The coming year looks to be another challenging period for many businesses, with various external and internal forces from the complex universes of IT, political instability, economic factors and regulatory pressures, amongst others. But it is also one laden with opportunities.

Drawing on our conversations with board risk committee chairs and company secretaries over the past twelve months, we have highlighted the following issues that, in our opinion, board risk committees (BRCs) should keep in mind as they approach and execute their 2019 agendas:

1. **Maintain a focus on the fundamentals.**

An effective BRC provides a structure that focuses in detail on the risk management framework and all key risks. The BRC should be an independent and objective advisory committee – a ‘review and recommend’ committee – not an approving committee, and the committee’s terms of reference should be clear on this point. It needs to adopt a broader perspective, while always looking over the horizon to understand the true nature of the organisation’s exposures and concentrations. It is also important to identify and consider emerging risks, assessing these through the use of scenarios and other approaches.

Think about the risk function. Is the board risk committee positioned to provide the Chief Risk Officer (CRO) with the necessary safe harbour and protection? Can the CRO speak up when risk is rising too high or there is the risk of potentially significant deterioration in the overall risk appetite and tolerances of the organization?

2. **Access to information and external advice.**

The remit of the BRC requires its members to have dependable access to sound risk management information. This needs to inform, provide insight of trends and underlying themes, and also provoke questions and challenges to the organization and its environment.

Where necessary, recourse to a high-quality source of external advice can help non-executives to articulate the core issues as well as supplement and validate information received. Does the committee have access to external inputs that can help stress-test a business strategy, addressing in particular the connectivity of risk and whether the array of low-probability, high-impact events taken into such testing has been drawn sufficiently widely?

3. **Geopolitics**

Managing the geo-political risk landscape is an organizational capability that many CEOs feel is lacking. It is clear that geopolitical instability needs to remain high on the board’s radar. Brexit, conflict in the Middle East, the unpredictability of Russian foreign policy, increasing tension with North Korea, and China’s economic sluggishness – these are just some of the issues shaping the geopolitical landscape.

4. **Culture, ethnics and conduct risk**

Conduct risk has risen up the risk committee agenda. In April 2018, the Monetary Authority of Singapore (MAS) sought feedback on proposals to strengthen the individual accountability of senior managers and raise the standards of conduct in financial institutions. Some of the proposed guidelines include requiring financial institutions to identify senior managers who are responsible for core management functions and clearly specifying their individual accountability.

Understanding and addressing the drivers of conduct risk is essential in improving standards of behaviour. The committee needs to understand how the business is mitigating the risk of poor conduct outcomes. Is the conduct risk programme tailored to the needs of the organization?

Think about size, business model, and geographic reach. Is the executive team fully engaged on conduct risk and helping to raise its visibility within the organization? Does the organization focus too heavily on crystallized risk such as fines and losses, as opposed to developing forward-looking risk indicators?
Is the organization clear as to when a product or behavior moves from being reasonable to unreasonable?

Beyond conduct risk, employees and customers are increasingly demonstrating a social and ethical conscience. Radical transparency enabled by social media and the ever-sharpening focus by customers, employees, investors, regulators, and other stakeholders has put culture on display as never before.

Pay particular attention to potential risks posed by tone at the top, culture, and incentives. Does the culture align with the company’s strategy and encourage behaviours that are essential to the execution of that strategy? Is the board continually gauging not only tone at the top, but the mood in the middle and the buzz at the bottom?

5. Artificial intelligence and other new technologies

Organizations must look to innovation to create operational efficiencies and enhance customer experience. With advances in big data, cloud computing and other technologies, more and more organizations seem set to use machine learning and cognitive computing. BRCs can help by considering how big data and technical advances can be used to improve modelling capabilities, support decision making and gain a deeper understanding of customers and their expectations. If necessary, legacy systems that are no longer fit for purpose should be replaced even if this might be expensive and time consuming in the short term.

6. Regulation

Regulators and tax authorities are able to better identify and target non-compliance through their use of data and analytical techniques. Organizations need to ensure their systems are capable of capturing and interpreting the relevant data sets and that they have the internal capability, including from a resource and skillset point of view, to cope with the regulator’s increasing reach.

The laundry list of regulatory risk looks set to continue into 2019 and beyond. With all this change comes elevated operational risks that need to be appropriately managed. Is the organization quick to understand the impact of new regulation and the interlinkage of regulatory change across different jurisdictions? Are appropriate awareness and educational programmes in place?

7. Cyber security

BRC oversight must continue to evolve in line with the changing cyber landscape. The threat to data confidentiality, integrity and availability of systems remains high. BRCs should seek to ensure the company’s cyber risk mind-set is elevated to an enterprise level. Cyber risk must be managed as a business or enterprise risk – not simply an IT risk – and needs to be factored in in discussions about business strategy.

Help ensure that awareness of, and accountability for, cyber security permeates the organization with a security mind-set, proper training, and preparation for incident response. Is cyber security risk given regular and adequate time on the board’s agenda? Does the company understand its third party relationships, and the controls that exist around those with access to its proprietary data? Does it have a robust cyber incident response plan? Is that plan rehearsed and are the scenarios up to date? Where does accountability and responsibility for cyber security lie? Does the board need a separate committee to focus on it?

8. Connectivity

Risk is unpredictable and contagious, and connected globally within complex organizational structures. Understanding an organization’s true risk profile can be significantly improved by identifying the interrelationships between risk and potential risk contagion. Does the committee look beyond conventional depictions of risk based on likelihood and severity, and take a view of risk that allows for the contagion effect of risks — one of the most significant learnings of the Global Financial Crisis?

Contact us

Irving Low
Partner, Head of Advisory
T: +65 6213 2071
E: irvinglow@kpmg.com.sg

Emilie Williams
Director, Risk Consulting
T: +65 6411 8007
E: emiliewilliams@kpmg.com.sg

KPMG Services Pte Ltd
16 Raffles Quay
#22-00 Hong Leong Building
Singapore 048581
T:+65 6213 3388
F: +65 6225 0940

kpmg.com.sg/socialmedia  kpmg.com/app

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 endeavour 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.

© 2019 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in Singapore.