Enterprise Risk Management

Rethinking risk management in a time of a global pandemic

Enterprise Risk Management (ERM) is commonly understood as being a crucial governance framework that supports a corporation in effectively identifying, objectively assessing, and actively governing the key risks of an organization. However, during the pandemic challenges of the past 18 months, the board of directors together with executive management have faced considerable uncertainties to which the existing, institutionalized ERM framework provided only limited answers or guidance. As we will outline in this article, this had little to do with the fact that the pandemic variables were not part of the key risk catalogue.

Who was prepared and did it make a difference?

A recent survey by the Institute of Financial Services Zug (IFZ)[1] noted that only 46% of the risk managers interviewed had a pandemic risk fully or partially integrated into their risk radar / repository. This was seconded by impressions and experiences we encountered during discussions with clients[2] as to how organizations would need to respond to the short-term pandemic challenges. Furthermore, the IFZ study noted that if an organization had the pandemic on their risk radar, they mostly defined countermeasures in the following areas: readily available disinfectants, a documented and tested pandemic plan, recurring crisis exercises, and contingency plans for waves of influenza.

The majority of corporations did not have any specific risks listed in their risk register that would address potential pandemic outbreaks nor were any mitigation actions or assigned roles and responsibilities specifically defined. The rationale behind this decision was mostly that the occurrence of such a deeply impacting situation would be highly unlikely and if even in the event of materialization, would allow for sufficient time to prepare. Thus, pandemic risks were considered as "black swans".

Nevertheless, while most governments and business were taken greatly by surprise by the velocity and impact the pandemic had on their society, economy and infrastructure, corporations in general reacted swiftly and focused on immediate adjustment to the new condition (supported also by governmental measures to cushion the general economic consequences of the pandemic). Companies were quick and agile in adapting to the new work regime, i.e. allowing for employees to work from home during the lockdown of offices, finding alternative means to procure while international trade and supply routes were shut down, adjusting production planning (i.e. shifts) to allow temporarily closed factories and plants to re-open[3], and providing employees with the necessary tools and assets (i.e. computers) to work remotely.

[1] Hunziker et al (2020:34): "Die Rolle der Risk Manager in der COVID-19 Krise", ERM Report 2020 (https://hub.hslu.ch/financialmanagement/2020/11/05/erm-report-2020/)
[2] Zupan (2020): "Perception of key and emerging risks" (https://home.kpmg/ch/de/blogs/home/posts/2020/12/ia-after-covid-emerging-risks.html)
[3] March 2020 to June 2020; December 2020 to May 2021

In summary, while the overall infrastructures of countries were challenged with tremendous governmental implications, individual corporations acted surprisingly agile and were quick in adjusting to the new circumstances. This is best evidenced by the fact that while in Q2 2020 a material economic decay was experienced, it was compensated to a certain extent in Q3, and economists suggest that by the end of 2021, the Swiss economy will be back to the level before the pandemic crisis.

How well did those charged with oversight and management understand the implications?

Yet, while short term adjustments to the work environment (i.e. location, office attendance, use of digital tools to uphold communication) were implemented very effectively and efficiently, questions raised by the oversight committees (i.e. board, audit committee, etc.) regarding the robustness of internal governance, control and managerial processes, and how they would respond to these suddenly imposed adjustments and alterations remained unanswered.

The basic prerequisite of an organization was to interrupt operations as little as needed and to allow for business to continue as effectively as possible – indifferent as to how the internal checks and balances would adjust to the new situation. Retrospectively, this approach was mostly contributed to the fact that companies had defined business continuity plans readily available for short-term disruptions but not to the extent that these conditions would last for a longer period of time. It was assumed that within a period of one to two weeks, the situation would go "back to normal".

This was clearly not the case and what was planned to be a two-week interruption period has continued to this day for some organizations. As a result, for most corporations the design of internal governance and control frameworks became partially ineffective. Cause-and-effect assessments were not transparent and interdependences between risks were no longer transparent to those charged with responsibilities.

For example, (1) manual controls and assessment processes that include exchange, review or approval of transactions (i.e. invoicing, dunning, order-processing) now needed to be done virtually or required more time to be completed due to the home-office regime. Similarly, (2) documents submitted for review, approval and signatures (i.e. contracts, purchase orders) could no longer be handed over in person but either needed time-consuming courier services or used electronic copies of signatures that were mostly not properly certified[4]. (3) Budgeting and forecast processes for the coming periods needed to be assessed using completely different clusters of variables and assumptions while demand, supply and economic forecasts were highly ambiguous. Newly installed (4) government grants and furlough support that could be requested by companies needed to follow clearly defined rules and regulations that corporations were not fully able to comprehend or from which the long-term impact/implication (i.e. loosing flexibility in adjusting the workforce level to a new demand situation) could not be understood.

In short, the cause-and-effect of the mid- and long-term implications that the pandemic situation had on the risk profile of an organization were not clear or difficult to apprehend. The board of directors as the ultimate oversight committee of an organization was faced with challenges around supervising and governing the company from a risk control perspective without having enough transparency over cause-and-effect.

Which ERM lessons have been learned from a board and executive management perspective?

From a lessons-learned perspective and as a recommendation, the board together with management should require ERM to have a more holistic and forward-looking view that interlinks existing risks (i.e. dependency), incorporates the time variable (i.e. lag between identification and materialization of a risk), and a potential response strategy (i.e. how to tackle a risk), and that ultimately challenges not the state the organization is in today, but how it might be considered in the short, mid- and long-term (cause-and-effect of strategic decisions) and thus how it would impact the risk universe of the corporation.

[4] Experience showed that most companies had not yet introduced an electronic/digital signing procedure

Going forward, the ERM function should be more effectively trained to identify "black swans". That is, a potentially emerging risk that was not on the radar of the organization or had any strategies or back-up plans as to how to react to such instances. While they are called "black swans", risks for a reason (i.e. unpredictable, unlikely future events with a material impact) should be still expected and requested by those charged with oversight and management. ERM should at least annually show an extended horizon of potential threats and opportunities that are too far away to be relevant for the organization today but might have a serious impact tomorrow.

Furthermore, ERM should not only focus on identifying potential events that might affect the organization, it should also assess the impact in the context of a root-cause analysis as well as the extended effect on the entire risk register of the organization, i.e. through ERM the board should get a glimpse of a potentially emerging risk on the organization not only in its singular outbreak but also in the context of how it can potentially influence or impact other risks of the organization.

As to the pandemic risk, even if had been on the radar of a corporation, it usually provided little to no assurance for the board regarding the question of its possible impact on business, the organization, the processes as well as governance and control frameworks in the mid-term.

As a lesson learned, the board should be vigorous in questioning existing, simplified risk maps that outline risk as a matrix of impact and probability. Instead, interactive dependencies, time factors and a response strategy should be included for key risks in order for the board to better understand and challenge the seriousness of the impact, to assess the time left to prepare, as well as to what extent management should consider appropriate measures.

The quest for new ERM skills

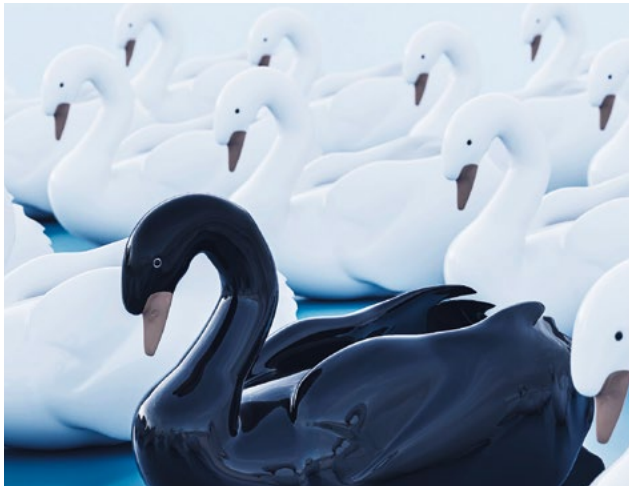
These developments will also influence the skills and capabilities needed by risk management professionals to provide the services expected of them. Traditionally, the ERM's risk focus has mostly been on internal, financial, operational and compliance related risks that were identified and based on the assessment of existing organizational structures, processes as well as governance and control frameworks.

In the post-pandemic perspective however, risk managers need to comprehend the strategic and operational direction a business will have in the future, how external circumstances, conditions and events can impact an organization in its deepest roots, and how all this can or could be interlinked through the perspective of risk management.

ERM managers are expected to be strategic business partners for the board, executive management and the wider stakeholder family within organizations when discussing the cause-and-effects of potential decisions in the short-, mid- and long-term perspective. As such, they need to comprehend how the corporate strategy process is designed, how mid-term objectives are defined and operationalized as part of the planning process, and, at the same time, comprehend the impact of new business models or changes to the organization and its processes.

Additionally, they need to be able to break silos within the organization and collaborate with other departments to understand the increasing interconnectivity between risks, be this from an internal as well as an external perspective (i.e. production-related supply risks from a pandemic breakout will not only will have a short-term effect on production capacities but also have an effect on long-term contractual sales agreements and potential legal penalties while, at the same time, impact production, margin and pricing calculations – to name just a few chain reactions). This leads to an increased need for interpersonal and holistic capabilities that go beyond the usual analytical and technical skills.

Finally, risk managers need to have a more agile approach to risk management. The methodology should be less focused on spending time assessing existing risks, but instead use more time "scanning the horizon" for new eventualities and



even more importantly, support the definition and execution of risk responses from a cause-and-effect point of view and keep a holistic risk view that includes not only probability and impact but also time, dependency and capabilities to respond.

Emphasis should be more on "identification" and "mitigation" and less about the discussion as to whether a risk probability should be labeled as "very high" or only "high". Clearly defined strategies on the risk response (i.e. transfer, avoid, accept, reduce/act) should influence the consolidated risk perspective and allow the risk manager to discern if a risk can have multiple dependencies (i.e. a pandemic risk impacts the organizational set-up, impacts control and governance, impacts short-term planning, impacts the long-term economic growth strategy, etc.).

Furthermore, the ERM manager should place emphasis on the actual execution of risk responses, i.e. putting the plans and ideas on how to respond to a risk in reality. As such, the ERM manager of tomorrow should have a new skill set that allows him/her to respond in an agile and flexible manner to new circumstances, quickly comprehend the combined impact on the organization, and demonstrate to those charged with oversight, supervision or management how cause-and-effect decisions impact the overall risk landscape of the organization.

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

+41 58 249 36 61
lzupan@kpmg.com

Conclusion

The pandemic avalanche of the past 18 months has clearly demonstrated that material external hazards cannot be avoided by individual organizations and can impact them in ways not considered possible. Risk managers will require a new skill set in order to be familiar with such crisis management, be capable of seeing beyond existing boundaries and accordingly provide responses on the cause-and-effect of such materialized incidences to the board and the executive management.

This article is part of the KPMG Board Leadership News. To receive this newsletter for board members three times a year, you can 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