels that must be supported and resourced. Establishing and implementing an operational risk definition that is part of a board-approved risk management policy is crucial to developing an operational risk management culture (Young, 2020). Corporate or organizational culture reflects its intended behaviors, ethics, values, beliefs, and risk perception (COSO 2017; Hac et al., 2021).

Therefore, achieving the organization's strategic objectives should be supported by an operational risk management culture. According to Chapman (2011), to support the achievement of an organization's strategic and business objectives, an approved risk policy should include the organization's declaration of the importance of managing risks. In this regard, Girling (2013) stated that it is important that the board approves a risk policy. Risk policies should also be reviewed whenever operational risk profiles change (BCBS, 2011). Rasmussen (2020b) posited that policies are critical because they establish boundaries of behavior for individuals, processes, relationships, and transactions.

According to the Institute of Operational Risk (IOR) (2019), a risk culture will ensure that staff accept the importance of operational risk management and behave in a manner consistent with the organization's operational risk policies, procedures, and appetite. According to Hillson (2012), a risk-aware culture can be established through a clear statement of intent that outlines the vision, risk policy, and the risk management process. This approach requires the involvement of top management, who should act as risk champions and communicate the seriousness of risk management throughout the organization. In addition, as the concept of risk management evolves, a risk culture will naturally emerge, ensuring that all necessary elements are in place to manage risks effectively, with adequate personnel, processes, and tools (Hillson, 2012). Hac et al. (2021) also noted that a risk culture reflects the values, beliefs, and norms surrounding risk, indicating how risk is perceived and managed; therefore, risk management maturity requires a robust risk culture. According to Chapman (2018), a risk management culture ensures that risk management is integral to all aspects of an organization's activities. Čech and Januška (2020) further showed that risk management influences every aspect and activity of an organization and can be used to ensure that the organization's objectives are achieved.

A risk culture forms a platform for effective operational risk management. Furthermore, establishing of an operational risk culture begins with defining operational risk. In addition, a risk culture must also incorporate values and attitudes toward risk management. According to Young (2022), a risk management culture requires a set of principles for managing operational risk and evaluating the value that risk management can add to the organization. However, developing and embedding these principles and experiencing the actual value of operational risk management will take time and is not a one-off instantaneous process. Finally, board approval of an operational risk management policy incorporating the risk culture is essential. Therefore, an effective risk management culture is supported by the following criteria:

- Approved and embedded definition of operational risk.
- A board-approved operational risk management policy.
- A set of principles and values to guide the management of operational risks.
- Management's active involvement at all levels is to embed a risk culture that reflects the organization's ethics, values, beliefs, and attitudes in managing operational risks.

Risk Management Strategy

An organization's strategic management process must incorporate elements of risk management. This should ensure that a business strategy and objectives can be approved at acceptable risk exposure levels. Strategic objectives are high-level goals that align with an organization's mission and vision, according to COSO (2017). When setting these strategic objectives, management should identify risks and potential implications to ensure that business objectives are considered and approved within acceptable levels of risks. The Federation of European Risk Management Association (FERMA) (2011) stated that risk management should be a continuous process that supports the development and execution of an organization's strategy.

Furthermore, determining the risk appetite during an integrated strategy and risk management process is essential. According to Girling (2013), an organization's risk appetite refers to the level of risk that it is prepared to assume. Determining the risk appetite is an important step in the strategic planning process. Establishing a realistic risk appetite for the organization is one of the main goals of a strategic management process. It can be assumed that an integrated strategic and risk management process is important for effective risk management. Therefore, the following criteria add value to a level of operational risk maturity:

- An integrated strategic and risk management process should determine the formulation of risk-based strategic objectives.
- A continuous risk management process should support the development and execution of the business strategy and objectives.
- An integrated strategic and risk management process should include a realistic operational risk appetite.

The Governance Structure for Risk Management

According to Kusumawardhani and Murdianingrum (2022), good corporate governance is a structure in which management and all stakeholders set the organization's objectives, with the means to achieve the goals and track the performance through an integrated process. David et al. (2021) also indicated that corporate governance can be used to govern and control organizational operations, increasing management transparency. Good governance requires allocating and managing resources to achieve organizational objectives (Masenya & Mthombeni, 2023). A Barnowl (2016) report on key changes in King IV (2016) posited that risk governance requires responsible bodies to manage risk in a way that aids the organization in establishing and accomplishing its strategic goals. Coetzee (2016) mentioned that every organization requires a different risk management structure, depending on its needs and business plan. This structure should encompass all levels of management that are involved in risk management. Nuhić-Mešković and Mešković (2023) noted that all employees, regardless of their management level, should be involved and understand their specific duties and responsibilities related to risk management. Therefore, risk management must include the roles and responsibilities necessary to ensure an effective risk governance framework. According to Young (2020), all role players must be aware of the duties and obligations of each line of defence to guarantee the efficacy of each function and prevent duplication.

Three lines of defence can be identified in operational risk governance: business management in the first line, risk management in the second, and internal audit in the third. In this sense, it is vital that the board appropriately mandates the key risk governance bodies, including the audit and risk committees, to perform their responsibilities for operational risk management. Risk governance structures are crucial for ensuring effective operational risk management. As such, the following criteria are identified as leading to risk maturity:

- Risk governance bodies should ensure risk management to support the achievement of strategic business objectives.
- Risk management structures should be established according to the organization's strategic needs.
- The roles and responsibilities related to risk management should be clearly defined and demarcated at all levels of management.
- All employees should be aware of their roles and responsibilities regarding risk management at all organisational levels.
- The board of directors should mandate the governance bodies involved in risk

management.

Risk Management Process

According to BCBS (2020), risk management involves identifying risks, measuring and assessing exposures, monitoring these exposures, taking steps to control or mitigate exposures, and reporting to top management. According to Van Wyk et al. (2008), a risk management process entails identifying, analyzing, mitigating, monitoring, and reporting risk. ISO 31000 (2018) posited that a risk management process is a systematic process applied to management policies, practices, and procedures to identify, analyze, evaluate, treat, monitor, and review risk. Girling (2013) further showed that an operational risk process incorporates identifying, assessing, monitoring, controlling and mitigating operational risks. Wieczorek-Kosmala (2013) further stated that the risk management process supports the growth of an organization and should be integrated into all decision-making areas. Based on these sources, it can be deduced that a risk management process should include risk identification, risk assessment, risk mitigation and control measures, and risk monitoring and reporting. Each component will be discussed to determine the tools available to an organization as part of an operational risk management process and identify relevant criteria for risk maturity.

Risk Identification

Moinzad et al. (2021) posited that risk identification aims to identify various risks that can affect the organization to achieve the organizational goals. This is supported by ISO 31000 (2018), which states that the identified risks could affect the achievement of an organization's business objectives. Nuhić-Mešković and Mešković (2023) mentioned that risk should be identified at all levels of the organization, which would allow for the identification and quantification of most risks as well as the interconnectedness between the various risks. Chapman (2011) argued that risk identification is a process that creates a series of risks and opportunities that can be included in a risk register. As part of the compilation of such a register, management should ensure that information on loss incidents is acquired throughout the organization using a Loss Incident Database (Kalyvas et al., 2006). Organizations can also use scenarios to identify risks, which is a means of obtaining professional opinion from experts that provides a rational evaluation of the probability and impact of potential operational losses (Kalyvas et al., 2006). Blunden and Thirlwell (2013) inferred that scenarios can also assist in building an understanding of an organization's limits when setting a realistic risk appetite. A Loss Incident Database and Scenarios are fundamental in identifying risks when compiling a risk register. Following the identification of risks, the subsequent phase involves conducting a comprehensive risk assessment.

Risk Assessment

According to ISO 31000 (2018), a risk assessment aims to assist in making decisions based on risk analysis results to determine which risks must be prioritized and treated. Moinzad et al. (2021) inferred that risk analysis should not only be used to decrease risks but also to identify opportunities to assist an organization in improving its performance. According to Croitoru (2014), risk assessments aim to determine vulnerable operations carried out according to the likelihood of occurrences and the potential financial impact on the organization. Paricio (2019) further stated that risk assessment could be used as a communication tool to support decision-making by translating data into usable information that aligns with organizational objectives. According to BCBS (2020), a sound risk assessment process will allow an organization to understand its risk profile better and allocate management resources and strategies. Risk assessments analyse

identified risks to determine the likelihood and impact of potential risks and possible business opportunities. Risk and Control Self-Assessments (RCSA) are tools available to assess risks. Girling (2013) stated that RCSA are used to identify and assess risks to control and mitigate unacceptable risks. Moinzad et al. (2021) further noted that risk control should be employed to develop an effective strategy for addressing identified risks and to evaluate the effectiveness of these strategies through ongoing reviews. In addition, Blunden and Thirlwell (2013) posited that RCSAs attempt to evaluate the number of risks and relevant control measures at the lowest levels. Therefore, an RCSA process can be assumed to be a bottom-up activity that includes all employees involved in the relevant business processes. The assessed risks should also be included in the risk register.

Risk Mitigation and Control Measures

According to Proença et al. (2017), all organizations are exposed to risks and uncertainty, and it is imperative that a well-organized risk control system be implemented. Risk mitigation is a strategy employed to avoid or reduce the impact of identified risks that may arise, aiming to reduce the losses due to risk (Henni et al., 2024). Young (2022) stated that risk control involves strategies to reduce the probability of loss. It seeks to minimize or eliminate the potential effects of the identified risk exposure. Olson and Wu (2008) stated that risk control involves implementing control measures to minimize the effects or avoid the consequences of risk events. In this regard, insurance is an important risk mitigation approach (Young, 2022). This valuable risk financing mechanism can be used to support the definition of the risk appetite. Other risk financing and risk control mechanisms include internal funding for smaller losses and capital allocation for high-impact loss events. In addition, Croitoru (2014) argued that risk control aims to change uncertainties into advantages for organizations with acceptable levels of risk exposure. Chapman (2011) inferred that risk control measures must be relevant regarding significant issues or events and associated with primary business objectives. Therefore, risk mitigation and control measures must be monitored continuously to ensure their effectiveness.

Risk Monitoring and Reporting

The BCBS (2020) posited that incorporating an appropriate control monitoring framework facilitates a structured approach to the evaluation, review, and ongoing monitoring and testing of controls. According to ISO 31000 (2018), risk monitoring should be planned to ensure effective risk mitigation and control measures. Chapman (2011) stated that the primary goal of risk monitoring is to observe the functioning of risk control actions and to serve as a guide for proactive management intervention. Deloitte (2019) mentioned that ongoing risk assessments can lead to continuous risk monitoring throughout an organization to monitor and alert management to emerging risks. According to Young (2020), the risk monitoring process will be sufficient if it satisfies the following objectives:

- Development of warning indicators.
- Monitoring of internal and external environments to ensure the determination of various risks and opportunities.
- The timeous implementation of responses to risks and opportunities.
- Continuous updating of risk registers with changing circumstances and related actions.
- Reporting on risk management initiatives to assess the progress made regarding the success or failure of these initiatives.

According to the BCBS (2020), operational risk data and risk and control assessments can be used to develop metrics to assess and monitor risk exposures. These metrics can, for example, serve

as indicators. Tripathi (2013) noted that the outcome of a risk identification and evaluation process is probably one of several risk indicators that may help with ongoing operational risk monitoring. Chapman (2011) suggested that risk indicators should be used to facilitate regular assessments and monitoring of risk exposures and to mitigate responses. According to Girling (2013), Key Risk Indicators (KRIs) are a management tool that can predict a change in risk exposures that could require proactive intervention. COSO (2017) stated that when a risk manifests, KRIs should be reported to the organizational levels that are most suited to handle its emergence. A risk report sent to management for decision-making should be based on a comprehensive monitoring process (ISO 31000, 2018).

According to the BCBS (2020), appropriate risk reporting mechanisms should be in place at all management levels to support the proactive management of operational risks. Makiwane and Padia (2012) stated that risk management is essential to corporate governance, specifically aimed at identifying threats and proactively taking appropriate action to protect the organization. As such, timely and accurate risk reports are crucial for management. According to Hain (2009), effective risk reporting can be achieved through sound risk management which depends on employee support and a willingness to provide adequate and accurate information. In addition, it is essential to ensure that risk information is adequately reported and used for decision-making at all relevant organizational levels (ISO 31000, 2018). Risk reporting plays a fundamental role in risk management, and ensuring adequate and accurate risk information for decision-making is crucial. When dealing with a risk management process as a component of an operational risk management framework, the following criteria can be derived to determine the level of risk maturity:

- An operational risk management process should be developed and embedded in an operational risk management framework.
- A risk identification process should be included in a risk management policy approved by the board of directors.
- A risk management process should include a risk identification process to identify risks that could influence the achievement of business objectives.
- A risk identification process should include an analysis of business processes to identify risks.
- The risk identification process should include the identification of business opportunities.
- The identified risks should be included in the risk register.
- A risk identification process should include using a Loss Incident Database.
- The risk identification process should include scenarios to determine potential future risks.
- A risk management process should include an assessment of identified risks to determine their likelihood and potential impact on the business.
- Risk assessments should involve risk and control self-assessments.
- Risk mitigation and control measures should aim to reduce or eliminate the potential effects of a risk event.
- Risk control measures should be significant and associated with business objectives.
- Risk financing mechanisms (insurance, self-funding, and capital allocation) should be used for risk mitigation.
- Risk monitoring should ensure continuous testing of control measures.
- Risk monitoring should provide information to guide proactive management interventions.
- Risk monitoring should use key indicators to determine potential threats and ensure proactive intervention.
- A risk reporting process should be an integral part of a risk management process.
- Risk reporting should be in place at all management levels to ensure appropriate actions to

protect the organization.

- Risk reports should provide adequate risk information for risk-based decision-making.

This section is relevant to dealing with the components of an operational risk management framework because it identifies potential criteria that can be used to determine an organization's risk maturity. Although the identified criteria, based on the literature, cannot be seen as an exhaustive list, they may provide a solid platform for organizations to establish risk management maturity. Table 1 outlines a non-exhaustive list of criteria derived from the literature review, which can serve as a platform to determine an organization's operational risk maturity status.

Table 1. Criteria for Levels of Operational Risk Management Maturity

#	Criteria for Operational Risk Management Maturity
1	An operational risk management framework serves as the foundation for the basis for an operational risk maturity model.
2	The definition of operational risk is approved and embedded in the organization.
3	An operational risk management policy has been approved by the board.
4	A set of principles and values is established to guide the management of operational risks.
5	An integrated strategy and risk management process can determine the formulation of risk-based objectives.
6	A continuous risk management process supports the formulation and execution of the organization's strategy and business objectives.
7	An integrated strategy and risk management process results in a realistic operational risk appetite.
8	Risk management structures are established according to the strategic needs of an organization.
9	Roles and responsibilities related to operational risk management are clearly defined and demarcated at all levels of management.
10	All employees are aware of their roles and responsibilities related to managing operational risks.
11	The board mandates governance bodies involved in risk management.
12	A risk management process is part of an operational risk management framework.
13	A risk identification process is included in a risk management policy approved by the board.
14	A risk management process includes risk identification to identify risks that could influence the achievement of business objectives.
15	The risk identification process includes analysis of business processes to identify risks.
16	The risk identification process identifies business opportunities.
17	Identified risks are included in the risk register.
18	The risk identification process includes the use of a loss incident database.

#	Criteria for Operational Risk Management Maturity
19	The risk identification process involves creating scenarios to identify potential future risks.
20	A risk management process includes the assessment of identified risks to determine their likelihood and potential impact on the business.
21	Risk and control self-assessments are performed to assess risks.
22	Risk mitigation and control measures are used to eliminate or reduce the potential effects of a risk event.
23	Risk control measures are significant and are associated with business objectives.
24	Risk financing mechanisms, including allocation (insurance, self-funding, and capital allocation) are employed, for risk mitigation.
25	Risk monitoring ensures continuous testing of control measures.
26	Risk monitoring provides information to guide proactive management interventions.
27	Risk monitoring uses Key Risk Indicators to determine potential threats and facilitate proactive interventions.
28	Risk reporting is an integral part of risk management processes.
29	Risk reporting is in place at all management levels to ensure appropriate action to protect the organization.
30	Risk reports provide adequate risk information for risk-based decision-making.

A mature risk culture can be linked to successful risk management by adopting consistent behaviour in risk management procedures at all organizational levels. The literature review on risk management culture revealed four criteria that support effective risk management and should form part of operational risk maturity. These include having an approved and embedded operational risk definition, as Young (2020) supported. The second criterion is a board-approved operational risk management policy. This was supported by Chapman (2011), Girling (2013), and Rasmussen (2020b), who indicated that policies are crucial in establishing behavioral boundaries. The third criterion is for organizations to have principles and values guiding operational risk management. These guidelines reflect the values, beliefs, and norms about risk and how risk is perceived and managed (Hac et al., 2021). Under risk management culture, another criterion is for management to be actively involved at all levels to embed a risk culture. This will ensure that risk management is integral to all aspects of an organization (Chapman, 2018). Top management, especially the board, must create a strong risk management culture to guarantee that risk policies are regularly examined, revised, and integrated into the organization. Therefore, staff members must recognize the value of risk management, and organizations must provide the necessary tools, personnel, and resources to incorporate this culture into day-to-day operations.

Organizations can set risk-based strategic objectives and help management align risk appetite with strategic goals through a well-integrated risk management strategy. The second component that was evaluated was the risk management strategy. Under this component, the literature reveals three criteria for operational risk maturity. The first criterion is to form risk-based strategic objectives through an integrated strategic and risk management process. These strategic objectives are high-level goals aligned with an organization's mission and vision (COSO, 2017) and should be used to set risk parameters. The second criterion is to develop and execute the

business strategy and objectives through a continuous risk management process (FERMA, 2011). The third criterion under risk management strategy is to set a realistic operational risk appetite. The risk appetite is the amount of risk an organization is willing to take (Girling, 2013), and this should align with the organization's strategic objectives. Managing strategic decisions while continuously assessing risks guarantees the organization's risk appetite is realistic and aligned with the objectives. Management must review these strategies regularly to adapt their response to emerging risks.

The governance structures enable organizations to administer, manage and report risks effectively. The third component addresses governance structures for risk management, encompassing five criteria that should form part of operational risk maturity. The first two criteria, as supported by King IV (2016), require risk governance bodies to ensure risk management aligns with strategic business objectives and for the risk management structure to be established based on these objectives. The next two criteria are to have clear roles and responsibilities for risk management and to ensure that all employees know these roles to manage risk efficiently (Coetzee, 2016). The fifth criterion is that the board of directors should clearly mandate governance bodies' involvement in risk management. The governance structure helps management set clear role allocation and accountability within the organization. Employees across the organization need to understand their duties in relation to risk management; this can be achieved through regular communication and training.

The risk management process should be continuous and systematic to guide management in decision-making. The last component evaluated was the risk management process. Some identified criteria included a risk identification process that included a risk register, the use of incident databases, and scenarios to determine potential future risks. Additional criteria include significant risk controls associated with business objectives and monitoring risks to guide proactive management interventions (Makiwane & Padia, 2012). The final criterion has risk reports that provide adequate information for risk-based decision-making (Hain, 2009). The risk management process requires organizations to identify, assess, and monitor risks continuously to allow them to foresee potential risks and intervene proactively. Therefore, timely reporting of risks at all levels is necessary for making informed decisions.

CONCLUSIONS

This review paper highlights criteria that can assist organizations in effectively mapping and evaluating their operational risk management maturity. Various risk maturity models primarily focus on enterprise or project risk maturity; however, an effective risk maturity model for operational risk requires more detailed research and development. Operational risk maturity will help organizations assess their current risk management strengths and weaknesses. Organizations can follow the following steps for implementation: Create a risk-aware culture, incorporate top management into the risk process, establish a realistic risk appetite, and monitor risks using various tools and metrics. Through these steps, organizations can develop a mature operational risk management framework that supports strategic goals and objectives and long-term sustainability. This research offers a list of criteria that should help organizations assess, develop, and benchmark operational risk maturity. Such a model is essential for organizations to be more prepared for unforeseen events like the COVID-19 pandemic. The evaluation of various articles, policies, and regulations highlights that the 30 criteria identified in risk culture, risk strategy, risk governance structures, and risk management process should assist organizations in having a more holistic view of their status regarding operational risk maturity. Organizational risk management practices must constantly evolve and adapt to emerging risks, new tools, and technology.

LIMITATION & FURTHER RESEARCH

Although this study highlights the importance of various criteria for operational risk management maturity, it primarily focuses on a literature review. The recommendation for future research is for these criteria to be empirically tested for their importance as part of an operational risk maturity model and their applicability within different organizations and industries. The criteria can then be adjusted and updated to serve as a platform to develop an operational risk maturity model that will optimally evaluate various organizations' operational risk management maturity and indicate potential areas for improvement to be resilient toward major risk events.

REFERENCES

Barnowl. (2016). Key changes in King IV. *King IV Report: Risk, Compliance and Assurance*. BARNOWL Insights,chttp://www.barnowl.co.za/insights/king-iv-report-risk-compliance-and-assurance/

Basel Committee on Banking Supervision (BCBS). (2011). *Principles for the sound management of operational risk management*. Bank for International Settlements.

Basel Committee on Banking Supervision (BCBS). (2020). *Principles for operational resilience: A consultative document*. Bank for International Settlements.

Blunden, T., & Thirlwell, J. (2013). *Mastering operational risk: A practical guide to understanding operational risk and how to manage it* (2nd ed.). Pearson UK.

Cavalcante de Souza Feitosa, I. S., Ribeiro Carpinetti, L. C., & de Almeida-Filho, A. T. (2021). A supply chain risk management maturity model and a multi-criteria classification approach. *Benchmarking: An International Journal, 28*(9), 2636-2655. https://doi.org/10.1108/BIJ-09-2020-0487

Čech, M., & Januška, M. (2020). Evaluation of risk management maturity in the Czech automotive industry: Model and methodology. *Amfiteatru Economic, 22*(55), 824-845. http://dx.doi.org/10.24818/EA/2020/55/824

Chapman, R. (2011). *Simple tools and techniques for enterprise risk management* (2nd ed.). John Wiley & Sons.

Chapman, R. (2018). Ineffective risk management and the collapse of Carillion. *PM World J, VII*(XII), 1-16.

Coetzee, G. P., & Lubbe, D. (2013). Risk maturity of South African private and public sector organizations. *South African Journal of Accountability and Auditing Research, 14*(1), 45-56. https://hdl.handle.net/10520/EJC132262

Coetzee, P. (2016). Contribution of internal auditing to risk management: Perceptions of public sector senior management. *International Journal of Public Sector Management, 29*(4), 348-364. https://doi.org/10.1108/IJPSM-12-2015-0215

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*.https://aaahq.org/portals/0/documents/coso/coso_erm_2017_main_v1_20230815.pdf

Croitoru, I. (2014). Operational risk management and monitoring. *Journal: Internal Auditing and Risk Management, 4*(3), 21-31.

David, C. Y. N., Chang, Y. W., & Cheng, L. S. (2021). Corporate governance mechanisms with firm performance: A study of Malaysia's and Hong Kong's real estate investment trust (REITs) public listed companies. *Journal of Governance, Risk, Compliance, and Sustainability, 1*(1), 61-74. https://doi.org/10.31098/jgrcs.v1i1.511

Deloitte. (2019). *Internal audit insights 2019: High-impact areas of focus*. Deloitte US. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-ia-high-impact-areas-of-focus.pdf

Federation of European Risk Management Association (FERMA). (2011). *A structured approach to enterprise risk management and the requirements of ISO 31000*. https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

Girling, P. (2013). *Operational risk management: A complete guide to a successful operational risk*

framework. John Wiley & Sons.

Hac, L. D., Huy, D. T. N., Thach, N. N., Chuyen, B. M., Than, T. D., Nhung, P. T. H., Thang, T. D., & Anh, T. T. (2021). Enhancing risk management culture for sustainable growth of the Asia Commercial Bank (ACB) in Vietnam under mixed effects of macro factors. *Entrepreneurship and Sustainability Issues, 8*(3), 291-307. http://doi.org/10.9770/jesi.2021.8.3(18)

Hain, S. (2009). Managing operational risk: Incentives for reporting and disclosure. *Journal of Risk Management in Financial Institutions, 2*(3), 284-300. https://doi.org/10.69554/WSYT6337

Henni, H., Pramestari, D., Dinariana, D., Suryani, F., Sujatini, S., & Arby, A. I. (2024). Development of supply chain risk mitigation to develop an effective strategy for small and medium enterprises. *Logistic and Operation Management Research (LOMR), 3*(1), 17-27. https://doi.org/10.31098/lomr.v3i1.1553

Hillson, D. (2012). *Developing a risk culture: First or last?* https://risk-doctor.com/wp-content/uploads/2020/06/67-Risk-culture-first-or-last.pdf

Hillson, D. (2013). Prerequisites for effective enterprise risk management. *PM World Journal, 2*(2), 1-3. https://pmworldlibrary.net/wp-content/uploads/2013/09/pmwj7-feb2013-hillson-effective-enterprise-risk-management-series-article.pdf

Hoseini, E., Hertogh, M., & Bosch-Rekveldt, M. (2021). Developing a generic risk maturity module (GRMM) to evaluate risk management in construction projects. *Journal of Risk Management, 24*(7), 889-908. https://doi.org/10.1080/13669877.2019.1646309

Institute of Operational Risk. (2019). *Risk culture: Operational risk sound practice guidance*. Institute of Risk Management. https://www.ior-institute.org/sound-practice-guidance/risk-culture-2/

IOR Webinar Videos. (2018). Best practices for designing and implementing an effective operational risk framework [Video]. YouTube. https://www.youtube.com/watch?v=KGUjCCfKjac

International Standards Organization (ISO). (2018). *Risk management guidelines (ISO Standard No. 31000:2018(en))*. www.iso.org

Kalyvas, L., Akkizidis, I., Zourka, I., & Bouchereau, V. (2006). *Integrating market, credit, and operational risk: A complete guide for bankers and risk professionals*. Risk Books Incisive Financial Publishing.

Karunarathne, B. V. G., & Kim, B. (2021). Risk management application-level analysis in South Korea construction companies using a generic risk maturity model. *KSCE Journal of Civil Engineering, 25*(9), 3235-3244. https://doi.org/10.1007/s12205-021-2277-x

King IV. (2016). *King IV Report on Corporate Governance for South Africa 2016*. Institute of Directors in Southern Africa. https://www.iodsa.co.za/page/king-iv

Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., Mukherjee, D., Corvello, V., Piñeiro-Chousa, J., Liguori, E., Palacios-Marqués, D., Schiavone, F., Ferraris, A., Fernandes, C., & Ferreira, J. J. (2022). Literature reviews as independent studies: Guidelines for academic practice. *Review of Managerial Science, 16*, 2577-2595. https://doi.org/10.1007/s11846-022-00588-8

Kusumawardhani, I., & Murdianingrum, S. L. (2022). The effect of institutional ownership, managerial ownership, and delayed tax expenses on earnings management. *Journal of Governance, Risk Management, Compliance, and Sustainability, 2*(1), 1-9. https://doi.org/10.31098/jgrcs.v2i1.801

Makiwane, T., & Padia, N. (2012). Evaluation of corporate integrated reporting in South Africa post King III release South Africa–an exploratory enquiry. *Journal of Economic and Financial Sciences, 6*(2), 421-438. https://doi.org/10.4102/jef.v6i2.268

Masenya, M. J., & Mthombeni, A. (2023). Governance, ethics, and public service delivery: The ramifications of corruption. *Journal of Governance, Risk Management, Compliance and Sustainability, 3*(2), 39-48. https://doi.org/10.31098/jgrcs.v3i2.1893

Moinzad, H., Torakh, M. J., & Taghavifard, M. T. (2021). An approach to simultaneously assess operational risk and maturity levels in information technology management. *Journal of Operational Risk, 16*(2), 1-29. http://dx.doi.org/10.21314/JOP.2021.001

Naude, M. J., & Chiweshe, N. (2017). The proposed operational risk management framework for small and medium enterprises. *South African Journal of Economic and Management Sciences,*

20(1), a1621. https://doi.org/10.4102/sajems.v20i1.1621

Nuhić-Mešković, M., & Mešković, A. (2023). Risk management culture, structure, and process: Theoretical insights and empirical evidence. *International Business Research, 16*(10), 10-23. http://dx.doi.org/10.5539/ibr.v16n10p10

Olson, D. L., & Wu, D. D. (2008). *Enterprise risk management*. World Scientific.

Paricio, H. (2019). Risk-based approach in maintenance planning in the context of road and railway infrastructure. In *IABSE Symposium: Toward a Resilient Built Environment – Risk and Asset Management*. https://doi.org/10.1080/10168664.2019.1624344

Proença, D., Estevens, J., Vieira, R., & Borbinha, J. (2017, July 24-27). Risk management: A maturity model based on ISO 31000. 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece. http://dx.doi.org/10.1109/CBI.2017.40

Rasmussen, M. (2020a). *Rethinking risk management RFP requirements*. The GRC Pundit Blog.

Rasmussen, M. (2020b). *Why policies, and policy management matters*. The GRC Pundit Blog.

Roghabadi, M. A., & Moselhi, O. (2020). A fuzzy-based decision support model for risk maturity evaluation of construction organizations. *Algorithms, 13*(5), 115. https://doi.org/10.3390/a13050115

Tripathi, A. (2013). A model framework for measuring and managing operational risks in treasury operations in financial institutions. [Thesis Birla Institute of Technology and Science, Pilani] India. http://dx.doi.org/10.2139/ssrn.3049173

Valsamakis, A. C., Vivian, R. W., Du Toit, G. S., & Young, J. (2023). *Risk management* (5th ed.). Maskew Miller Learning.

Van Wyk, R., Bowen, P., & Akintoye, A. (2008). Project risk management practice: The case of a South African utility company. *International Journal of Project Management, 26*(2), 149-163. https://doi.org/10.1016/j.ijproman.2007.03.011

Weeserik, B. P., & Spruit, M. (2018). Improving operational risk management using business performance management technologies. *Sustainability, 10*(3), 640. https://doi.org/10.3390/su10030640

Wieczorek-Kosmala, M. (2013). Risk management practices from a risk maturity model perspective. *Journal of East European Management Studies, 19*(2), 133-159. https://doi.org/10.1688/JEEMS-2014-02-Wieczorek-Kosmala

Young, J. (2020). Determinants for a risk-based audit of an operational risk management framework: A South African approach. *Academy of Accounting & Financial Studies Journal, 24*(2), 1-19. https://www.abacademies.org/articles/determinants-for-a-riskbased-audit-of-an-operational-risk-management-framework-a-south-african-perspective-9168.html

Young, J. (2022). *Operational risk management* (3rd ed.). Van Schaik.