Effective board-level risk oversight

Practices and principles

home.kpmg/be

Table of contents

Introduction

Today's businesses navigate a complex and rapidly changing environment. Macroeconomic uncertainty, climate change, geopolitical turbulence, and accelerated technological evolution are creating extraordinary challenges for organizations and their boards of directors. On top of these uncertainties, the recent global pandemic and the resulting emergency measures taken by various governments have been causing unprecedented business disruption. In these turbulent times, robust board leadership is more important than ever. As part of their oversight duties, boards are responsible for making sure their organizations have put in place the necessary risk management framework and policies to deal with the consequences of unforeseen events. Despite the increased interest in risk governance since the 2008 financial crisis, we know relatively little about actual board practices and how the board's role in overseeing risk has evolved in recent times. Vlerick Business School and KPMG joined forces to shed light on how board directors perform their risk oversight duties and to learn from the successes and challenges they face in the pursuit of sustainable value creation. This study combines extensive practitioner experience with solid academic rigor and provides a unique insider look into the boardroom.

The first conclusion from this study is that there is an increased general recognition of the critical importance of board-level risk oversight, beyond compliance. Second, there is a growing appreciation that, when implemented properly, formal risk oversight strengthens rather than impedes entrepreneurial activity. Third, effective risk oversight is supported by an appropriate board-level structure and processes. Essential governance design choices relate to the risk governance structure, formal risk oversight process, and risk reporting to the board. Fourth, board risk oversight relies on creating the right culture to guide appropriate risk taking at all levels in the organization. Finally, there is still some work to be done to integrate strategy and risk effectively at board level, both in terms of embedding risk in strategic decision-making and setting the desired risk appetite in line with stakeholder expectations. We conclude that there is no one-size-fits-all approach to board-level risk oversight. The differences in board practices reflect the nature, scale, and complexity of the organization's activities, as well as the ownership structure and the board's vision on risk-taking. That said, we believe several principles highlighted in this report are relevant to both large and smaller organizations across a wide range of different industries.

We hope this report will provide inspiration for board and committee chairs by documenting the risk oversight practices of a cross-section of organizations and industries. Today's uncertain business environment presents a unique opportunity for boards to test the strength of their organization's risk governance structures and processes. Our study offers useful insights on the challenges and potential gaps to address. We leave it to the individual board members to decide which of the practices highlighted in this study are most relevant to implement as part of their efforts to enhance the effectiveness of their board-level risk oversight.

Regine Slagmulder
Full Professor of Accounting & Control
and Senior Partner at Vlerick Business School

Research methodology

The findings from this report are based on 20 semi-structured interviews conducted with chairmen of boards and audit committees from a wide range of organizations and sectors, including manufacturing, telecom, retail, chemicals, and real estate. The participating organizations vary from large, listed organizations to privately owned organizations, including SMEs and non-quoted family firms, to entities that are part of multinational groups or where the state is a majority shareholder. Most interviewed board members, especially the non-executive directors, are serving on the board of multiple organizations, which enabled us to collect information on board-level risk oversight activities in a large set of organizations. The research focuses on Belgium-based organizations, although several of them are multinational in their operations.

We want to take this opportunity to thank the board and audit committee chairs interviewed for this study, for their time and candor in discussing their organizations' practices and challenges in the domain of board risk oversight. To protect our respondents' anonymity, we have deliberately chosen not to identify individuals or organizations throughout the report.

Risk oversight: a framework

Today's businesses navigate a complex and rapidly changing environment. Risk oversight in the broad sense is a key component of corporate governance. It refers to the boundaries in which the organization wants to operate to achieve its objectives, on the one hand, and ensuring that these boundaries are respected, on the other hand.

These boundaries are defined by four cornerstones:

1. The level of risk the organization is willing to take to achieve its objectives;
2. The compliance requirements applicable to the organization;
3. The policies and procedures put in place by the organization;
4. The culture and behavior the organization wants to establish.

Risk oversight involves:

- The board, the risk and audit committee(s) in charge of validating the framework and overseeing the risk management activities
- Management (first-line functions) in charge of implementing the framework
- The second-line functions (risk, internal control, compliance, health & safety, etc.) in charge of setting standards and providing oversight for specific risk and compliance domains
- Internal Audit (third-line function) in charge of providing independent and objective assurance to the risk and audit committee
- External stakeholders who rely on the risk & internal control framework and process of the organization (shareholders, external audit, regulators, etc.)

Belgian Corporate Governance Code 2020, article 2.14: "The board should approve the framework of internal control and risk management proposed by the executive management and review the implementation of this framework."

Code Buysse III

- article 8.2: "It is the board's duty to define the risk management policy of the organization." …"the board performs oversight on its implementation."
- article 8.3: "The board of directors has to ensure that management implements a proper system of internal control"

The KPMG Take

Board-level risk oversight is on the rise, now more than ever

We observe a growing awareness of the importance of effective board-level risk oversight. All participants in the study concur that it is important for board members to dedicate sufficient time to discuss the risks that might impact long-term value creation for the organization, as opposed to focusing merely on reviewing past performance or compliance matters. Rather than seeing risk oversight as a routine exercise in operational loss prevention and compliance, the interviewees generally agree that boards have a strategic role to play in overseeing the risks their organization is faced with. This role has become increasingly challenging, as today's business ecosystems are more dynamic and interconnected than ever before. The board chair of an industrial organization put it as follows:

> *"Proper risk oversight implies that the risk dimension is continuously considered in all of your board discussions. It is the task of the audit and/or risk committee to ensure this is done in a systematic and comprehensive way so that nothing is overlooked. The purpose of a risk assessment is to take a step back and look from a distance at the major risks and trends observed in the organization and in the broader environment (e.g., IT security risk, digitalization), and ask yourself: how well is the organization – and the board – prepared for this?"*

Disruptions, such as the COVID-19 pandemic, are an acid test of the maturity and robustness of board-level risk oversight. These events not only put organizations' risk models and processes to the test, but also stretch the organization's ability to capitalize on opportunities presented by the disruption. Both are essential to the organization's survival and long-term prosperity, thus underscoring the importance of adequate risk oversight.

Risk oversight starts with asking the right questions

Audit and risk committee discussions on risk matters are often triggered by events reported in the media, internal incidents, or questions and requests from stakeholders. These are important and valuable discussions, but they should go together with more structural questions and reflections at board level, such as:

- Do we have a view of the global risk landscape of the organization?
- Which mechanisms are in place to ensure that risks are managed in accordance with the organization's risk appetite?
- How do we ensure that the activities of the three lines of defense are properly coordinated to limit the cost of assurance, to avoid gaps and overlaps in the risk landscape, and to ensure integrated risk reporting?
- Do we have the necessary competences and experience on Governance, Risk & Compliance available in the organization and the risk committee?
- How are our risk and strategy processes aligned and which mechanisms do we have in place to identify emerging risks and signals of change?
- Do the organization's culture, code of conduct, human resource policies and performance management and reward system support the risk management and internal control system?
- Which internal audit activities and processes are in place to provide independent and objective assurance on risk management activities and the organization's key controls?
- If disruptive events occur, how are we organized to deal with these in terms of Business Continuity Management, Crisis Management and Disaster Recovery?
- What and how do we learn from previous incidents?

The KPMG Take

Professional risk oversight and entrepreneurship go hand in hand

Several respondents highlight regulatory pressures as one of the factors driving the adoption of formal risk oversight systems. At the same time, they are aware that a compliance-oriented mindset to risk oversight might lead to a "box-ticking" attitude. Those who have served on boards in regulated industries, such as financial services, are particularly sensitive to this unintended consequence, but they appreciate the benefits of applying a professional approach to risk oversight. Most interviewees are in favor of implementing formal risk oversight practices also in non-regulated sectors. One interviewee uses the analogy of a sports car:

> *"The faster you want the car to go, the better the brakes should be. The more entrepreneurial you want to be as a organization, the better your risk management should be to map your risks and keep them under control. Because if you want to go fast, things can get out of control quickly and with major impact compared to a slow-growth, stable organization."*

The board members in our study insist on a pragmatic approach to risk oversight that avoids creating rigid structures and processes. In principle, they see no problem reconciling sophisticated risk governance with the need for entrepreneurship to the extent that formalization does not create a false sense of security or blindside management from leveraging opportunities.

Implicit versus explicit risk management and oversight

Can risk management and risk oversight work without implementing a formal risk management framework and process?

In principle yes – in the same way an organization can buy goods and services without a procurement process and sell without a sales organization. However, in our opinion and supported by corporate governance requirements, a professional organization does require a risk management framework and process.

Should this be a heavy and costly set-up that negatively impacts the entrepreneurship of the organization?

Absolutely not: the art lies in the design of an enterprise risk management (ERM) operating model that fits your organization.

The KPMG Take

Effective risk oversight requires the right structure and processes

Our in-depth interviews with seasoned board and audit committee chairs reveal that to perform effective risk oversight, directors need to carefully consider both the way risk governance is organized, as well as its operating processes. Three governance aspects are identified as essential in this respect – the risk governance structure, a formal risk oversight process, and risk reporting to the board.

Risk governance structure

Effective risk oversight requires the appropriate assignment of responsibilities to a board-level audit and/or risk committee that acts as an advisory committee to the full board. In most organizations included in our study, the audit committee is tasked with leading the board's risk oversight activities, on top of its responsibilities with respect to financial reporting and internal control. The audit committee is also often the driving force behind the professionalization of board-level risk oversight. In contrast with financial institutions, where a risk committee at board level is mandatory, none of the organizations studied has established a separate risk committee because of size limitations and the potential overlap in membership with the audit committee. Potential disadvantages of not having a dedicated board-level risk committee in place are the likelihood of a more limited focus on non-financial reporting risks and the lack of specific risk competences and experience.

Some of the larger organizations in our sample have a risk committee at management level that coordinates the risk assessment process and risk reporting to the executive committee and the audit committee. In contrast with financial services organizations where a chief risk officer (CRO) is mandatory and a member of the executive committee, few of the interviewed organizations have a dedicated CRO who has direct access to top management and the board. Those that have a risk function often combine the role with internal audit (IA) or insurance. One audit committee chair comments on the three lines (of defense) model that is commonly used in structuring risk oversight:

> *"In many non-financial sector organizations the second line of defense (risk management, internal control, and compliance) is only minimally present – and in smaller organizations often not present at all. Here the responsibility for risk management lies with the first line (i.e., management), and the third line (i.e., IA) performs the supervision. However, the larger and more complex the organization, the more the risk oversight should be structured according to the three lines of defense."*

IA is often described as the "eyes and ears" of the audit committee. An interviewee insists that, because of the need for independence and, in line with the Institute of Internal Auditors (IIA) standards, the correct approach for IA is to report to (the chair of) the audit committee, and to the CEO – although in practice it is sometimes to the CFO or legal counsel. In some larger organizations, it's possible that IA also has direct access to the chair of the board. Several interviewees emphasize the need for close collaboration and coordination between IA and the risk management function to avoid duplication of efforts. One of the challenges highlighted by a director from a large, listed company is the integration between, on the one hand, the risk assessment performed by the management and, on the other hand, the work of IA, which is analyzing the risk universe and proposing their audit plan. Alignment between risk management and IA is considered particularly challenging in regulated environments in terms of streamlining the definition of the risk universe and a single tracking of risks, actions, and issues.

The right risk governance structure for your organization

As illustrated by this study and aligned with our KPMG experience, very different governance structures are observed related to risk oversight, if not prescribed by regulatory requirements (cf. the financial sector). Dedicated risk committees (instead of combined risk and audit committees) are not common practice yet in the non-financial sector although this might evolve in the future. The advantage of dedicated risk committees (at board, strategic, and operational level) is that they allow for an increased focus on risks beyond financial reporting. In addition, directors with relevant competences and experience related to Governance, Risk & Compliance are not always represented in the combined audit and risk committees. This obviously impacts the intensity and quality of the risk oversight function. A potential disadvantage of separating the risk committee from the audit committee is that it may create a silo-approach towards risks and controls.

Banks have a CRO who is accountable to the board for risk oversight, with direct reporting lines to the chair of the Board Risk Committee and/or the Audit Committee, as well as to the CEO. Outside of the banking sector very different practices are observed concerning the positioning and reporting lines of the CRO. Irrespective of the chosen positioning, leading practice is to have a CRO with direct access to, and support from, board and C-level, and clearly defined mandates, roles, and responsibilities across the three lines of defense and governing bodies.

Formal risk oversight process

Most organizations in our study perform a formal risk assessment at the request of the board, typically on an annual basis. It consists of comprehensive risk mapping and analysis to ensure that management is properly reflecting on the risks the organization is facing and taking appropriate measures to mitigate them. In organizations with a sophisticated approach to risk oversight, an independent risk function – often IA – takes the lead in coordinating the risk assessment based on input from the management team. The outcome of this exercise is reported in detail to the audit committee, with a summary going to the full board. The management team is then responsible for developing and executing an action plan based on the risk assessment, which is followed up in the (quarterly) audit committee meetings.

A few board members in the sample express their concern that the standard annual risk assessment may not always provide the board with fresh insights on strategic or emerging risks. Traditional risk management often limits itself to reporting on the likelihood and impact of a set of identified "known" risks to support resource allocation decisions and compliance requirements. These types of exercises, however, provide limited insights into unexpected or atypical risks. To counter this problem and get the most value out of the risk assessment, several of our sample organizations opt for a less frequent but more targeted form of engagement (for example, once every two to three years) instead of a fixed annual process. This approach is explained by the following board member:

"Our scheduled risk assessment exercise happens approximately once every two years. This frequency is considered sufficient because it allows the organization and the risks to evolve. The frequency is largely decided by the board as certain events trigger the need to revise the risks; for example, our organization has done several acquisitions in recent years, which may entail new risks."

One organization uses a two-year cycle and alternates as to who takes the lead of the risk assessment process. One year it is a bottom-up initiative driven by management, the other year it is more of a top-down risk oversight exercise led by the audit committee. This approach not only serves to reduce the burden on the management team of having to perform a detailed analysis every year but also provides an opportunity for the audit committee members in the board to thoroughly reflect on the organization's risks. In a few organizations, the board does not follow a calendar-driven approach to their risk oversight activities but prefers an ongoing dialogue with management.

Some of the interviewed directors feel there is still some room for improvement in terms of further structuring and formalizing the analysis, elaboration, and follow-up of the action plans. They emphasize the importance of devoting sufficient time at every board meeting to pressure-test the progress management is making on the risk mitigation actions. At one organization, for example, the board drives a strong focus on action by making sure all the members of the management team have a designated responsibility for the risks included in the risk map.

Risk reporting to the board

Risk reporting is key to ensuring the board has a clear understanding of the risks included in the organization's strategic and financial plans, as well as management's preparedness to take the necessary risk mitigation actions. A risk report to the board typically contains a description of the top risks to be discussed in the audit and/or risk committee and the full board (e.g., strategic risks, compliance risks, financial risks, IT risks, etc.). It also features a visual representation of the impact versus likelihood (or frequency of occurrence), based on the risk assessment performed by management. The risk information is delivered to the board in a summary form, such as a heat map, to avoid information overload and enable productive decision-making. Contrary to the financial sector, where all the risks are quantified in financial terms (e.g., expected losses), risk reporting in non-financial firms is often based on a qualitative assessment of impact and likelihood.

The organizations in our study, especially those with well-developed formal risk oversight, appear to have a system of timely reporting on the risks and the corresponding actions to the board. Board members find it important to ensure that the flow of information to the board keeps pace with changes in the business and risk environment, as one director explains:

> *"If your risk report comes up with very different things than what you have included in your mid-term strategy, then I think you have a major problem. Of course, some risks that were previously identified but not yet considered a threat, could always evolve into a hazard. But if a completely new risk suddenly pops up in the report that is life threatening for the business, it means you did not see it coming."*

To ensure that the information going to the board stays relevant and does not lead to complacency, some organizations pay specific attention to new trends and emerging risks. In most organizations, the responsibility for identifying these emerging risks lies more with the strategy or management team than with the risk professionals.

Despite our interviewees' overall satisfaction with their organization's risk reporting to the board, several board members are skeptical of overly detailed risk reporting systems that require a substantial amount of input from across the organization. Such reporting is seen as requiring major effort with relatively little added value for the business. In some organizations, the risk reporting is integrated into the standard management reporting instead of being delivered as a separate report to the board. Another, more high-level report that informs the board about potential risks the organization could be facing, is the CEO activity report. It provides an overview of the evolution of the business and trends in the broader environment and is usually discussed at the start of the board meetings.

Culture is king

In evaluating the effectiveness of an organization's risk management, the primary attention of the audit and/or risk committee members tends to go to the risk control systems and procedures the organization has put in place. However, it is important to also put a behavioral lens on how risks are managed and consider how the organizational culture impacts the risk management environment. An organization's risk culture refers to the employees' mind-sets and behaviors based on a shared understanding of the key risks.

Most of our interviewees stress the importance of fostering the right risk culture to help create risk awareness in the organization. By encouraging timely identification and escalation of risk issues, it provides the board with additional assurance on the effectiveness of the organization's risk management processes. Most of our interviewed board members acknowledge the difficulty of dealing with the concept of risk culture in an explicit, structured manner. All of them, however, underscore the importance of the so-called tone-at-the-top in the context of risk, as expressed by this board member of a retail organization:

> *"The chair of our audit committee considers risk assessment an absolute priority. He makes it very clear to all the managers involved that this is not a box-ticking exercise but something they should take seriously and put in the necessary effort."*

The emphasis on values and culture is common practice in family firms, where the reference shareholder's long-term and prudent vision of running the business tends to pervade the organization. The directors from family firms in our study reveal that the presence of family members on the board of their organization encourages the right level of managerial risk-taking within the boundaries of the family's risk appetite. In these cases, culture is viewed as a meaningful complement to – and even substitute for – formal risk procedures.

Making risk culture tangible

A sound risk culture encourages transparency and open dialogue across the three lines of defense. In order to establish a sound risk culture the board should define the key characteristics (see below) of the target risk culture of the firm and demonstrate the right tone at the top.

In practice, organizational culture is often referred to as a reason why the risk management and internal control system (partially) fails. Whereas almost all organizations recognize the importance of risk culture, only a few have a clear strategy only a few have a clear strategy on how to make risk culture tangible.

To address this, KPMG's risk culture framework distinguishes eight risk culture drivers/components (see Illustration 1):

1. **Clarity:** the desired risk framework and risk appetite are clear to management and employees;
2. **Visibility:** behavior of management and employees is sufficiently visible;
3. **Involvement:** management and employees feel called to actively uphold the organization's interests;
4. **Role modeling:** management sets the right risk management example;
5. **Practicability:** there is sufficient time, resources, information, capacity, and authority to fulfil risk management responsibilities;
6. **Openness:** management and employees feel comfortable discussing (latent) risks and there is an atmosphere of challenge and mutual respect;
7. **Enforcement:** decisions are acted upon, desired behavior is rewarded and inappropriate behavior is discouraged;
8. **Improvement:** people learn from mistakes and incidents (root cause analysis).

In order to have a clear baseline, it is recommended to measure the current risk culture through a survey, interviews or internal audits. This will allow the organization to define an action plan bridging the gap between the current state and the desired risk culture.

The table below provides an overview of the cultural drivers as well as the entity level instruments that can be used to influence them.

	Cultural drivers		Entity level instruments (examples)
Knowledge & Understanding	Clarity	Visibility	— Strategic objectives and key risks — Role descriptions and expectations — Policies and processes — Organization values — Code of conducts — Risk manual, Risk Control framework — Risk appetite
Belief & Commitment	Involvement	Role Modeling	— Information/communication moments — Planning — Clear governance — Management messages — Part of (management) agenda — Minutes
Competencies & Context	Practicability	Openness	— Access to expertise — Competency profiles — Processes stimulating consideration — Tools: workshops, assessments, E-learning
Action & Determination	Enforcement	Improvement	— Escalation procedures, incident reports — Indicators — Root cause analyses and recommendations — Risk dashboards, monitoring process

Illustration 1. KPMG's risk culture framework

Integrating risk and strategy in board-level decision making is key

Most of our interviewees believe the board has a strategic role to play when it comes to risk oversight, not only by protecting the business from threats, but also by helping identify and exploit opportunities to maximize sustainable value creation. The boards in our sample are taking various steps to connect the dots between their strategic and risk oversight responsibilities. One way to integrate risk and strategy at board level is by embedding risk in their strategic decision-making processes. Another is for boards to set the desired risk appetite in alignment with the organizational strategy, which serves as a guideline for managerial decision-making.

Embedding risk in the board's strategic decision making

We observe in our study that risk is increasingly included as an important element in board-level decision-making. The integration between strategy and risk is typically accomplished through relatively simple processes, such as a brief management presentation during the annual strategic planning exercise about the risks that they foresee in achieving their business plan and which actions are planned to contain those risks. In some of our sample organizations, strategy and risk are connected in an implicit, ad-hoc manner during board-level discussions about strategic initiatives. While such an informal approach to risk oversight appears to satisfy some boards' needs, directors do acknowledge that it may expose the organization to unnecessary risk in the pursuit of value-creating opportunities.

A limited number of organizations in our study establish a formal link between risk management activities and the strategic planning and review process all the way up to board level. The directors of these organizations indicate that the risks associated with specific strategic options are a standard item on the board agenda during the strategy-setting phase. An audit committee chair describes the different channels through which risk enters the organization's strategic dialogue at board level:

> *"First, risk is included in the monthly reporting to the board about the current performance of each business unit and the strategic outlook in terms of market trends, competitors, technology and innovation, people issues, etc. Second, once a year a strategy review meeting is being held, where the board and the management decide on the strategic direction of the organization, taking into consideration the strategic risks and opportunities. Third, during every quarterly board meeting management updates the board on the progress being made in the execution of the strategy and any risks encountered along the way."*

A telecom organization in our sample explicitly integrates the input from their ERM cycle into the strategic planning process. The outcome of the detailed risk assessment performed as part of their ERM process (impact-likelihood analysis and risk mitigation actions) is discussed extensively in the audit committee and subsequently inserted into the strategic plan presented to the board for approval.

Aligning strategic decisions with the organization's risk appetite

An important risk oversight responsibility of the board is to define the organization's risk appetite and ensure that it is respected when management makes strategic decisions. For example, an executive director of a family business describes how his organization's risk appetite is based on two elements – business continuity and debt ratio. The business continuity factor stems from the family's desire to build a business for the next generation(s), which leads them to say "no" to any risks that could jeopardize the firm's existence. The second criterion is linked to the financial health of the organization and mandates the rejection of project proposals that exceed certain debt limits. All managers in the organization know these principles and understand the rationale when one of their proposals gets rejected.

While financial sector organizations have a tradition of estimating risk in financial terms, most directors in our study admit to the difficulty of expressing risk appetite in a quantified manner. Instead, most boards define risk appetite qualitatively as the types or levels of risks their organizations want to avoid, or less explicitly, by fostering the right organizational culture towards risk. A board member describes her organization's approach to making strategic decisions in line with the risk appetite as follows:

"Our board has a clear opinion about what the risk appetite should be and what level of risk can or cannot be accepted. For major decisions, such as investment projects or acquisitions, the board asks management to analyze different scenarios based on different hypotheses or assumptions, market conditions, and other business parameters so that they can discuss and decide what proposals are acceptable and in line with the desired risk profile."

Risk & strategy alignment as key success factor

The right starting point for risk management is the organization's strategy and its derived operational objectives. Jumping into risk management activities without a clearly defined strategy and related objectives is a mistake observed mainly at organizations that have implemented risk management with a "tick the box" approach.

Aligning the organization's strategy cycle with the risk management process allows for proactive reflection on risks when defining and evaluating the different strategic options. We encourage the positive evolution where risk managers get a seat at the table when strategy is being discussed. Indeed, risk management should be able to provide insights when defining the organization's strategy and not only receive the strategic plan as a given.

The KPMG Take

No one-size-fits-all approach

The board members we interviewed acknowledge that there is not a single optimal approach to risk oversight and directors must think pragmatically about how they want to govern the risks of their organizations. The specific approach any given board uses to perform risk oversight is influenced by several factors, such as the type of industry and regulatory context, the size and complexity of the business, the ownership structure, the board's vision on risk taking, and the overall maturity of the organization's internal governance. Directors with experience in the financial services sector indicate that these boards' risk oversight approach is very structured and formalized because of the regulatory requirements (e.g., the mandatory presence of a board-level risk committee). In contrast, boards of SMEs and family-owned businesses appear to be mostly implicit in their approach. In those organizations, risk discussions are part of the board's strategic reflections on how to react to new market developments, diversify the organization's portfolio, or reduce leverage. The board's follow-up of the risks is then embedded in the quarterly review of the operational results.

Most directors of family-owned businesses in our study reveal that their boards tend to be more focused on business opportunities than on formal risk management. The corporate culture and values around risk-taking expressed by the family members in the board appear to compensate for the lack of explicit risk management processes. Nevertheless, there is a growing awareness that systematic risk identification, assessment, and monitoring processes enable the organization to confidently take on risks (in terms of new products, new markets, and new processes) to create future growth. Several directors see formalization as a useful driving force to start the necessary risk conversations, as testified by this independent director of a large retail organization:

"Making things transparent to the board is not the most important motivation for having a formal process. Only the 10% most significant items are reported at board level, so the board is just the final capstone of the whole process. However, what is important is that those top risks, as well as the other 90%, get on everybody's radar, that employees at different levels discuss them and think of ways to deal with them. Risk oversight is first and foremost about creating a culture of awareness and action."

Our observations demonstrate that every approach to risk oversight has its own strengths and weaknesses. It is important to strike the right balance between "hard" and "soft" risk controls depending on the context and needs of the organization. The concepts of risk appetite and risk culture are common elements across the different approaches. They are supported in varying degrees by formal governance structures and risk reporting systems to provide satisfactory assurance about the effective functioning of the organization's risk management framework. It is important to note that even though corporate governance guidelines advocate that boards approve and monitor the organization's risk management framework, organizations outside of the financial sector still do not appear to favor a highly structured approach to risk oversight.

A balanced risk oversight process

The findings of this study align with our observations that risk oversight and reporting frequencies range from daily active risk oversight (often through operational risk committees) up to yearly or even multi-year high-level risk oversight activities at board/audit & risk committee level.

Organizations with a low official risk oversight frequency (e.g. yearly) and intensity often:

- rely strongly on the first-line functions to actively monitor and oversee the risks, implying a limited level of independence, objectivity, and outside-in views.
- do not systematically report all risk information to the audit and risk committee.
- have a small risk management team in place focused on consolidating the information on top residual risks on a regular (mainly quarterly to yearly) basis, with a limited active risk oversight role and no complete view of the risk & compliance landscape.

This approach is not necessarily inferior to more active risk oversight. Active risk oversight has a cost, which needs to be carefully balanced with the benefits. Our recommendation for boards and risk committees is to have an in-depth discussion and reflection on the level of risk oversight required, taking into account the organization's vision, risk appetite, culture, and organizational context. An assurance map can be a powerful instrument to structure this discussion. Such a map shows for each risk and compliance category which first, second and third line activities are undertaken, and what is done to gain reasonable assurance that these activities are under control.

Conclusion

This research seeks to draw out insights on the ways in which boards of directors handle risk oversight in practice. It is clear from our observations that boards are making significant progress in achieving effective risk oversight, yet the risk governance structures and processes need to be shared more widely to become standard practice. While many boards' current approaches to risk oversight seem fit for purpose, some could still be elevated to a higher level of maturity and depth. At some non-financial organizations, risk management has long remained a somewhat underdeveloped and siloed topic in the organization, receiving rather limited attention from the board. Nowadays, we observe an increased board-level awareness of the importance of looking at both sides of the risk-return equation, fueled by regulatory pressures and the recent global crises that act as catalysts for greater maturity in risk oversight. The interviewees in our study generally agree that boards have a critical role to play in overseeing the risks their organizations are faced with. One board director sums it up as follows:

> *"Risk oversight is about ensuring that the organization either generates the same return but at a lower level of risk or, alternatively, achieves a greater returnfor the same level of risk."*

To perform effective risk oversight, directors need to carefully consider the way risk governance is structured, as well as the formal monitoring and reporting processes. Our research shows that formalization of risk governance reconciles with corporate entrepreneurship, provided that organizations implement risk oversight in a pragmatic way. However, it is also – if not more – important to foster the right culture to create proper risk awareness across the organization. Organizations increasingly integrate risk into the board's strategic decision-making processes. This integration involves a delicate balancing act between, on the one hand, protecting the business from undesirable threats, and on the other hand, taking on new business opportunities in the pursuit of sustainable growth.

We believe our findings form a solid foundation for board and audit committee chairs to reflect on their organization's risk oversight practices. Whether applying the principles outlined in this paper, is an evolutionary or revolutionary step for their specific organization will depend on the broader context in which their risk governance is embedded. We trust the insights presented in this report are of keen interest to all those concerned with ensuring effective risk oversight at board level.

The art of defining your ERM target operating model

Risk management oversight is a broad concept, and there is not a one-size-fits-all definition for its operating model, as confirmed by this study. There is a reason why leading frameworks such as ISO31000 and COSO ERM and Internal Control are principle-based; indeed they need to be tailored to the context of the specific organization in order to be successful.

Setting-up risk management properly requires the following:

- A good understanding of the organizational context;
- A good understanding of the vision of the board, the audit and risk committee(s) and management;
- A clearly defined strategy and operational objectives framework;
- An understanding of the existing first, second and third line functions in order to achieve proper alignment of their activities in the context of achieving integrated assurance;
- An alignment with the internal audit plan and activities;
- A proper identification of the regulatory compliance landscape;
- An understanding of the stakeholder requirements;
- An understanding of the current and desired organizational culture;
- An evaluation of the current and desired maturity in risk management and a view of a realistic roadmap to close the gaps;
- Expertise in setting-up risk management and a broad understanding of governance, risk & compliance concepts.

We are convinced that the added value of an organization's risk management framework and process strongly relies on the design of the risk management and internal control-operating model. Unfortunately, this too often receives limited specific attention when the organization's global target operating model is defined during business transformations. As a result we see uncoordinated activities among the three lines of defense, no holistic view on the risk and compliance landscape, fragmented reporting to those charged with risk oversight, a lack of ownership, as well as overly administrative and low value-adding risk activities. A design that is not fit for purpose can obviously not lead to the desired results.

We recommend organizations have a structured concept for their three lines of defense and risk oversight set-up when going through a business transformation or when the Governance, Risk & Compliance system is not delivering the expected value. The table below illustrates the ERM Operating Models.

Governance	Risk strategy & objectives	Risk identification	Risk assessment	Risk mgmt. & control	Risk monitoring & reporting	Data & technology	People & culture
Committees and org. Structure	Risk strategy & appetite	Risk categories	Rating scale	Risk actions	Reporting methodology	Data & tech. Strategy	Staffing & sourcing
Roles & resp., reporting lines	Breach protocols	Identification process	Risk rolling up	Control suite	Quality assurance	Risk integration in technology	Training & development
ERM framework & policies		Repository	Risk modelling	Control testing	KRI		Risk culture
Taxonomy & definitions			Stress testing		Issue & remediation follow-up		

Illustration 2. KPMG ERM Target Operating Model Components

Authors

Regine Slagmulder

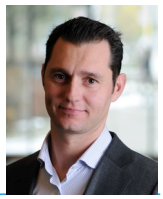
Regine Slagmulder is a Full Professor of Accounting & Control and Senior Partner at Vlerick Business School (Belgium). Her research and teaching activities focus on strategic risk management and board effectiveness. Her most recent work explores how risk governance, risk reporting, and board-level decision-making processes are organized to enable effective risk oversight and sustainable value creation. Regine has been a non-executive director and audit committee chair of the Belgium-based investment organization Quest for Growth (since 2011), MDxHealth, a commercial-stage multinational healthcare organization (since 2020), and Ekopak, an industrial water treatment organization (since 2021), all listed on Euronext.

Patrick De Schutter

Patrick De Schutter is a Partner in the Audit practice at KPMG in Belgium and has 37 years of relevant experience in audit, risk, controls, financial reporting and forensic audits. He is also Head of the Family Business Practice of KPMG in Belgium and member of the Audit Management Team. Patrick's clients include large listed and private corporates with a particular emphasis on Family Owned Businesses, which is his main professional passion and domain expertise.

Patrick is co-Founder and co-Managing Director of the Institute for Family Businesses and co-Founder and Director of FBN Belgium, a unique platform for the 200 largest Belgian family businesses. He has been an independent Director at ECS/2XL and specialized in governance and board evaluations.

Olivier Elst



Olivier Elst leads the Risk & Assurance practice of KPMG in Belgium and is specialized in Risk Management, Internal Control and Internal Audit for corporates and the public sector. Active in these domains since 2006, Olivier has delivered a large number of Risk Management projects across sectors and for organizations of different sizes throughout Europe.

Olivier is a certified ISO31000 Risk Management practitioner, a certified Internal Control Specialist and a certified Internal Auditor (IIA).

home.kpmg/be/social