The (mis)perception of risk maturity

The potential gap between the Board of Directors, the Executive Management and Internal Audit function as to how key risks are managed by the organization

A recent publication by the Institute of Internal Audit shows that the understanding as to how key risks are being assessed and managed across the organization varies strongly between the Board of Directors, Executive Management and Chief Audit Executives (CAE). For certain key risks, Board members appear to be consistently more optimistic than Executive Management or Internal Audit as to how the organization is addressing them. This raises the questions as to where the various stakeholders get their information on the maturity of the organization and if there is a systemic information gap between the oversight committee and the operational functions of companies.

Organizations are faced with a multitude of risks that can affect their strategic, operational or financial goals, having a negative impact for example on the financials, their reputation, regulatory compliance and adherence to laws or business operations.

It is the Board of Directors' (BoD, Board) duty to ensure that management identifies and properly addresses these inherent risks[1] through various types of mitigating measures in order to reduce the residual risk[2] to an acceptable level in a timely manner.

Such risk-mitigating measures could include eliminating the risk by abandoning certain business activities, reducing the risk by using internal controls and monitoring instruments, externalizing the potential impact through underwriting or by simply asserting a position that the risk is knowingly and purposely borne by the business.

Internal Audit, as the third line of defense, is usually mandated by the Board to provide independent and objective assurance by assessing the design and effectiveness of these mitigating measures that the organization has implemented to reduce its exposure to key risks.

Misperception of risk knowledge and capabilities

The natural challenge of any organization is to identify potential key risks that matter to the organization in a timely manner, to have a common and accurate understanding across all stakeholders (i.e. Board, Management, Risk Management, Internal Audit) of the potential impact of risks and to effectively design and implement long-term mitigating measures.

Figure 1: How to identify potential key risks

[1] Inherent risk = gross risk exposure that a company faces without taking any counter measures

[2] Residual risk = net risk exposure after taking into account mitigating measures

The recent study "OnRisk 2020"[3] by the Institute of Internal Audit (IIA) reports that the perception of **knowledge** and **capabilities** to identify and address the key risks of an organization varies between the different key stakeholders and that there is a certain bias as to how key risks are understood.

The study assessed the misalignment using 11 key risks[4] that are currently considered as key within the corporate world. Indeed, these 11 risks match those also identified in a KPMG publication on key risks to be considered by Internal Audit (IA) until 2020[5].

Interviews with members of the Board, Executive Management and Internal Audit show a **strong alignment regarding the knowledge and understanding** of accurately recognizing and exploring key risks. As such, it suggests that everyone shares a common understanding of these key risks, not only in their nature but also how they should be rated (i.e. severity, impact, probability).

However, this **picture changes when assessing the perception regarding the capabilities** of the organization to effectively and efficiently address and manage these risks.

The study suggests that **members of the Board rate the capabilities of the organization** to address key risks and maintain a sustainable system of mitigating measures **to be more mature than Executive Management**.

It also comes as a surprise that the usually more critical **Chief Audit Executives (CAE) are somewhat more positive**. They tend to assess the capabilities of the organization to mitigate risk (i.e. develop and maintain countermeasures) more positively than Executive Management.

This raises the following questions:

- Are Boards and to a certain extent CAEs somewhat overconfident regarding the capabilities of the organization to effectively address risk while Executive Management is too critical in the perception of the maturity level of risk management?
- Is there a systemic information bias between the different stakeholders despite the introduction of a second (i.e. risk management, compliance) and a third line of defense (i.e. internal audit)?

---

[3] Reference: OnRisk 2020 Report - A Guide to Understanding, Aligning, and Optimizing Risk (2020). The study is based on more than 90 qualitative interviews with Board members, Executive Management and Chief Audit Executives (CAE). Institute of Internal Audit (IIA); na.theiia.org/periodicals/OnRisk/Pages/default.aspx (retrieved 25.02.2020)

[4] Key risk include: cyber security, data protection, regulatory change, business continuity management, data and new technology, third party, talent management, culture, board information, data ethics, sustainability

[5] Reference: 20 key risks to consider by Internal Audit before 2020; Luka Zupan; KPMG Switzerland; assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf (retrieved 25.02.2020)

The confidence gap

Surprisingly, when confronting the various interview participants (Board, Executive Management, CAE) many suggested that this misperception gap regarding the organizational capabilities is a "**healthy level of disconnect**" thus somewhat downplaying the danger of misalignment.

Notwithstanding this obvious misalignment, this would suggest that the Board has a natural "trust" towards Executive Management to report potential cases where key risks could materialize in a timely and accurate manner or if the organization is not doing enough to effectively mitigate risks.

Another explanation for the "healthy disconnect" could also be the perspective of the three groups involved (Boards, Executive Management, CAE). While all interview participants rated their personal knowledge and understanding of the 11 key risks as somewhat equal, their focus differs slightly.

CAEs concentrate on the day-to-day operations when it comes to tackling risks (i.e. tactical response to risk). Members of the Board and Executive Management on the other hand focus on the general strategic response (i.e. strategy how to deal with risks).

This suggests that each stakeholder group has a sound understanding of the relevant risks but assesses these from a different angle (tactical vs. strategic) when determining the organization's strength to effectively address a risk.

The information bias

Another rationale that could explain the misperception is the potential information bias. Members of the Board often state that they are somewhat **disconnected** from daily operations. Reasons for that can be the lack of business experience in the respective industry, not enough time for the respective mandate or the fact that Executive Management plays such a dominant role that members of the Board can only discreetly steer the direction of the organization[6].

Furthermore, Board members fully depend on signals from within the organization to accurately assess a potential risk as they usually don't play a role in the day-to-day business. Potential strategies to overcome such a biased situation is to invite risk owners to present to the Board their assessment and countermeasures used to mitigate or even eliminate risks.

While such presentations often allow board members to better understand inherent risk situations, it remains difficult for them to accurately assess how effective the mitigation actually is (i.e. tactical measures to manage risk).

In such situations Internal Audit can play a role by addressing these concerns as part of their assurance mandate. However, usually their resources are limited and require a comprehensive understanding of a particular risk situation. Ideally, they also want good practice examples (for instance, measures to secure an effective cybersecurity strategy) so they can benchmark the case on hand. As a result, Internal Audit usually does not have the resources and means to address risks as they should, also because they may lack specific expertise in an area.

Conclusion and potential countermeasures

So should Boards and to a certain extent CAEs be worried about the organization's capability to effectively address key risks? And who should compile a list of countermeasures? Internal Audit? Process owners? Executive Management?

The study shows that to a certain extent it is natural to misunderstand the organization's capabilities to effectively address risk; the culprit is the information gap. Executive Management and particularly the individual risk owners will always have a better and more comprehensive understanding regarding the inherent and residual risk situation of the organization. It is thus important that the maturity of the organization enables a proactive and open communication with the Board in case the assessment of a risk has changed, is simply wrong or if mitigating measures appear to be only partially effective.

A good strategy for board members to overcome such misalignments is to have risk owners present the status of risk mitigation efforts during Audit Committee or Board meetings. This will allow a wider group of stakeholders to assess the situation, provide room for an open discussion and evaluate if the mitigating measures are robust enough to manage the risk effectively.

[6] Reference: Die Überforderung von Verwaltungsräten (2020) Hansueli Schöchli – Neue Züricher Zeitung (NZZ); www.nzz.ch/meinung/die-ueberforderung-von-verwaltungsraeten-ld.1541134 (retrieved 25.02.2020)

Boards are also well-advised to use external information (i.e. thought leadership publications, news on emerging risks etc.)to personally assess the potential shifts in the risk evaluation or to determine whether new risks have emerged, which so far have not been given high priority. A good example are the recent developments regarding cybersecurity. Until recently, most companies addressed this risk at best partially, resulting in a much higher risk exposure than the organization's risk appetite would allow.

Last but not least, if the Board feels genuinely uncomfortable with the actions the organization takes to address key risks, it should have the possibility to mandate external subject matter specialists to provide an independent and objective assessment of the risk situation. Such an external assessment not only provides a fresh and unbiased view of the organization's risk, but it also allows an assessment whether the organization compares favorably with peers when it comes to effectively mitigating key risks (i.e. benchmarking or peer review, good-practice comparison).

Finally, the most effective strategy to overcome the misalignment is to openly discuss key risks on a recurring basis (i.e. list risk discussion as a standard agenda topic) and have Executive Management commit to provide a reliable and unbiased view as to how they assess the inherent and residual risk situation.

Luka Zupan
Partner, Head of Internal Audit, Risk and Compliance (IARCS)
KPMG Switzerland

lzupan@kpmg.com

This article is part of KPMG's Board Leadership News. To receive this newsletter three times per year, please register here.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2020 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative (»KPMG International»), a Swiss legal entity. All rights reserved.