Financial Reporting (ISSN 2036-671X, ISSNe 2036-6779), 2026, 1, pp. 5-22 *Opinion Piece*

Enterprise Risk Management: Empirical foundations, governance integration, and future directions for ERM research

Mark Beasley[*], Don Pagach[**]

Abstract

Academic research has played an important role in examining the Enterprise Risk Management (ERM) process and thinking about its organizational implications and value. Collectively, this literature reframes ERM as an organizational capability whose effectiveness depends on engagement from board and C-suite leadership, integration of governance activities overseeing both strategic direction and management's risk-taking, and alignment of risks with strategic incentives. The need for ERM has grown to become a defining element of modern corporate governance,

[*] ERM Initiative, Poole College of Management, NC State University. Mark S. Beasley is the Alan T. Dixon Distinguished Professor of Accounting and Director of North Carolina State's Enterprise Risk Management (ERM) Initiative, which provides thought leadership about ERM practices and their integration with strategy and corporate governance. He has authored over 100 research articles and business publications and regularly consults with boards and executive teams on effective enterprise risk management practices, helping to strengthen the connection with strategy planning and oversight. Mark served over seven years on the COSO board, including his involvement in the development of COSO's 2004 Enterprise Risk Management – Integrated Framework and its 2017 revision. He is currently serving as President of the American Accounting Association (AAA). Mark received his B.S. in Accounting from Auburn University and PhD from Michigan State University.

[**] ERM Initiative, Poole College of Management, NC State University. Don Pagach received his bachelor's and master's degrees in accounting from the University of Wisconsin-Madison. He later received his Ph.D. from Florida State University. His research focuses on enterprise risk management and financial accounting, with a specific focus on ERM culture and financial statement analysis. Professor Pagach has been named a University Outstanding Teacher and has received research awards for his work on Enterprise Risk Management. He holds a CPA certificate in the state of North Carolina and is a member of the AICPA's CPA Exam Committee. *Corresponding Author*: Department of Accounting, NC State University, Raleigh, NC 27695, +1-919-515-4447.

Doi: 10.3280/fr202622593

reflecting organizations' need to manage increasingly complex strategic, operational, financial, and compliance risks that are increasingly present and rapidly evolving in today's global business environment. Whereas traditional risk management focuses primarily on insurable and financial risks within siloed, functional areas, ERM represents an enterprise-wide approach linking risk identification, assessment, and response to strategic objectives and performance outcomes (COSO 2017). We believe that advances in financial regulations, especially in Europe, provide an opportunity to create a forward-looking research agenda centered on better understanding the dynamics and practices of establishing an appropriate risk culture, risk appetite and risk management disclosure credibility – three mechanisms that increasingly define ERM effectiveness yet remain underexplored in accounting research.

Keywords: Enterprise Risk Management, risk governance, risk appetite, risk culture

JEL: G32, G34, M10, M14

First submission: April 17, 2026. Accepted: May 20, 2026.

1. Introduction

In 2005, we published our first Enterprise Risk Management (ERM) focused article related to the security market reaction to ERM adoptions, and this has led to a two-decade examination of ERM as a critical approach to an enterprise's risk governance. Our research has evolved to address ERM maturity, strategic impact, governance ecosystems, climate and AI risk, and disclosure substance. Many other academics from a variety of disciplines including strategy, operations, insurance, accounting, finance, among others, have contributed to the advancement of ERM academic literature. In parallel, many European scholars have provided additional evidence on ERM effectiveness in governance settings in other global settings.

This contribution for *Financial Reporting* examines ERM research with an explicit focus on the relevance of disclosures of risk management practices and institutional environments. We first examine the two initial focuses of ERM research: the adoption of ERM and the benefits obtained from the use of ERM. We highlight how initially ERM researchers faced identification and risk management disclosure issues that made it difficult to make specific conclusions about critical factors that influence ERM's adoption, maturity or effectiveness. We use that as a backdrop to highlight how advances in European financial regulations now provide an opportunity to create a forward-looking research agenda centered on better understanding the dynamics and practices of establishing an appropriate risk culture, risk appe-

tite and risk management disclosure credibility – three mechanisms that increasingly define ERM effectiveness yet remain underexplored in accounting research.

2. Structural foundations of ERM: Adoption and governance signals

Organizations' use of ERM began in the late 1990s to early 2000s, mostly starting within the insurance industry. An initial attempt to provide guidance was made in the mid-1990s by Standards Australia and Standards New Zealand, two national organizations working in the field of standardization. That led to issuance of the Australia/New Zealand AS/NZS 4360, *Risk Management*. But it wasn't until the early 2000s, that other frameworks were introduced, although none resulted in mandating ERM. In 2003, the Casualty Actuarial Society issued its *Overview of Enterprise Risk Management* (CAS, 2003), that outlines best practices principles for designing and implementing an effective ERM process. Additional frameworks have been developed by other organizations, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004, 2017) and its *Enterprise Risk Management – Integrated Framework*, the International Organization for Standardization's ISO 31000 – *Risk Management Framework* (ISO, 2009), the United Kingdom's *Corporate Governance Code* (UK, 2012), Australia/New Zealand's 4360 *Risk Management*[1] standard (AS/NZS, 2004), and Tillinghast-Tower Perrin's *Enterprise Risk Management: An Analytic Approach* (Miccolis & Shah, 2000). However, these frameworks only provide principals-focused guidance to provide organizations with a conceptual overview about key elements of an enterprise-wide approach to ERM and do not require a specific version of ERM be implemented, nor do they provide a checklist of tasks to be implemented.

Many regulatory agencies have emphasized that boards of directors take responsibility for the oversight of risk but have not made specific requirements to implement ERM as a risk management approach. For example, the New York Stock Exchange (NYSE) Corporate Governance Rules note that it is the responsibility of management to assess and manage the company's exposure to risks, the audit committee is required to "*discuss policies with*

[1] Originally issued in 1995 and updated in 1999 and revised in 2004 by the Standards New Zealand, the joint Australian/New Zealand Committee decided to not revise that standard in 2009 and instead agreed to promote ISO's 31000 - *Risk Management* standard.

respect to risk assessment and risk management." European regulators have also emphasized risk oversight, with country level corporate codes focused on risk management and oversight. In addition, other market participants, such as rating agencies, have stated that they consider organizations' ERM programs when providing credit ratings (Gates & Hexter, 2005).

Despite the development of these frameworks for organizations to consider as they evaluate the implementation of ERM processes, an issue that has long been a problem for academic research examining ERM is the identification of firms that have implemented ERM, and if so, to what extent they have implemented a variety of key elements of an ERM process. Without specific requirements to implement ERM and varying components of effective ERM across the different frameworks and despite the lack of requirements for public disclosures of ERM adoptions and practices, academic researchers have struggled to identify instances of ERM implementations and the associated process details. In response, researchers have generally used four methods to determine if an organization has adopted ERM, all of which have unique advantages and disadvantages.

The first method that researchers used examines organizations' public announcements of the hiring of a Chief Risk Officer (CRO) or equivalent type position (Liebenberg & Hoyt, 2003; Beasley et al., 2008; Pagach & Warr, 2011). These studies drew inspiration from the Aabo, Fraser and Simkins (2005) and Nocco and Stulz (2006) cases that focused on the role of the CRO in organizations' ERM programs. While the initial research papers were able to obtain firm samples based on company announcements, sample sizes were often small. In addition, the measurement was simple and dichotomous in that either the organization adopted ERM or did not. Another drawback to this method is that it may provide a false positive signal of ERM adoption since the CRO position is popular and firms could announce the position without actually adopting ERM. This might be especially true in certain regulated industries, such as banking, insurance, and utilities, that often appoint individuals to serve as CRO while those entities do not have ERM in place. One explanation is the *catering approach*, which suggests that managers take actions in order to boost share prices above fundamental value by imitating strong corporate governance actions (Baker & Wurgler, 2011). The appointment of a CRO might merely be a signal to the marketplace implying enhanced risk governance. Moreover, this research approach might also mean that researchers overlook firms that have ERM in place, if those entities have another executive position overseeing the process that does not have the CRO title.

The second method used by researchers to identify ERM adopting firms is to search for evidence of ERM by searching for keywords, like "enterprise

risk management" and "risk committee," in databases such as Lexis/Nexis, Dow Jones. Some of the earlier studies, such as Hoyt and Liebenberg (2003) and Lin et al. (2012), used this approach. Gordon et al. (2009) used a more sophisticated version of this approach by creating an index of ERM dimensions based on the related COSO framework factors of strategy, operations, reporting and compliance. They search financial reports for evidence of meeting these factors to create an ERM effectiveness index. Desender (2011) also used the COSO framework to create a list of 70 elements based on risk management disclosures in the financial reports of pharmaceutical companies. However, using keywords reflecting certain ERM activities or components that are not mandatory for ERM, such as the formation of a risk committee, may cause researchers to overlook many firms that are adopting ERM but not reporting the specific activity being measured.

One advantage of searching for evidence of ERM implementation is that it allows for the creation of a more multifaceted measure of ERM implementation. Many researchers have used these types of measures as a proxy for the level of an organization's ERM maturity. This is especially true with respect to governance requirements related to board risk oversight. In February 2010, the US Securities and Exchange Commission (SEC) issued new rules requiring proxy disclosures describing the board's role in risk oversight for all public companies whose securities are registered with the SEC (SEC, 2010). Beasley et al. (2020) used the board risk oversight statements in firms' proxy statements to develop a measure of the quality of the board of directors' and firms' risk management programs.

A third method of identifying ERM adopters is to use information from credit rating services. ERM ratings provided by Standard & Poor's are used as a proxy for the degree of ERM adoption by Baxter et al. (2013) and McShane et al. (2011). The advantage of using ratings is that they are developed independently from management of the entity examined. A drawback to this methodology is that currently these ratings are not widely available for many firms outside the insurance industry.

A fourth method is to survey firms to determine to what degree they have adopted ERM processes. Beasley et al. (2005) do so by *asking* firms to score the level of their ERM implementation, from "no plans exist to implement ERM" to "complete ERM is in place". Paape and Spekle (2012), Beasley et al. (2015), and Beasley et al. (2023) also use this methodology. An advantage of the survey method is that it can provide more in-depth information about a firm's activities and processes. On the other hand, asking firms to score the level of their ERM program can potentially lead to biased results since managers might tend to overstate the level of ERM programs that they are lead-

ing. This may occur for several reasons such as the popularity of ERM, trying to be seen as strong in risk management in a post-financial crisis and so on.

Lundqvist (2015) improves on Desender's public disclosure measure by creating a survey based on the dimensions to assess the degree of implementation. Using factor analysis, the author finds four "pillars" of ERM. The first two pillars, general internal environment and general control activities, are considered necessary for ERM implementation but may not be specific to ERM. The fourth pillar, specific risk identification and risk assessment, is consistent with risk management and considered necessary for ERM but not specific to ERM. The third pillar, the holistic organization of risk management, is what the author considers the true defining element of a robust ERM program.

In addition, there have been influential research papers that have used the case study approach to understand how ERM practices evolve within organizations. Arena, et al. (2010) examine specific companies to understand how ERM is actually implemented and find that processes do not simply follow a COSO or ISO methodology but are subject to formal practices and how risk practices are embedded in strategy and decision making. In a follow-on study Arena et al. (2017) document the difficulty that practitioners have in aggregating all risks into a single enterprise risk and that an organization's goal of having a standardized risk management process can result in resistance and internal rejection.

Collectively, early empirical research established that ERM adoption is systematic rather than random. Survey-based evidence showed that firms implementing ERM tend to be larger, more operationally complex, and subject to greater regulatory scrutiny, with stronger board involvement and internal audit engagement. These findings suggested that ERM emerges as part of broader governance modernization rather than as a random and isolated control initiative. This is a key finding of the influential works of Powers (2007) which suggests that ERM frameworks create new categories of expertise, reporting routines, and oversight structures that influence how organizations define and consider risk, resulting in risk management becoming part of corporate governance, internal audit and managerial responsibility. However, Powers (2009) warns that ERM can become a simple compliance exercise and not provide value if it does not take into account the operational and strategic focuses of the individual organization.

This early phase of research repositioned ERM as strategic governance infrastructure – an organizational response to increasing uncertainty embedded within senior leadership and board oversight. However, in order to move the ERM research agenda forward more detailed disclosures about ERM

components, processes, and extent of implementation are necessary to better understand how ERM works and adds value.

2.1. From adoption to maturity: Strategic impact and firm performance

As ERM became more prevalent, scholarly attention shifted from ERM adoption to ERM effectiveness. Mixed results were found using large scale empirical studies, mainly due to difficulty knowing when ERM started and the confounding factors that make long-term longitudinal studies difficult. Executive survey evidence revealed substantial heterogeneity in ERM maturity, with strategic impact strongest when ERM is proactive, integrated with planning and strategy, and supported by senior leadership. A central insight emerging from this phase is that ERM quality matters more than ERM's existence.

Complementary work examining the association of ERM and firm performance emphasized conditional rather than universal effects. ERM is theorized to influence outcomes through improved capital allocation, reduced downside risk, enhanced coordination across risk silos, and greater strategic flexibility. At the same time, persistent endogeneity challenges complicate causal inference, underscoring the importance of organizational context and implementation depth.

European research reinforces these conclusions. One of the first and best studies to examine the effectiveness of ERM was Florio and Leoni (2017). In this study of Italian firms, the authors document that firms with advanced levels of ERM implementation have higher firm performance. The research not only focuses on the association between ERM implementation and performance but also highlights institutional differences in governance structures and regulatory environments. Similarly, Braumann (2018) in an innovative study examines ERM effectiveness. Using a survey approach, the author finds that risk awareness, defined as "*the result of all employees, including top management, sharing and reflecting on how their behavior and actions are associated with causes and outcomes of potential risks to the firm*" is an important cultural component in a firm's ERM system. The study provides a unique contribution to ERM research by providing insights into the role specific components of ERM contribute to increasing ERM's impact on firm performance. The work emphasizes that ERM effectiveness depends on integration with strategic decision-making rather than mere structural adoption.

More recent scholarship advances ERM research by adopting a systems perspective. Rather than focusing on isolated governance mechanisms such

as CROs or risk committees, Beasley et al. (2015) conceptualize ERM as embedded within a broader governance ecosystem involving boards, audit committees, executive management, internal audit, and risk professionals. Evidence from this research suggests that ERM effectiveness depends on interactions among governance actors. The presence of formal structures alone is insufficient; what matters is how risk information flows across organizational levels, how responsibilities are allocated, and how risk considerations influence strategic choices. Beasley et al. (2023) examine the ecosystem of risk governance. They find that risk governance is best described as a service dependent on a network or ecosystem of participants who include users of risk information and providers who design and implement risk governance processes. This ecosystem framing aligns closely with European governance models that emphasize collegial boards and stakeholder engagement.

Taken together, these findings underscore that ERM is best understood as a strategic capability whose benefits materialize only when embedded in enterprise-wide processes with a holistic embrace across the organization. This perspective motivates questions into how organizations define acceptable risk, translate risk considerations into operational decisions, and sustain ERM through organizational culture.

2.2. Risk management process disclosure and reporting challenges

Recent surveys of executives and risk professionals document an evolving risk landscape characterized by increased attention to strategic risks, greater board engagement, and growing recognition of ERM's importance (Beasley & Branson, 2022). However, these surveys also reveal persistent challenges in operationalizing ERM, particularly in articulating risk appetite, embedding ERM into day-to-day decisions, and fostering consistent risk cultures across organizations.

Since the financial crisis there has been an increased focus by global regulators to increase firm disclosures of risk oversight and risk management practices (SEC, 2010, 2023, 2024; ESRS 1, 2024). These calls for greater risk disclosures have stemmed in part due to various macroeconomic, political, social and climate events that have occurred. In the United States (US), regulations require firms to disclose information around the board of director's role in risk oversight (SEC, 2010), oversight of compensation plan risks (2010), cybersecurity risk (SEC, 2023), and climate risk (SEC, 2024). In Europe newly adopted regulations require disclosure about "*material infor-*

mation regarding impacts, risks and opportunities in relation to environmental, social and governance matters."

At the same time, research examining mandated proxy disclosures regarding the board's role in risk oversight reveals substantial limitations in external transparency. Despite regulatory requirements, proxy or annual financial report disclosures are often highly standardized and provide limited firm-specific insight. Empirical analysis shows weak alignment between disclosure language and observable governance structures, suggesting that mandated reporting frequently results in symbolic boilerplate disclosures for compliance purposes rather than substantive communication.

Complementary work on risk disclosure emphasizes that reporting practices remain largely backward-looking and generic. Although narrative risk management sections in public documents have expanded, they often provide limited insight into how risks are actively managed or how risk considerations shape strategy. Financial statement users' calls for more forward-looking and decision-useful disclosures reflect frustration with boilerplate language that offers little differentiation about risk management processes across firms. There is empirical evidence, however, that boards more engaged in risk oversight are able to use the discretion provided by the SEC's disclosure rule to provide substantive and potentially value-relevant information for stakeholders about the entity's risk management processes and board risk oversight activities (Beasley, et al, 2020).

These findings highlight a fundamental tension: while internal ERM practices may be advancing, external disclosures about those practices to an organization's stakeholders often fail to convey their substance. For accounting researchers and standard setters, this raises important questions about the informational value of current risk management disclosure reporting regimes.

3. Moving ERM research forward

The major question that ERM researchers face currently is how to better understand internal ERM practices in a setting in which limited disclosures about ERM processes exist to allow opportunities for specific conclusions to be reached. We believe that changes and advances in European regulatory reporting, which are also leading to changes in the US, may now provide new opportunities for advancement of ERM research. Integrated reporting and sustainability disclosures, where firms are increasingly expected to explain not only what risks exist but how risks are identified, managed and mitigated, provide a unique ability to allow firms to provide detailed information about their

ERM processes. In addition, the Netherlands has been at the forefront of asking firms to be additionally transparent in their risk governance. The Dutch Corporate Governance Code (2025) which grew from the Royal Ahold scandal provides a framework that Dutch firms must follow for effective collaboration and management. We examine these reporting practices to suggest a research agenda focused on risk culture, risk appetite and disclosure.

3.1. Risk culture: The behavioral engine of ERM

The first component of the COSO framework is governance and culture and focuses on the role of organizational culture in supporting effective ERM. Risk culture determines how and to what extent ERM frameworks function in practice. Risk culture encompasses shared norms, incentives, and behaviors within an enterprise that shape how individuals identify, communicate, and respond to risk. The COSO framework examines the importance of risk culture and states that:

"A culture that is embraced by all personnel – one in which people do the right thing at the right time – is critical to the organization being able to seize opportunities and minimize risk to achieve the strategy and business objectives."

Existing research suggests that formal ERM structures alone are insufficient to ensure effective risk management. Instead, ERM success depends on leadership tone, accountability mechanisms, and the ability for employees to safely raise risk concerns. This is an important finding from Braumann, et al. (2020) which finds that open dialogue, discussion of uncertainty and managerial engagement strengthen leadership tone on organizational awareness of risk while monitoring targets is a less effective way of building a risk aware organization. Middle management plays a particularly critical role in translating board-level policies into day-to-day operational decisions, yet this layer remains largely unexplored in archival ERM research.

Despite the behavioral importance and impact an organization's culture can have on risk taking and the related management of risks, there is limited empirical evidence about how an organization's culture might impact ERM and its value proposition. Several behavioral questions warrant attention. How do executive compensation structures influence the embrace of ERM and the reinforcement of its value across other employees? And, how do compensation structures impact the extent of risk taking, risk reporting and escalation? To what extent does organizational culture encourage early identification of emerging risks versus suppression of unfavorable information?

How do employees interpret and apply risk appetite guidance in decentralized organizations?

Addressing these issues will require surveys, interviews, experiments, and field studies that can complement archival approaches by revealing internal processes invisible in publicly disclosed data. Cross-country studies may be especially informative, given documented institutional differences in governance practices, variations in cultural norms, and stakeholder orientations across different country settings, including those across Europe. Understanding risk culture represents a natural extension of governance ecosystem research.

The recently passed European Sustainability Reporting Standards (ESRS) provides a unique ability to examine how organizations develop a culture. Specifically, ESRS G1 focuses on corporate culture and requires organizations to "*disclose initiatives to establish, develop and promote a corporate culture as well as its policies with respect to business conduct matters. … provide an understanding of how the administrative, management and supervisory bodies are involved in forming, monitoring, promoting and assessing the corporate culture.*" Examining these disclosures will allow researchers to understand how employees are introduced and integrated into the culture of an organization. For example, Ferrari's annual report (2024) states in its disclosures "*To ease employees into their new jobs, we provide a preinduction activity that is provided in a digital format, to foster team building, followed by a two-day induction program. The first day is dedicated to introducing the Company culture and mission, as well as guiding new employees through the corporate offices and production plants.*" Researchers will also be able to examine other questions related to risk culture such as how incentive pay is structured and if it instills behavior consistent with core values.

3.2. Risk appetite: How it affects strategy

The second component of the COSO framework is strategy and objective setting with principles focused on analyzing business context, defining risk appetite and formulating business objectives. This component focuses on the important process of integrating ERM with the organization's strategic initiatives.

Risk-taking is fundamental to value creation. As emphasized by Stulz (2016), firms do not fail because they take risks, but because they take the *wrong* risks or fail to govern risk-taking effectively. A central mechanism through which boards seek to govern risk-taking is the articulation of risk appetite – the amount and type of risk an organization is willing to accept in pursuit of its objectives.

Importantly, risk appetite is not intended to predict outcomes, but to constrain managerial behavior and align risk-taking with strategy.

However, despite the prominence of risk appetite as an important component highlighted in ERM frameworks, risk appetite has historically remained an internal governance tool and often not formally articulated across different dimensions of risk-taking. This changed with the 2022 revision of the Dutch Corporate Code, which requires firms to publicly disclose their risk appetite across strategic, operational, compliance, and reporting objectives. While the Code mandates disclosure, it provides little guidance on how risk appetite should be designed and communicated. As a result, firms retain substantial discretion not only over the *level* of risk appetite disclosed, but also over the *specificity* with which it is articulated.

This discretion over disclosure form is central to understanding the economic role of risk appetite disclosures. Prior research in accounting shows that disclosure specificity enhances credibility and informational value by reducing ambiguity and limiting opportunistic reinterpretation (Hope et al., 2016; Heinle & Smith, 2017). Applied to risk governance, more specific risk appetite disclosures may serve as stronger commitments that better constrain managerial discretion, while vague or purely narrative disclosures may function largely as symbolic statements.

Recent research using risk appetite disclosures of Dutch firms provides some insights about risk appetite. Pagach (2026) codes risk appetite disclosures along multiple dimensions, including specificity, use of quantitative thresholds, linkage to strategy, and evidence of operationalization. These measures were then related to observable governance characteristics and financial indicators. Examination of financial reports results in three primary patterns. First, while most firms provide some form of risk appetite statement, disclosures are predominantly qualitative and high-level. Many firms articulate broad aspirations (for example, maintaining a “moderate” or “balanced” risk profile) without specifying measurable tolerances or decision thresholds.

Second, only a subset of firms explicitly link risk appetite to strategic objectives, capital allocation, or performance metrics. Where such links exist, disclosures tend to be more detailed and are accompanied by stronger governance features, including active board engagement and formal ERM structures.

Third, even among firms with relatively sophisticated disclosures, external reporting rarely explains how risk appetite is cascaded into business-unit decisions or incentive systems. This suggests that risk appetite often remains a board-level concept rather than an operational guidepost and decision-making tool.

3.3. Risk disclosure: Management credibility

These findings reinforce a central theme of the broader ERM literature: internal practices appear to be advancing faster than their external representation. Risk appetite disclosures frequently satisfy formal requirements without providing decision-useful information to investors or other stakeholders.

The Netherlands evidence illustrates this gap clearly. While most firms provide formal risk appetite statements, few translate those statements into measurable thresholds or explicit decision rules. Instead, risk appetite is frequently expressed in qualitative terms that offer limited guidance for capital allocation, performance evaluation, or operational risk management.

Future research could address several fundamental questions. First, how do firms articulate and quantify risk appetite across financial, operational, and strategic domains? Second, do stated risk appetite levels align with observed risk-taking behavior, including leverage decisions, investment intensity, and hedging activity? Third, how are articulations of risk appetite cascaded from boards to business units, and how is adherence monitored? One study that has provided important evidence in this area is Crovini et al. (2024) who find that when firms connect risks to their business model investors are better able to evaluate the relevance and implications of the risks.

Methodologically, these questions invite integration of textual analysis with archival measures of risk-taking and performance. Developing continuous measures of risk appetite specificity and linking them to financial outcomes would move ERM research beyond binary adoption indicators toward operational relevance.

Building on the cumulative literature and the Netherlands evidence, this section advances a conceptual framework organized around three interrelated pillars: risk governance and culture, risk strategy and objective setting and external disclosure or communication. Together, these dimensions provide a coherent structure for future ERM research and may explain observed variation in ERM maturity and effectiveness. In addition, a 2025 change to the Dutch Corporate Code provides the opportunity to integrate risk culture, risk appetite and disclosure further. For financial years 2025 and onward, the Dutch Corporate Code requires that Dutch listed firms include a Risk Management Statement (*Verklaring Omtrent Risicobeheersing*) which provides an assessment of risk management and control systems in relation to the operational, compliance and reporting risks during the past financial year. For example, the Netherlands-based company, Acomo Group, in its 2025 annual report provided the following information about how it is performing the as-

sessment of its risk management process in compliance with the revised Dutch Corporate Code's Risk Management statement:

The following steps were taken to perform the assessment:

- **Establishing the foundational elements**: Defining the level of certainty and risk appetite to set the criteria for the assessment;

Acomo achieves this first step by setting its risk appetite for four dimensions: Strategic, Operational, Compliance and Financial. For each category the company categorizes its risk appetite as Averse, Minimal or Cautious.

- **Evaluating the existing activities against established criteria**: Evaluating current risk management, internal control, and assurance activities against the established criteria to assess their effectiveness in risk mitigation and identify potential gaps;

Acomo provides this information in a chart for each of its principal risks. For example, Acomo has an averse risk appetite for its operational cyber risk and the company provides numerous mitigating factors and controls that it is using to reduce the likelihood and impact of the risk exposure.

- **Determining conclusion**: Concluding based on the assessment for in-scope risks whether the intended level of certainty is achieved and creating development areas where gaps have been identified;
- **Developing a risk statement**: that reflects the results from the assessment performed.

The results of the final two steps are not disclosed beyond the fact that the Audit Committee reported to the Board of Directors on the substantiation of the Risk Management Statement and that it was also discussed with the external auditor. However, analysis of firm performance and an examination of the time series of disclosures of firms may allow researchers to better understand the effectiveness of risk governance practices documented in these statements.

3.4. Implications for financial reporting and regulation

The findings synthesized in this paper carry important implications for financial reporting disclosure practices and regulation, particularly in European contexts. First, regulators should recognize that mandated narrative disclosures about risk management practices alone are unlikely to convey ERM's substance within an enterprise. Greater emphasis on disclosure specificity, linkage of ERM to strategy, and measurable thresholds may enhance the decision-usefulness of risk management disclosures. Encouraging firms

to articulate how risk appetite informs capital allocation and performance management could improve transparency.

Second, boards and preparers should view risk appetite disclosures not merely as compliance exercises but as opportunities to communicate how risk considerations shape strategic priorities and operational decisions. This may be particularly relevant for those organizations with robust, value-adding ERM processes in place. Doing so may strengthen stakeholder confidence and reinforce internal accountability.

Third, standard setters may wish to explore frameworks that better integrate ERM with financial and sustainability reporting. As climate risk, supply-chain resilience, and cyber threats become increasingly salient, ERM disclosures must evolve to reflect the interconnected nature of modern risks.

4. Conclusions

Over the past two decades, ERM research has progressed from documenting adoption to examining strategic impact, governance ecosystems, and disclosure credibility. The field now stands at an inflection point. Structural questions about ERM adoption have largely been answered. The most pressing challenges concern how organizations operationalize the ERM process, how does risk culture get instilled? How is risk appetite set? How does culture enable or constrain ERM effectiveness? and how does financial reporting faithfully demonstrate internal risk governance. Ultimately, ERM researchers who help answer these questions can help lead to a better understanding of how ERM creates strategic value for organizations.

References

Aabo, T., Fraser, J. R. S., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: Enterprise Risk Management at Hydro One. *Journal of Applied Corporate Finance, 17*, 62-75. Doi: 10.1111/j.1745-6622.2005.00045.x.

Acomo Group (2025). *Acomo: 2025 Annual Report*. Retrieved from -- https://www.acomo.com/.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society, 35*(7), 659-675. Doi: 10.1016/j.aos.2010.07.003.

Arena, M., Arnaboldi, M., & Palermo, T. (2017). The dynamics of (dis)integrated risk management: A comparative field study. *Accounting, Organizations and Society, 62*, 65-81. Doi: 10.1016/j.aos.2017.08.006.

AS/NZS (2004). *Risk Management Standard AS/NZS 4360: 2004*: Standards Australia/Standards New Zealand.

Baker, M., & Wurgler, J. (2011). Behavioral corporate finance: An updated survey. In: *Handbook of the Economics of Finance* (Vol. 2, pp. 357-424), Elsevier.

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. Doi: 10.1111/j.1911-3846.2012.01194.x.

Beasley, M. S., Branson, B., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in enterprise risk management. *Journal of Accounting and Public Policy*, *33*(4), 334-349. Doi: 10.1016/j.jaccpubpol.2015.01.001.

Beasley, M. S., Branson, B., & Pagach, D. (2023). Improving disclosures about management of ever-evolving risks. *Controlling*. Doi: 10.15358/0935-0381-2023-S-20.

Beasley, M. S., Branson, B., & Pagach, D. (2023). An evolving risk landscape: Insights from a decade of surveys of executives and risk professionals. *Journal of Risk and Financial Management*, *16*(1), 29. Doi: 10.3390/jrfm16010029.

Beasley, M. S., Branson, B., Braumann, E., & Pagach, D. (2023). Understanding the ecosystem of enterprise risk management governance. *The Accounting Review*, *97*(4), 1-32. Doi: 10.2308/TAR-2020-0488.

Beasley, M. S., Branson, B., Pagach, D., & Panfilo, S. (2020). Are required SEC proxy disclosures about the board's role in risk oversight substantive?. *Journal of Accounting and Public Policy*, *40*, 106816. Doi: 10.1016/j.jaccpubpol.2020.106816.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Accounting Horizons*, *19*(3), 157-177. Doi: 10.1016/j.jaccpubpol.2005.10.001.

Beasley, M. S., Pagach, D., & Warr, R. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. *Journal of Accounting, Auditing & Finance*, *23*(3), 311-332. Doi: 10.1177/0148558X0802300303.

Braumann, E. C. (2018). Analyzing the Role of Risk Awareness in Enterprise Risk Management. *Journal of Management Accounting Research*, *30*(2), 241-268. Doi: 10.2308/jmar-52084.

Braumann, E. C., Grabner, I., & Posch, A. (2020). Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness. *Accounting, Organizations and Society*, *84*, 101128. Doi: 10.1016/j.aos.2020.101128.

Crovini, C., Giunta, F., Nielsen, C., & Simoni, L. (2024). Market valuation of risk reporting: The role of business model disclosure. *Abacus*, Doi: 10.1111/abac.12342.

CAS (2003). *Overview of Enterprise Risk Management*. Retrieved from -- http://www.casact.org/area/erm/overview.pdf.

COSO (2004). *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

COSO (2017). *Enterprise Risk Management – Integrating with Strategy and Performance, COSO*. Available at -- https://www.coso.org/Pages/erm.aspx.

Desender, K., On the Determinants of Enterprise Risk Management Implementation (2011). *Enterprise IT Governance, Business Value and Performance Measurement*, Nan Si Shi and Gilbert Silvius, eds., IGI Global, 2011. Available at SSRN: -- https://ssrn.com/abstract=1025982.

European Commission (2023). Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards (European Sustainability Reporting Standards – ESRS 1 General Requirements). *Official Journal of the European Union*. -- https://eur-lex.europa.eu/eli/reg_del/2023/2772/oj.

Ferrari (2022). *Ferrari N.V.: 2022 Annual Report*. Retrieved from -- https://www.ferrari.com/.

Financial Reporting Council (FRC). UK Corporate Governance Code (September 2012).

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

Gates, S., & Hexter, E. (2005). *From risk management to risk strategy*. New York: The Conference Board, Inc.

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. Doi: 10.1016/j.jaccpubpol.2009.06.006.

Heinle, M., & Smith, K. (2017). A theory of risk disclosure. *Review of Accounting Studies*, *22*(4), 1459-1491. Doi: 10.1007/s11142-017-9406-9.

Hope, O.-K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *The Accounting Review*, *91*(4), 1005-1034. Doi: 10.2308/accr-51258.

ISO. 2009. 31000-Risk Management. Geneva, Switzerland: International Organization for Standardization.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, *6*, 37-52. Doi: 1098-1616.00019.

Lin, Y., Wen, M., & Yu, J. (2012). Enterprise Risk Management. *North American Actuarial Journal*, *16*(1), 1-28. Doi: 10.1080/10920277.2012.10590630.

Lundqvist, S. A. (2015). Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, *34*, 441-466. Doi: 10.1016/j.jaccpubpol.2015.05.002.

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

Miccolis, J., & Shah, S. (2000). *Enterprise Risk Management: An Analytic Approach*. Tillinghast: Tower Perrin.

Monitoring Committee Corporate Governance Code (2025). *The revised Dutch Corporate Governance Code*. Retrieved from -- https://www.mccg.nl/english.

Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance, 18*, 8-20. Doi: 10.1111/j.1745-6622.2006.00106.x.

Paape, L., & Speklé, R. F. (2012). The adoption and design of Enterprise Risk Management Practices: An empirical study. *European Accounting Review*, 21, 533-564. Doi: 10.1080/09638180.2012.661937.

Pagach, D. (2026). *The Disclosure of Risk Appetite*. Working paper, NC State University.

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

Pagach, D., & Warr, R. (2015). The effects of enterprise risk management on firm performance. In *The Routledge Companion on Strategic Risk Management*. Routledge.

Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6-7), 849-855. Doi: 10.1016/j.aos.2009.06.001.

Securities and Exchange Commission (2009). *Proxy Disclosure Enhancements* (Release Nos. 33-9089; 34-61175; IC-29092; File No. S7-13-09). -- http://www.sec.gov/rules/final/2009/33-9089.pdf.

Securities and Exchange Commission (2023). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (Release Nos. 33-11216; 34-97989; File No. S7-09-22). -- https://www.sec.gov/rules-regulations/2023/07/s7-09-22.

Securities and Exchange Commission (2024). *The Enhancement and Standardization of Climate-Related Disclosures for Investors* (Release Nos. 33-11275; 34-99678; File No. S7-10-22). -- https://www.sec.gov/rules-regulations/2024/03/s7-10-22.

Stulz, R. (2016). Risk management, governance, culture, and risk taking in banks. *Economic Policy Review*, Aug, 43-60.