Enterprise risk management: The maturity model for the ISO 31000 adopters

Franciskus Antonius Alijoyo[1], Ridwan Hendra[2,*], and Kevin Bastian Sirait[2]

[1]*Faculty of Economics, Parahyangan Catholic University, Indonesia*

[2]*Center for Risk Management and Sustainability, Indonesia*

Abstract

This paper aims to examine and shed light on the essential criteria for assessing the organization's enterprise risk management (ERM) maturity and test whether the existing ERM maturity models have fulfilled those criteria, both of the non-ISO 31000 based and the ISO 31000 based version. A literature review is conducted to identify, analyze and validate the essential criteria that should be considered when an organization exercises its ERM maturity assessment. Those criteria are then mapped against the elements of existing risk management maturity models, which are grouped as non-ISO 31000 and ISO 31000 based models. In using the mapping result, further analysis is made to understand the reason and argumentation if one or more of the essential criteria is absent or additional or alternative criteria infused into the model. The literature review discovers seven criteria that are considered essential in measuring an organization's ERM maturity. However, the mapping produces a result that shows that those seven essential criteria are not fully reflected or practically used by the existing ERM maturity models of the non-ISO 31000 and the ISO 31000. Whereas there is no explanation of the missing criteria in the non-ISO 31000 based model, a well-noted argumentation is made that relates to the ISO 31000 based model. As such, the ISO 31000 based risk management maturity model put forward an argumentation that is basically in line with the underlying reasoning of ISO 31000 standard itself, which emphasizes its generic features as a standard (i.e., regardless of the size).

Keywords: Enterprise risk management, risk management maturity, ISO 31000

1. Introduction

Enterprise risk management (ERM) has a critical role in creating and protecting the organization's value. Although the role of ERM is straightforward, the necessity for its implementation has become more apparent due to the 2008 financial crisis, in which a poorly managed risk has manifested into chains of detrimental situations that affected both of the organization's financial and non-financial aspects. Fraser and Simkins (2010, p. 27) pointed out that one of the reasons for such occurrence is the failure of conventional risk management practice. Naturally, it has pushed the concept where risks cannot solely be managed and mitigated through the traditional practice of risk

management (i.e., silo-based approach) due to the interdependent nature of the risk itself (Farrell & Gallagher, 2015).

Since then, the concept and the role of ERM have been evolved to be implemented holistically. In other words, ERM has been developed to operate within an integrated framework to manage the risk's interdependent nature, shaping the organization's perspective to become more forward-looking and embed the idea of risk management into the organization's objectives formulation and decision- making process (Lechner & Gatzert, 2018; McShane et al., 2011). Due to the increase of demands and needs for an integrated ERM, the International Organization for Standardization (ISO, 2009) has published a standard entitled "Risk management – Principles and Guidelines" (i.e., ISO 31000:2009) in 2009. The purpose of the ISO 31000:2009 is to help the organization build an integrated ERM, imbue the ERM concepts within its corporate governance mechanism, and add value to its strategic decision-making process.

Furthermore, the ISO 31000:2009 encourage each of its adopters to adjust its ERM mechanism and process to match with its business activities, culture, and values under the three fundamental components of the standard (i.e., the principles, the framework, and the process of ERM) rather than solely enforcing the best practice of risk management (Dali & Lajtha, 2012). As a result, the ISO 31000:2009 standard does not have the trait of "one-size-fits-all" where the implementation of an integrated ERM are different among its adopters, and each of the adopters has its distinct challenges in reconciling and consolidating the ISO 31000:2009 components within its activities to create and protect its value.

After the use of almost ten years, ISO (2018) has published the second edition of the standard in 2018 entitled "Risk management – Guidelines'" (i.e., ISO 31000:2018). Accordingly, the significant changes within the ISO 31000:2018 standard are the simplification of the terminologies and the definition of risks along with the ERM framework and process. Moreover, it is still upholding the same three fundamental components of the previous edition of the ISO 31000 in building and implementing an efficient, effective, and integrated ERM. Thus, the ISO 31000:2018 is more comprehensive than its previous edition, which includes the strategic vision of ERM to the risk practitioners and articulates the principles and approach of ERM on a granular level (Silva Rampini et al., 2019).

Despite the effort ISO has made, it still has not addressed the gap between the adopter's ERM implementation and its ERM effectiveness. Specifically, the need for the ERM maturity model for the ISO 31000 adopters. This issue emerged due to no available guidelines or details concerning the execution of risk maturity strategies since the introduction of the ISO 31000 standard (Antonucci, 2016 p. 53). Hence, little is known about the ERM maturity model that is designed under the specification of the ISO 31000 standard in assessing the organizations or its adopters' ERM maturity level.

Following the introduction above, the purpose of this research is to explore the existing ERM maturity models that are suitable for the adopters of the ISO 31000 standard with two objectives. Namely, (1) to examine and shed light on the essential

criteria for assessing the organization's enterprise risk management (ERM) maturity and (2) to test whether the existing ERM maturity models have fulfilled those criteria, both the non-ISO 31000 based and the ISO 31000 based version.

This research's findings should provide the risk practitioners with a greater understanding in assessing an organization's ERM maturity level, especially the ERM maturity level of the ISO 31000 adopters. Furthermore, it also provides the criteria that the risk practitioners can use in determining the most influential factor that contributes to the effectiveness of the organization's ERM practice that is relevant to its distinct characteristics and the nature of its industry.

2. Research method

In uncovering the essential criteria in measuring the organization's ERM maturity, the integrative literature review approach is applied. The application of an integrative literature review enables the activities of assessing and synthesizing the literature on the predetermined topic for creating a new theoretical framework and perspective (Snyder, 2019). In which, through the process of problem identification, literature search, data evaluation, data analysis, and presentation in accordance to the integrative literature review (Whittemore & Knafl, 2005), the literature that has the highest relevancy to the topic of ERM and the criteria that influence its effectiveness can be pinpointed. Therefore, in uncovering the essential criteria for assessing the ERM maturity level of the adopters of ISO 31000:2018 standard, it follows the four steps below.

First, by using the steps of an integrative literature review, the previous studies that focused on the criteria that significantly influence the effectiveness of the organization's ERM are analyzed. As such, it is to explore the interconnection between the organization's ERM process with its characteristics. In particular, the relationship between the implication of the changes within its internal and external environments to ERM implementation within the organization and its risk management effectiveness. As explained by Mikes and Kaplan (2014) and Power (2009), the organization's ERM process is dependent on the controllability and the interconnectedness of the risks it faces. As a result, the determination of these criteria is to uncover the association between the organization's capacity to realize an integrated ERM implementation and the nature of the risks that originate either internally or externally, along with the inclusion of these criteria in the assessment of the organization's risk management maturity within the ERM maturity model.

Second, in relation to the criteria which are associated with the effectiveness of the organization's ERM, it is then compared to the components from the existing ERM generic maturity models that are widely used. Specifically, the ERM maturity models of interest are the model developed by Chapman (2011, Appendix 6), Hillson (1997), and the Risk and Insurance Management Society (RIMS, 2006). In this regard, the discrepancy between the ERM criteria and the criteria within the ERM maturity model can be determined.

Third, concerning the ISO 31000 standard, the comparison between the criteria that have the capabilities to influence the organization's ERM effectiveness and the three main components of the ISO 31000:2018 standard (i.e., principles, framework, and process) is conducted. Specifically, the ERM maturity model developed by the Enterprise Risk Management Academy (ERMA, 2020) is used as the primary reference for comparison as it explicitly confirms that ISO 31000:2018 is used as their reference. It acts as the basis for determining the essential criteria in assessing the organizations and the ISO 31000:2018 standard adopters' ERM maturity. For the sake of maintaining consistency with the current edition of the ISO 31000 standard, any ERM maturity model that uses the first edition of the standard (i.e., ISO 31000:2009) are excluded from the analysis. Accordingly, the terminology, framework, and process defined by ISO (2018) are used to maintain consistency along with the references to the corporate governance mechanism, internal control, audit committee, and the availability of resources, which is construed as the primary foundation for the principles and the concepts to be embedded within the organization's culture and activities.

Lastly, the potential inclusion that can be made to the ERM maturity model under the ISO 31000:2018 standard to enhance the organization and the standard adopters' ERM maturity assessment. It uses the findings regarding the existence of the identified essential criteria within the selected ERM maturity model in general and the ERM maturity model explicitly designed under the ISO 31000:2018. Moreover, the findings regarding the existence of the identified essential criteria within the three fundamental components of ISO 31000:2018 standard are also used to determine the potential criteria that can be included within the ERM maturity assessment.

3. Findings and discussions

3.1. The essential criteria of ERM maturity assessment

The literature review produces a finding that there are seven essential criteria of ERM maturity assessment. The findings regarding the criteria that significantly influence the effectiveness of the organization's ERM are summarized in Table 1. The determined seven criteria are oriented on the organization's capability and capacity in adapting its internal ERM process to the changes that occurred externally. Also, it is dependent on the organization's capability in ensuring the adequate amount of resources (i.e., financial and human capital resources) in maintaining the operability of its ERM process and the utilization of its corporate governance mechanism and audit committee in providing the support to the organization's ERM mechanism in identifying and managing the risks that are originated from its internal and external environment.

Table 1: The theoretical base of the seven criteria of ERM effectiveness

Author	EC	IC	GM	AC	RA	FS	FC
Baxter et al. (2013)			✓		✓		
Cohen et al. (2017)			✓	✓			
Doyle et al. (2007)			✓	✓	✓	✓	✓
Elahi (2013)	✓	✓			✓		✓

Author	EC	IC	GM	AC	RA	FS	FC
Gatzert and Martin (2015)				✓		✓	
Gordon et al. (2009)	✓	✓	✓	✓	✓	✓	✓
Kaplan and Mikes (2012)	✓	✓	✓			✓	✓
Kleffner et al. (2003)		✓	✓			✓	
Lechner and Gatzert (2018)		✓		✓		✓	
McShane et al. (2011)				✓		✓	
Mikes and Kaplan (2014)	✓		✓	✓	✓		
Paape and Speklé (2012)			✓	✓		✓	
Spira & Page (2003)			✓	✓			

Notes: EC = Environmental Uncertainty, IC = Industry Competition, GM = Governance Mechanism, AC = Audit Committee, RA = Resource Availability, FS = Firm Size, FC = Firm Complexity

As shown in Table 1, the effectiveness of the organization's ERM is dependent on its capability and capacity in becoming aware of the uncertainty that exists within surroundings and adjusts its internal process accordingly to manage the impact that arises from it. As such, the seven identified criteria are oriented to the organization's internal performance in conducting risk management activities.

As for the first criteria of ERM effectiveness, it is the environmental uncertainty. The criterion of environmental uncertainty focuses on the organization's external changes (e.g., regulatory changes and market movement).

The second criteria of ERM effectiveness are the level of competition within the organization's industry (i.e., industry competition). This criterion focuses on the concentration level of the industries in which the organization is operated. In other words, the more concentrated the industries, the less competition that the organization has to face. Accordingly, taken into account the similarities between the criteria of environmental uncertainty and industry competition, the organization's capability in obtaining the information on the dynamic changes within its surroundings contributes to the effectiveness of its ERM, which can be used to adjust the organization's risk-oriented perspective and approach in identifying and mitigating the external risks. While also enabling the organization to make and take a strategic risk-based decision to obtain a competitive advantage within its industry.

In regards to the third and fourth criteria of ERM effectiveness, it is the organization's governance mechanism and audit committee. The criterion of governance mechanism focuses on the quality and the performance of the organization in ensuring the operability and the effectiveness of its ERM process. Meanwhile, the criterion of the audit committee, it is focusing on the committee's commitment and the responsibilities in supervising the qualities of the deployment of ERM within the organization, along with its capabilities in ensuring the transparency of the organization's ERM effectiveness and maintaining an adequate flow of risk-related information in order to prevent information asymmetry between the organization's management and its stakeholders. Besides, it also includes the audit committee's performance in complementing the organization's ERM process in terms of identifying and managing risks while at the same time ensuring the risk management approach that is applied align with its risk appetite and the value of the organization.

Lastly, in terms of the last three criteria of ERM effectiveness, it is the firm size, firm complexity, and resource availability. These three criteria are associated with the characteristics of the firm. The orientation of the criterion of the firm size is the scale of operations and the number of assets it has. On the other hand, the criterion of firm complexity focuses on the number of business segments within the firm. These two criteria imply that it determines the scale of ERM implementation within the organization in managing the risks that inherently exist within its business activities and dictates the number of resources for supporting its ERM process, which is dependent on the scale of the organization. Concerning these two criteria is the resource availability criterion. It is oriented on the organization's flexibility and capability to allocate the necessary resources (i.e., financial and human capital resources) for its ERM activities with respect to the constraints that exist within the firm. Consequently, the bigger the organization's size and the more complex its activities, the higher the resources required for the organization to allocate in maintaining the operability of the organization's ERM process and the level of its ERM effectiveness.

3.2. The criteria within the existing ERM maturity model

Overall, the inclusion of the seven criteria of ERM effectiveness within the predetermined ERM maturity models is presented in Table 2. Although there is a gap among the ERM maturity models in terms of the year of its creation, the similarities between all the selected ERM maturity models cover the criterion of environmental uncertainty, audit committee, governance mechanism, and resource availability. Moreover, it is concentrated on measuring the level of integration and the holistic of the ERM process on the organization's activities and its alignment with its value and strategic objectives. Thus, within these three ERM maturity models, it considers the value, role, and applicability of ERM in shaping the risk-oriented culture, decision-making, and mechanism within the firm.

Apart from the similarities shown in Table 2, not all criteria of ERM effectiveness are included within the maturity model. Nonetheless, it is found that the ERM maturity model of ERMA (2020) and RIMS (2006) has the highest inclusion of the essential criteria of ERM effectiveness. Nonetheless, the criterion of firm size is not presented within the four models.

Table 2: The inclusion of essential risk management criteria within the ERM maturity models

Criteria	Non-ISO 31000 based			ISO 31000-based
	Chapman (2011, Appendix 6)	Hillson (1997)	RIMS (2006)	ERMA (2020)
Environmental uncertainty	✓	✓	✓	✓
Industry competition			✓	✓
Governance mechanism	✓	✓	✓	✓
Audit committee	✓	✓	✓	✓
Resource availability	✓	✓	✓	✓
Firm size				
Firm complexity			✓	✓

From a practical standpoint, the organization is encouraged to adjust its ERM process in accordance with its needs, specifications, and characteristics. By design, each organization has its own procedure and mechanism in conducting the ERM process, even though the underlying idea and principles of risk management are the same in every organization that operates within the same or different industry. Accordingly, the needs and the characteristics vary from one organization to another. Although this particular aspect is well-known, it is not yet explicitly articulated within the specified ERM maturity models. As such, with increases in the scale of operations of an organization, the level of the organization's ERM effectiveness has the potential to be decreased if the organization makes no necessary adjustments. Hence, the result of the ERM maturity assessment has the potential to become inaccurate if the criterion of the firm size is not taken into account, especially within the context of benchmarking the risk management maturity level between two or more organizations.

With the exclusion of the firm size criterion, it has the potential to affect the accuracy of the organization's ERM maturity under the consideration of its complexity (i.e., the number of business segments within the firm). As such, the increase of business segments within an organization increases the inherent risks that the organization needs to manage. This particular issue has the potential to affect the maturity level of an organization's ERM in a way that the level of its departments' ERM effectiveness is not equal or proportional in identifying and managing the specific risks that exist within the departments' activities.

Consequently, if one of its departments has a shallow risk management effectiveness, it can hamper the organization's overall ERM effectiveness and the progression in making the organization more mature holistically due to the existence of disintegration within one of its departments. Therefore, under the context of the inclusion of the criteria of firm size and firm complexity in assessing the maturity of the organization's ERM, an optimum level of the risk management effectiveness and maturity can be achieved under the condition where the quality and capabilities of the organization's ERM are proportional to the scale of its operations and the number of business segments it has.

Respectively, in achieving a proportional ERM effectiveness to cope with the risks that exist within the organization's department and the scale of its operation, the criterion of resource availability is essential to its ERM maturity. The organization has to ensure fluidity in providing and allocating the necessary resources (i.e., both financial and human capital resources) to maintain an adequate level of quality and performance within its ERM activities, which is reflected in the scale of its ERM program that covers all of its business activities. Furthermore, the availability of the organization's resources determines its capabilities and capacity to implement an integrated and holistic ERM mechanism into its business activities and the rate of progression in shaping the risk-oriented culture that is shared within all the levels within its management.

Putting together the relationship between the criteria of firm size, firm complexity, and resource availability, the harmonization of these three criteria is crucial in regards to the effectiveness of the organization's ERM. Accordingly, the criteria of environmental uncertainty and industry competition consider the organization's capabilities in adapting its risk-based approach and ERM process to the dynamic changes that occur within its external environments. In regards to the criterion of industry competition, ERM's role within the organization is essential in ensuring the earning of a sustainable level of profits. In other words, the effectiveness of the organization's ERM should also consider the dynamicity of the competition of its industry and the capability of the organization in providing alternative options that added value to its decision-making process through the lens of risk management perspective. Therefore, under the context of ERM maturity, the measurement of the organization's ERM maturity should be constructed into one pertinent grouping that reflects its distinct characteristics and its capabilities in adapting to its surrounding.

Finally, the essential criteria of ERM effectiveness also include the organization's capabilities in maintaining the operability of its ERM process and the quality in supervising the role and the performance of its ERM mechanism in supporting and complementing its business activities. With respect to the organization's internal control, the criterion of the audit committee under the context of risk management is to ensure the compliance of the ERM procedure within itself and ensure the flow of risk-related information is accessible to enhance the organization's risk-based decision and planning. This expands the audit committee's role within the organization beyond the task of financial reporting.

Concerning the aspect of maintaining the operability of the organization's ERM program and the level of integration of its ERM process across all departments, the criterion of governance mechanism is taken into account the perspective in building the reliability of the organization's ERM mechanism as one cohesive process that is connected with all of the layers within the firm's management. Since the concept of governance mechanism is oriented on the set of rules, policies, and practices taken by the organization's executives, it is also dictated how the ERM process within the firm is applied. Consequently, under the context of assessing the ERM maturity level of a firm, the criteria of governance mechanism and audit committee are influential in determining the degree of the organization's ERM effectiveness and the level of integration of its ERM process in achieving its strategic objectives. Nonetheless, an organization can achieve the state of mature ERM under the condition where its governance mechanisms and audit committee matched the organization's characteristics and the nature of the risks that exist within its external environment and, most of all, aligned with the value of the organizations.

3.3. Potential inclusion for the ISO 31000:2018-based ERM maturity model

Under the context of the ERM's nature according to the definition construed by ISO (2018), it focuses on the harmonization between the components of the principles of risk management, its framework, and process. Accordingly, the guideline in

implementing an integrated ERM mechanism within the ISO 31000:2018 standard considers the whole spectrum of the organization's characteristics and the nature of the specific risks that exist within its internal and external environments. Similar to the previous subsection's findings, the criterion of firm size is also not included within the three components of the ISO 31000:2018 standard, as shown in Table 3.

Table 3: The inclusion of risk management essential criteria within the ISO 3100:2018 standard

Criteria	ISO 31000:2018 standard components		
	Principles	Framework	Process
Environmental uncertainty	✓	✓	✓
Industry competition		✓	✓
Governance mechanism	✓	✓	
Audit committee		✓	✓
Resource availability		✓	
Firm size			
Firm complexity		✓	✓

Within the similar context on the implication from the exclusion of firm size criterion described in the previous subsection, the scale of operations of an organization or the adopters of the ISO 31000:2018 standard are also affects the ERM effectiveness of the organization as a whole and the approach in implementing an integrated risk management process into its activities.

In particular, the ISO 31000:2018 adopters face the challenge of ensuring the quality and the effectiveness of its ERM process covers all of its business segments and the operability of its risk management mechanism on the whole spectrum of its operational activities. As such, if the organization has a bigger scale regarding its operations, the organization will experience a higher degree of difficulty in making its ERM process integrated and holistically complementing its activities. In relation to the seven criteria of ERM effectiveness, both the ISO 31000:2018 standard and the ERM maturity model of ERMA (2020) do not explicitly consider the criterion of firm size due to the common advice in implementing an integrated ERM process is based on the organization or the standard adopter's needs and specification. As a result, the phrase "*Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization's needs and culture*" within the ISO 31000:2018 standard is still remains vague due to no detailed specification or guideline that corresponds to the organization's size.

Following the implication from excluding the criterion of firm size within the ERM maturity, it cannot fully reflect the organization's overall ERM effectiveness and its risk management maturity. Although the ISO 31000:2018 standard takes into account the perspective of the cohesiveness of the role and function of the ERM process in supporting the organization's business activities and its corporate governance mechanism, it does not explicitly articulate the proportionality of the ERM effectiveness with the number of business segments of an organization and its scale of operations.

Considering the gap within the ISO 31000:2018 standard and ERM maturity model of ERMA (2020), it is determined that there is room for improvement that can be added to the standard and the ISO-based ERM maturity model. Although both the ISO 31000:2018 standard and the ERM maturity model of ERMA (2020) covers the whole aspect in regards to the implementation of an integrated ERM process that covers the adopters' internal control mechanism and its effectiveness in managing the internal and external risks, the criterion of firm size is not explicitly articulated along with the potential impact it might bring in establishing a holistic ERM process and mechanism in supporting the adopter's business activities.

With the inclusion of the criterion firm size, it has the potential to help the adopter of the ISO 31000:2018 standard in creating a road map for integrating the principles and process of risk management that suited with its scale of operation rather than giving a piece of generic advice to adjust their ERM process in accordance to its needs and specification. Furthermore, with the ERM maturity model of ERMA (2020), the criterion of firm size can be added to the model in measuring the organization's ERM effectiveness and the ISO 31000:2018 standard adopters that is proportional to its scale of operation.

Respectively, by adding the criterion of firm size into the ISO 31000-based ERM maturity model, it can generate two classifications. Namely, (1) the ERM maturity level of all the adopter's departments and (2) the overall ERM maturity of the standard adopter that is acquired through the average score from all of the departments' maturity results. As such, it is to give the organization and the adopters of the standard the complete picture of the level of its ERM effectiveness, efficacy, and maturity in aiding them to achieve its objectives. Thus, it has the potential to give the adopter of the ISO 31000:2018 standard the information that can pinpoint the weakest link within its structure and develop a plan that can be used to increase the maturity level of the department that has shallow ERM effectiveness and maturity in order to achieve an integrated and holistic ERM effectiveness that is reflected within each of the adopter's departments.

4. Conclusions

Literature review discovers seven criteria that are considered essential in measuring an organization's ERM maturity. They are (1) firm size, (2) firm complexity, (3) resource availability, (4) environmental uncertainty, (5) industry competition, (6) governance mechanism, and (7) audit committee. Whereas those seven criteria are supposed to be used or adopted by the existing ERM maturity models, the mapping shows that one of the criteria is not reflected or explicitly used by the existing ERM maturity models both of the non-ISO 31000 and the ISO 31000. In this regard, both models do not consider firm size explicitly as an essential criterion in measuring the organization's maturity.

Whereas there is no explanation of the missing criteria in the non-ISO 31000 based model, some well-noted argumentations are made that relate to the ISO 31000 based

model. In this regard, ISO 31000 based risk management maturity model puts forward an argumentation that is basically in line with the underlying reasoning of the ISO 31000 standard itself, which emphasizes its generic features as a standard (i.e., regardless of the size). Furthermore, ISO 31000 encapsulates such generic features inherently and practically into their risk management principle, framework, and process rather than explicitly needed as distinct maturity criteria. For example, the core of risk management principles in ISO 31000 (i.e., creating and protecting value) is relevant and contextual to any type of organization regardless of its size and myriad. The bigger the organization's size, the more challenging their pathway to create and protect value.

Further, the core of the risk management framework in ISO 31000 (i.e., leadership and commitment) is critically important to any type of organization regardless of its size and complexity. The bigger the size of an organization, the more dimensions of leadership and commitment are in place. Lastly, the initial step of the risk management process in ISO 31000 (i.e., establishing the context) where we must address specific and relevant external and internal contexts of an organization regardless of their size and the industry. The bigger the size of an organization, the more subsets of circumstances be generally addressed. Hence the criteria of the firm's size are implicitly taken into account.

This study's findings may help risk practitioners increase the effectiveness of their organization's risk management maturity assessment by knowing what essential criteria should be well addressed whenever they must assess their organization's risk management maturity. As such, regardless of the risk management maturity model, they would be able to cautiously consider what matters and therefore keep the effectiveness of their attempt. For those who are the ISO 31000 adopters, it is practically recommended to use the ISO 31000 based risk management maturity model as it addresses the whole seven essentials criteria as discovered through literature review. One caveat, however, needs to be noted that one particular criterion (i.e., firm size) needs to be addressed either specifically and intentionally as an additional element to the risk management maturity model or cautiously be embedded in one of the other criteria (e.g., firm complexity).

Apart from this study's contribution, which may help risk practitioners in general and ISO 31000 adopters in particular, however, there is a limitation. As a literature review and desk research, this study is theoretically bounded and limited with no direct empirical observation that could provide much more in-depth understanding and insights of how the risk management maturity assessment is conducted and how the seven criteria are well and practically addressed in a real-case environment to raise their effectiveness. Therefore, it is recommended to conduct such empirical direct observations and research in this area as further studies.

References

Antonucci, D. (2016). *Risk Maturity Models: How to assess risk management effectiveness*. Kogan Page Limited.

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. *Contemporary Accounting Research*, *30*(4), 1264–1295. https://doi.org/10.1111/j.1911-3846.2012.01194.x

Chapman, R. J. (2011). *Simple Tools and Techniques for Enterprise Risk Management* (2nd ed.). John Wiley & Sons. https://doi.org/10.1002/9781118467206

Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise Risk Management and the Financial Reporting Process: The Experiences of Audit Committee Members, CFOs, and External Auditors. *Contemporary Accounting Research*, *34*(2), 1178–1209. https://doi.org/10.1111/1911-3846.12294

Dali, A., & Lajtha, C. (2012). ISO 31000 Risk Management — "The Gold Standard." *EDPACS*, *45*(5), 1–8. https://doi.org/10.1080/07366981.2012.682494

Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, *44*(1), 193–223. https://doi.org/10.1016/j.jacceco.2006.10.003

Elahi, E. (2013). Risk management: the next source of competitive advantage. *Foresight*, *15*(2), 117–131. https://doi.org/10.1108/14636681311321121

ERMA. (2020). *ERMA ISO 31000 Risk Management Maturity Model (RM3)*. Enterprise Risk Management Academy.

Farrell, M., & Gallagher, R. (2015). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. https://doi.org/10.1111/jori.12035

Fraser, J., & Simkins, B. J. (2010). *Enterprise Risk Management: Today's Leading Research and Best Practice for Tomorrow's Executives*. John Wiley & Sons.

Gatzert, N., & Martin, M. (2015). Determinants and Value of Enterprise Risk Management: Empirical Evidence From the Literature. *Risk Management and Insurance Review*, *18*(1), 29–53. https://doi.org/10.1111/rmir.12028

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*(4), 301–327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Hillson, D. A. (1997). Towards a Risk Maturity Model. *International Journal of Project and Business Risk Management*, *1*(1), 35–45.

ISO. (2009). *Risk management - Principles and guidelines* (ISO 31000:2009). International Organization for Standardization.

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

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, *90*(6).

Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The Effect of Corporate Governance on the Use of Enterprise Risk Management: Evidence From Canada. *Risk Management and Insurance Review*, *6*(1), 53–73. https://doi.org/10.1111/1098-1616.00020

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

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does Enterprise Risk Management Increase Firm Value? *Journal of Accounting, Auditing & Finance*, *26*(4), 641–658. https://doi.org/10.1177/0148558X11409160

Mikes, A., & Kaplan, R. S. (2014). *Towards a Contingency Theory of Enterprise Risk Management* (No. 13–063; Working Paper). Harvard Business School.

Paape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review*, *21*(3), 533–564. https://doi.org/10.1080/09638180.2012.661937

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

RIMS. (2006). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management*. The Risk and Insurance Management Society, Inc.

Silva Rampini, G. H., Takia, H., & Berssaneti, F. T. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manufacturing*, *39*, 894–903. https://doi.org/10.1016/j.promfg.2020.01.400

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, *16*(4), 640–661. https://doi.org/10.1108/09513570310492335

Whittemore, R., & Knafl, K. (2005). The integrative review: updated methodology. *Journal of Advanced Nursing*, *52*(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x