

Discussion Paper

Shaping the Future: The Crucial Role of the Corporate Risk Manager

Introduction

In today's world, risk management plays a more essential role than ever. In an increasingly complex and unpredictable world, risk management encompasses a broad spectrum of responsibilities, including identifying, assessing and mitigating potential threats to an organisation's assets and operations. The emergence of new, interconnected risks (polycrisis, VUCA world) is not a new phenomenon, but the increasing frequency and severity of those risks in recent years makes risk management crucial to preserving company value, by helping organisations anticipate them and initiate proactive treatment measures.

In response to this ever-evolving risk landscape, the overall level of risk-maturity is rising across Europe. Corporate risk managers¹ are growing in prominence within their organisation, and the scope of their responsibilities is broadening. The value that risk management can bring to corporate strategy is increasingly recognised, and risk managers participate more frequently in Board and Executive Committee meetings.

There is still progress to be made, however, since the enterprise risk management (ERM) function remains underappreciated and underutilised in some organisations. Indeed, the value that the expertise of the corporate risk managers could bring to many organisations continues to be limited by a lack of clarity about the role of risk management, unclear governance structures and ill-defined capabilities.

That's why FERMA wants to elevate the standing of the risk management profession, building on its 2023 White Paper *The Roadmap to Strategic risk management*, to ensure that risk management receives the attention and resources necessary to protect and enhance organisational value. In order to achieve this goal, FERMA will work on four pillars:

1. Defining the profession;
2. Highlighting the importance of risk management;
3. Advocating for recognition; and
4. Guiding future developments.

The purpose of this discussion paper is to invite all relevant stakeholders to discuss the challenges facing corporate risk managers, focusing on three areas:

- **Corporate Governance**, i.e. the corporate governance options that determine the roles and responsibilities of a corporate risk manager,
- **Capabilities**, i.e. a descriptive and prospective capabilities framework, which will bring greater rigour to the definition of the profession of corporate risk manager.
- **Communication**, i.e. provide guidance to help corporate risk managers raise their profile and engage more effectively with other stakeholders.

¹ For the purpose of this discussion paper, "corporate risk manager" designates risk managers working at group level, and whose responsibilities include (but may not be limited to) ERM. Corporate risk managers may be known under other names in public-sector organisations. Additionally, risk managers who work in a subsidiary company but whose responsibilities are otherwise similar to those of a risk manager operating at group level will be considered to be a corporate risk manager for the purpose of this paper. The term has been chosen chiefly to distinguish corporate risk managers from (i) risk owners; and (ii) pure insurance managers – which are both outside the scope of this paper.

Based on your contributions to this discussion paper, FERMA will release a white paper in the coming months, addressing the issues raised and formulating recommendations to the European risk management community.

The Challenges facing Corporate Risk Managers

Corporate risk managers often face challenges that undermine the value that they could bring to their organisation. Those issues stem from various causes, from a lack of alignment on essential definitions regarding risk management to inadequate operating models, skills development and communication.

Lack of alignment on key risk management concepts

Firstly, corporate risk managers are confronted with difficult situations emerging from a lack of alignment between different functions regarding the definition of risks and the scope of ERM.

On one hand, managers and risk owners (i.e. commercial and operational teams, the first line of the Three Lines model) are increasingly aware of risks and of the need to properly manage them. But on the other hand, they often get confused about the distinction between an issue, a risk, an uncertainty or an opportunity.

Risk management policies and procedures usually provide only a very short definition of risks – for example: “Events and conditions that could prevent the organisation from achieving its objectives or the effects of uncertainty on objectives”. While compliance, financial and operational risks are well identified and classified, business risks at all levels (i.e. strategic, operational and tactical) are less well-documented, and governance not as well established between the risk owners and corporate risk managers. Moreover, opportunities are often mentioned in policies but not addressed further in procedures and methodologies. In practice, it is often unclear how opportunities are to be addressed as a part of ERM.

The lack of a clear risk definition and a risk methodology, including qualitative versus quantitative assessments, impact and probability, and scenario thinking, makes it difficult for corporate risk managers to contribute to short- and mid-term business planning. For risks beyond the planning horizon, very often defined as “emerging” and/or “strategic” risks, no clear methodology exists.

As a consequence, there is also a lack of clarity on what the corporate risk manager is expected to deliver. In other words, there currently is no consensus on what the corporate risk manager is responsible for or on the role they play in the organisation. For example, is the corporate risk manager responsible for assessing the risk identified by the risk owner? How do they assess whether risk management measures are appropriate and/or adequate? On what basis do they provide an assessment regarding risk management? What assurance is expected from them? How can they contribute to a risk-reward discussion and decision making?

Unsuitable governance structures

Regarding governance structures, the existing ERM frameworks (e.g. COSO ERM, ISO 31000) are, unlike the professional norms of Internal Audit (IA), excessively broad and not mandatory. As a consequence, every organisation interprets and applies risk frameworks and scope differently. For example, whereas IA professional norms clearly state that the Chief IA Officer (CIAO) reports to the President of the Audit Committee of the Board, there is no such rule for the Chief Risk Officer’s (CRO) reporting lines. In practice, some report to the CFO, some to the General Secretary, some to the CEO and others don’t even have a direct reporting line into the leadership team. There are even cases of heads of ERM reporting to the CIAO, which blurs the delineation between the second and third lines.

Similarly, there is a wide variety of practices with regards to the scope of the CRO/Head of Risks. Some deal mostly with financial and/or operational risks, while others embrace a 360° view of risks. Moreover, multiple actors are involved in 'sectoral' risk management, but they seldom agree on which risks must be managed by whom. Organisations lack efficient and practicable organisational structures defining and differentiating the responsibilities and reporting lines between Internal Audit, Compliance, Sustainability, Risk Management and Insurance (Risk) Management. Also, insufficient coordination between participating functions and the absence of unified methodology to assess risks create difficulties in leveraging operational risk management for strategic risk management purposes.

As a result of inadequate operating models, corporate risk managers are not systematically involved in strategic decision-making – such as strategic planning, investment decisions or new products. This is problematic, as these decisions are closely linked with the corporate risk manager's role in defining the organisation's risk appetite, so excluding them from the conversation goes counter to proper risk-based decision-making.

Lastly, corporate risk managers' positioning in their organisation often doesn't facilitate risk communication. Since risk management functions operate in silos under Safety and Security, Finance, Internal Audit, or other business units, effective enterprise-wide risk communication is hampered. This leads to delays in the sharing of critical information, particularly when the corporate risk manager is not part of the leadership team; all too often, decision-makers come to corporate risk managers after the fact instead using their expertise to inform the decision.

Skills and training issues

Moreover, corporate risk managers are expected to have a broad set of capabilities (i.e. skills and tools which allow them to fulfil their role), which brings its own set of challenges. In theory, corporate risk managers must possess technical skills, analytical skills, interpersonal skills, leadership and management skills, technological proficiency, industry-specific knowledge, continuous learning and adaptability and certification and education. This expectation is, however, challenged in practice.

Firstly, corporate risk managers may lack certain capabilities, since advancing along the maturity curve requires broader skills, such as enhanced soft skills, to integrate risk management into business processes and strategic decision-making beyond basic compliance requirements. It must also be noted that in some cases, corporate risk managers also lack technical capabilities, not just soft skills.

Secondly, the huge range of topics that ERM *should* cover might put into question the *actual* ability of the corporate risk manager to effectively master every one of them. In practice, there are many different types of risk managers including operational risk managers, financial risk managers, risk & insurance managers, risk managers for specific risks, business continuity managers, crisis managers etc. On one hand, despite their diverse roles, they all share a common foundation of essential universal capabilities that connect them across different areas of risk management. On the other hand, risk managers advancing along the maturity curve and stepping up in seniority need to be able to build teams with different specialists that can effectively work together and collaborate with stakeholders.

Thirdly, situations exist where adequate technical capabilities are perceived by the decision makers as over-engineered processes, leading to dissatisfaction when such sophisticated or very technical approaches don't improve practical risk insights and decision making. Therefore, corporate risk managers need to be equipped with a toolbox to tailor their approaches depending on the organisational context and objectives of the required decision.

The underlying issue is a lack of consensus on how corporate risk managers should be trained. This stands in sharp contrast to other regulated professions, which have a clear concept of the capabilities needed for the job and require their members to obtain a recognised professional certification demonstrating them.

Difficulties in Risk Communication

Corporate risk managers also need to coordinate with multiple stakeholders. As the business environment grows more challenging, the need for greater agility and timely communication intensifies, which results in a higher frequency of ad hoc reporting requests. Corporate risk managers must present and communicate information on strategic, operational and tactical dimensions to different levels of stakeholders. As risk-based decision-making frameworks become more common, corporate risk managers must differentiate themselves from other functions reporting on risks to stay relevant and provide value. As a result, corporate risk managers must have differential communication skills and establish rapport with various stakeholders, adjusting their approach to suit the audience.

However, corporate risk managers sometimes struggle to tailor their message to their audience. They may not always adopt a business-oriented perspective. Additionally, excessive use of technical terms and jargon often makes their message difficult to understand, creating a disconnect between risk language and business language.

Open Questions and Recommendations

FERMA aims to address these challenges, to allow risk management to fully deliver on its strategic benefits for organisations across Europe. This means reassessing the position of the risk management function within the organisation, defining more precisely the responsibilities and capabilities expected of corporate risk managers, and eliminating obstacles to effective strategic engagement. The following section outlines FERMA's intended approach to solving these issues, as well as open questions to help guide its final recommendations.

On Governance

1. Does the definition and scope of ERM need to be clarified within and across organisations?

FERMA should develop best practice guidelines for defining risks, through definitions and illustration of risk universes², and opportunities that can be adjusted to the individual need, with a focus on business risks. FERMA recommends applying to business risks the commonly used principle for financial and operational risks, while adapting it to capture opportunities – i.e.: “Events and conditions that could prevent the organisation from achieving its objectives or lead to opportunities which could arise from the same event”. This general principle should be elaborated upon to align the perception of risk and opportunities within and across organisations but would nonetheless provide a solid foundation for corporate risk managers to become a natural part of the business planning process and strategic decision-making.

Moreover, there need to be guidelines for end-to-end processes to integrate opportunities in an ERM approach. These guidelines should focus on the articulation of opportunity management with strategic planning, innovation and operational excellence.

1.1. Should the definition of risk universes be standardised within an organisation in line with FERMA's recommended general principle?

² A risk universe is a comprehensive catalogue of all potential risks that an organisation might face.

- 1.2. *Should the definition of risk universes be standardised across different organisations in line with FERMA's recommended general principle?*
- 1.3. *Should FERMA develop guidance to better identify and assess opportunities as part of the ERM process?*

2. Does the expected role and responsibilities of corporate risk managers need to be clarified?

FERMA should develop recommended mission statements for corporate risk managers, to clarify their responsibilities and role in the organisation and what assurances are expected of them. Such recommendations should constitute a baseline to define the responsibilities of risk managers of all kinds and could be further complemented to reflect the specific risk management needs of a given organisation.

Moreover, FERMA should clarify the expected contribution of corporate risk managers to corporate strategy, for example as it relates to strategic planning, investment decisions or the development of new products.

- 2.1. *Should FERMA provide guidelines outlining the responsibilities of corporate risk managers through recommended mission statements?*
- 2.2. *Should FERMA clarify the expected involvement of the corporate risk manager regarding corporate strategy?*

3. Does the IIA's "Three Lines Model" help corporate risk managers play a strategic role within their organisation?

FERMA should develop a standardised operating model describing the role of the corporate risk manager in relation to other stakeholders, namely: internal controls and internal audit; insurance management; other corporate functions (compliance, sustainability etc.) and their respective reporting lines; and the Board, as it is responsible for the oversight of the risk management function.

Moreover, FERMA should develop a recommended framework outlining key principles about the governance of an organisation's risk management function. These principles should remain general so as to be applicable to organisations of all sectors, and strive towards a more independent, transparent and integrated risk management function that is embedded in leadership and contributes to strategic decision-making.

- 3.1. *Should corporate risk managers be actively involved in risk treatment, including by deciding on and controlling the implementation of appropriate measures?*
- 3.2. *Should corporate risk managers leverage data from loss-event monitoring, results of internal control assessments (i.e., the efficiency of internal controls), and conclusions of internal audit (i.e., controls efficiency) to support and challenge risk owners in assessing risks?*
- 3.3. *Should insurance management be part of the corporate risk management function?*
- 3.4. *Should FERMA provide guidance to improve the application of ERM processes by other corporate functions?*

- 3.5. *Do you think that corporate risk managers should have a direct line of communication to the Board?*

On Capabilities

4. Do the capabilities expected from corporate risk managers need to be clarified?

FERMA should develop a European Unified Capability Framework as a constitutional guiding framework to ensure pan-European consistency and future thought leadership. Such a framework should be based on the rimap© certification, building up on the work done at national (e.g. AIRMIC, AMRAE) and international level (e.g., PARIMA), by related organisations (e.g., ISO, RMA e.V.) and continuously evolve and adapt.

Linked to such a European capability framework, mandatory professional certification should also be envisaged as a requirement to access the profession to ensure quality and consistency of required capabilities of corporate risk managers, replicating the model of other regulated professions.

Finally, national risk management associations should take a more proactive role in the diffusion of knowledge and best practices. Such practical capability support could take the form of roundtables and exchanges for its members, where risk management capability success stories and failures can be openly discussed to ensure continuous practical learning, and should be aligned with the aforementioned Unified European Capability Framework.

- 4.1. *Is the current offer of professional risk management training and certification adequate to meet current and future expectations?*
- 4.2. *Do corporate risk managers need to upskill and/or reskill in order to meet future expectations?*
- 4.3. *Should FERMA develop a European Unified Capability Framework based on the rimap© certification and other existing frameworks?*
- 4.4. *Should mandatory certification requirements to enter the risk management professions be enforced at EU and/or national level?*
- 4.5. *Should national risk management associations take a more proactive role in offering practical capability support to their members?*

On Communication

5. Do corporate risk managers need guidance to better communicate complex risk information to all relevant stakeholders?

FERMA recommends that corporate risk managers develop their communication skills. Firstly, risk information should be customised and communicated to stakeholders at various levels—strategic, tactical, and operational—according to their specific roles and goals. Corporate risk managers need to align the information with stakeholders' priorities by understanding the audience in advance, connecting the dots for them, and anticipating potential pushbacks or additional questions it may have.

Risk communication should emphasise the 'so what', informing top management about what is new and how it directly affects the organisation's value and strategy. Secondly, corporate risk managers must speak the language of their audience and avoid using 'risk jargon' when engaging with other

stakeholders. They may additionally follow communication training and be encouraged to acquire concrete business experience in operational, tactical and strategic risks.

Corporate risk managers should have access to the information they need (e.g. Board meeting minutes, management committee information, organisational financial and performance information, invitation to top management meetings, etc.).

Moreover, corporate risk managers should use tools to inform and engage the audience. Corporate risk managers should have efficient risk communication tools to support the Board and Top Management Team in predicting and addressing risks, helping to achieve strategic objectives. They should develop standardised and automated reporting dashboards, formats and templates for communicating risks for different stakeholders simply and clearly – these tools should be adapted to the needs of the companies and different stakeholders. They should also look into AI as a tool to enable quick risk reporting.

Finally, FERMA should develop guidance for risk communication and reporting, notably on: defining communication objectives; identifying stakeholders and their needs; identifying the most appropriate medium for risk reporting/communication; defining the frequency of reporting; and monitoring and evaluating the effectiveness of risk communication.

- 5.1. Do corporate risk managers have access to every piece of internal documentation that is necessary to fulfil their role?*
- 5.2. Should corporate risk managers leverage innovative tools and approaches in order to facilitate effective risk communication?*
- 5.3. Should FERMA develop guidance for effective risk communication and reporting?*

6. Are corporate risk managers successful in demonstrating the value that they bring to their organisation's strategic decision-making?

Corporate risk managers should demonstrate how risk management directly supports the achievement of business goals. By showing how risk treatment strategies contribute to the organisation's long-term success, they can prove their relevance to strategic decisions. Risk managers should always link their analysis and action to value at enterprise level and to the organisation's objectives

- 6.1. Does ineffective communication on the value of risk management prevent corporate risk managers from achieving a more strategic role?*
- 6.2. Do risk managers need to stress more the contribution of risk management to the organisation's objectives and value?*

Next Steps

To contribute to the discussion, you can answer the questions raised in this paper by answering the attached online questionnaire [\[link\]](#) by 30 June 2025, 23:59 CET. FERMA will develop the recommendations formulated in the discussion paper based on the feedback received during the consultation. Those recommendations will be consolidated in a white paper on the future of the risk management profession, which will be released in Q4 2025.