KPMG

On the 2018 Risk Committee agenda

KPMG Board Leadership Centre

Following a tumultuous 2017, 2018 looks to be another challenging year for many businesses - but one also laden with opportunities. Contending with the various external and internal forces from the increasingly complex universes of IT, political instability, economic factors and regulatory pressures, amongst others, is becoming more challenging and calling on increasingly diverse skill sets and experiences.

Drawing on insights from our conversations with board risk committee chairs and company secretaries over the past twelve months, we have highlighted ten issues that, in our opinion, risk committees should keep in mind as they approach and execute their 2018 agendas:

1. Maintain a focus on the fundamentals: Is there clarity over the role of the committee – is it an advisory committee or a decision making body? The board are responsible for making the big decisions – risk appetite, the enterprise wide risk management framework (EWRMF), the major policies, the ICAAP, ILAP etc. are all approved by the board – notwithstanding that these are all difficult issues and hard to digest. Furthermore, these issues need to be looked at every year in line with the Capital Requirements Directive and the budgetary cycle. Lines can get blurred in practice, but from a governance perspective the risk committee 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. Do committee members, other board members and the executive management team understand the role of the risk committee (and the full board)?

   Taking a strategic view of risk is risk committee issue #1. When management lean towards Value at Risk (VAR) and short term metrics, or focus unduly on a narrow set of metrics, then the risk committee needs to adopt a broader perspective and also to look over the horizon to understand the true nature of the organisation's exposures and concentrations. Does the committee have access to the right information? Is the committee looking beyond economic events and stress-testing to the fundamental issues that can impact strategy and disrupt the risk profile of the organisation? Also, focus closely on the big transactions (M&A) and look in depth at concentrations or understand the true economic risk characteristics.

   Risk committees tend to focus on the key risks that are of historical materiality in terms of the impact on the franchise, and there is often a tendency to devote too much time towards overseeing risks that are familiar to the committee and its members, or have historically been important. In a changing environment where technological changes bring both opportunities, disruption and fundamental change to established business models and customer behaviour, it's important to identify and consider emerging risks which are often without established historical data and patterns of behaviour. Accordingly be prepared to assess risks that are unfamiliar and in an environment which may have uncertainty and ambiguity. Be prepared to consider correlations between such risks and assess such matters through the use of scenarios and other approaches.

   New and emerging risks require the committee to have appropriate skills and awareness, but also to be soundly briefed; a questioning approach is to be encouraged. An informed approach is crucial. Think also about the risk function and skill sets it needs for the future.

   Finally, is the risk committee positioned to provide the Chief Risk Officer (CRO) with the necessary safe harbour and protection with

respect to remuneration, tenure, etc.? Does the risk committee encourage the CRO to operate as the 'circuit breaker' when risk is rising too high or there is the risk of potentially significant deterioration in the overall risk appetite and tolerances of the firm?

2. Access to information and external advice. The remit of the board risk committee calls for a high degree of rigour and judgement, and members must have dependable access to whatever material they need to enable them to discharge their responsibilities. But this should not require data and paper flow on the scale that is frequently encountered. Rather there is a need for effective distillation of key issues in a thematic way, and delivering this should be the responsibility of the CRO. Sound risk management information needs to inform, provide insight of trends and underlying themes but also provoke questions and challenge as to the firm and its environment.

   Given the priority and complexity of the risk monitoring role, recourse to a high-quality source of external advice might be found to serve the board risk committee as a sounding board. This sounding board can help non-executives by articulating the core issues via clear, succinct questioning, as well as supplementing and validating the information the committee receives from the executive.

   Does the committee have access to an external advisor? Does the committee seek external input to the stress and scenario-testing of 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 sufficiently widely drawn?

   Whether, and from whom, to take external advice on risk matters must ultimately be for decision by the board or board risk committee in its particular circumstances. In many cases, the "best" advice that is likely to be available and relevant will come from a bank's internal capability, provided that the risk function is independent of the executive in tendering its advice to the risk committee. But, where it is available, high-quality external advice would be likely to assist the board risk committee and board in reaching decisions on risk tolerance and strategy that, as far as possible and on the basis of rigorous stress-testing, minimise the risk of serious disruption in future.

3. Geopolitics: Brexit, the refugee crisis, conflict in the Middle East, the unpredictability of Russian foreign policy, increasing tension with North Korea, and China's economic sluggishness are just some of the issues shaping the geopolitical landscape. While some of these global issues are generating more traditional geopolitical risks, events such as the massive demographic shift created by the refugee crisis - and the pressures that they are creating in Europe for business and society alike - are different. Factor in the enormous uncertainty following the EU referendum and the US election and it is clear that geopolitical instability needs to remain high on the board's radar.

   While none of these geopolitical factors are as important to banks and some other financial institutions as the long-term structural and commercial decisions they will have been mulling over for some time, focus must rightly be directed to mitigating the effects of Brexit – whether that be duplicating back-office costs or coping with new regulations. The tone and direction of the Brexit negotiations means banks and other financial institutions must plan for the worst case scenario. Will financial services get special access? Will there be 'no deal' and a default to WTO rules? At this point no one knows and while the concept of a phased implementation to any deal is to be welcomed, the possibility of 'no deal' (and therefore a cliff-edge Brexit) means a 'wait and see' approach is no longer credible.

   How rapidly do you need to act as passporting (as we know it today) comes to an end? What are the practical implications on your staff? How will the cost of cross-border business change as we move to a more 'balkanised' approach to regulation? What shared services opportunities are there? How will regulatory arbitrage affect business models and domiciles? Think about other long-term trends catalysed by Brexit such as low interest rates, slow macro growth, competition from new entrants, technical innovation, higher capital and liquidity standards, IFRS 9 and IFRS 17, and on-going conduct issues – to name just a few.

4. Culture, ethics and trust: As high profile incidents of unethical behaviour continue to rattle the financial services industry, culture, ethics and trust are in the limelight once again. Beyond conduct risk, we are increasingly seeing that employees and customers have a social and ethical conscience and organisations need to respond to this if they are to thrive. Some already do and have a vivid and tangible strand to their ethics and CSR, whilst others have been beset with incidences of poor behaviour and immoral outcomes that can damage reputations, lead to large fines and other sanctions, and put potential customers and employees off.

   Corporate culture - what a company does, and how it does it - permeates virtually every aspect of a company, from strategy, innovation, risk, and compliance, to business processes,

employee performance, and long-term value creation. And, as many companies have experienced (or will) first-hand, the 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: Organisations, especially those within the financial services sector, must look to innovation to both create operational efficiencies and enhance customer experience. In particular, Artificial intelligence (AI) could soon transform how businesses operate – whether that be how we bank, invest or get insured. Insurers are already using AI to streamline process flows and combat fraud, banks are using chatbots to enhance customer experience and it's increasingly important to investment managers too.

   With advances in big data, cloud computing and processing speeds moving at pace, more and more organisations seem set to use machine learning and cognitive computing. Think about 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. Some technologies are mature enough to be used immediately and others are a little further off – but it is time to start planning for them now.

   Is the organisation consciously looking at technology as a means of achieving productivity improvements? If process automation can be integrated into existing interfaces then the cost of high frequency manual operations could be reduced dramatically. If not, core banking systems may need replacing and that can be expensive and time consuming. But, persisting with legacy systems that are no longer fit for purpose can be even more expensive in the long run. Has the committee considered the advantages of working with others on common platforms for (say) back-office processes, know your customer, anti-money laundering and other processes common across the industry? There are risks attached to entering into such arrangements (e.g., customer data and privacy), but these must be weighed up against the potential cost savings and efficiency gains.

6. Regulation: In recent years companies have been hit by increasing regulation from all angles and the dial only seems to be turning one way. The overhaul of the capital adequacy framework, widespread structural reforms, far reaching changes to accounting practices and tighter anti-money laundering controls, the laundry list of regulatory risk looks set to continue into 2018 and beyond. With all this change comes elevated operational risk that needs to be appropriately managed. Is the organisation 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? Are all employees aware of their role and responsibilities, as well as the ethical repercussions associated with regulation? Each product must address the client's needs and not end up on the wrong side of regulatory surveillance.

   Whilst businesses are increasing their use and reliance on data, so too are regulators and tax authorities who more than ever are able to better identify and target non-compliance through their use of data and analytical techniques. Firms need to respond to this 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 use of Regtech companies is expected to increase as the burden and penalties associated with regulation continue to escalate. Also think about collaboration across companies and industries in the form of shared information and resources as organisations seek to reduce cybercrime and uphold anti-money laundering requirements amongst other issues.

7. Conduct risk: Since the Financial Conduct Authority (FCA) took over the supervision of consumer protection in 2013, conduct risk has risen up the risk committee agenda. Every company faces a unique set of conduct risks based on their industry and size – but building an effective framework for managing that risk can be a Herculean task. Businesses that fail to bring conduct risk in line face regulatory action, fines, and reputational damage, which can harm a business for years beyond the event. We have seen significant financial impact on firms due to conduct-related regulatory action - and it can all stem from the actions of an individual. The latest report from the Fixed Income, Currencies and Commodities Markets Standards Board (FMSB) estimates banks have paid some $375 billion in conduct fines over the last five years.

Understanding and addressing the drivers of conduct risk is essential in improving standards of behaviour. While the starting point for this journey varies from firm to firm, the three core areas at the root of conduct risk are: the characteristics intrinsic to financial markets and their participants, such as information asymmetries between firms and their clients or the financial capability of clients; the entrenched behaviours and conflicts of interests within the financial sector that act to prevent markets from working as well as they could; and macro-economic developments that have the potential to impact financial markets and in turn the long-term needs of consumers. Does the committee understand how the business is mitigating the risk of poor conduct outcomes by responding to these pressures?

Is the conduct risk programme tailored to the needs of the organisation? 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 organisation? Does the framework should take into account both short and long-term goals? Are there regular board-level reviews to assess and challenge the conduct risk programme? Is the scenario planning appropriate? Does the organisation focus too heavily on crystalised risk, such as fines and losses, as opposed to developing forward looking risk indicators? Is the organisation clear as to when a product or behaviour moves from being reasonable to unreasonable?

8. Concentration risk: Concentration risk is relevant for the stability of both individual institutions and whole financial systems. Exposures to large borrowers like Enron and WorldCom contributed to financial problems of several U.S. banks in the early 2000s. A housing crisis combined with concentrated mortgage portfolios resulted in a number of bank failures in Scandinavian countries in the 1990s, and contributed to the Global Financial Crisis of 2007/08. Under the Basel Framework, Pillar 1 capital requirements for credit risk do not cover concentration risk, and those calculated under the Internal Ratings Based (IRB) approach explicitly exclude it. Banks are expected to compensate for this by autonomously estimating and setting aside appropriate capital buffers, which supervisors are required to assess and possibly challenge within the Pillar 2 process.

   Inadequate reflection of this risk can lead to insufficient capital levels even when the capital ratios seem high. For example, interest-only mortgages might look good from a credit risk perspective if mortgage holders are paying interest and the loan to value is adequate, but with an ageing client base, questions arise as to how the capital might be repaid. From a conduct risk perspective, this raises many questions such as: why did the bank lend; why hasn't the capital repayment situation been monitored; and why haven't customers been weaned onto repayment mortgages? Is the committee taking deep-dives into the organisation's big concentrations? How is the committee tackling the information asymmetries? Does the committee have access to third party perspectives?

9. Cyber security: Risk committee oversight must continue to evolve in line with the changing cyber landscape. Despite the intensifying focus on cyber security, the threat to data confidentiality, integrity and availability of systems remains high and the number of reported incidents at firms falling under the Financial Conduct Authority's jurisdiction has increased at an alarming rate. If the potential reputational damage were not enough to contend with, banks and other financial institutions also need to address increasingly tough regulation. Under the General Data Protection Regulation (GDPR), which comes into force in May 2018, organisations face fines of up to 4 percent of their global annual turnover for data privacy breaches.

   Discussions are shifting from prevention to an emphasis on detection and containment, and are increasingly focused on the company's 'adjacencies' which can serve as entry points for hackers. The Internet of Things, blockchain, cloud services and the digital records that surround people, organisations, processes, and products call for deeper - if not wholly different - conversations. The board risk committee should seek to ensure the company's cyber risk mind-set is elevated to an enterprise level, encompassing key business leaders, and help ensure that cyber risk is managed as a business or enterprise risk - not simply an IT risk. Do discussions about structural change, product development including new digital products, expansion into new geographies, and relationships with regulators, employees, suppliers, customers, partners, advisors, and other third parties factor in cyber risk?

   Help ensure that awareness of, and accountability for, cyber security permeates the organisation, 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? Where does accountability and responsibility for cyber security lie? Does the board need a separate committee to focus on it? Where are the company's biggest vulnerabilities and how is the company protecting its most critical data sets? Does the company benchmark itself against others in the industry and learn from high profile situations that other companies have faced?

Does the company understand the company's third party relationships, and the controls that exist around those with access to the company's proprietary data? Has the company explored its involvement in industry-wide alliances, where companies and other agencies can work together to detect and combat cyber-crime? Does the company have a cyber security scorecard and a robust cyber incident response plan, is the plan rehearsed and are the scenarios up to date? Do directors know the number and nature of policy breaches in the last period, and the consequences both for the company and individuals; and do they work under the assumption that any email could become public at any time?

10. Connectivity: In a world where economic volatility is the norm, and the past is no longer an indicator of things to come, disparate events can become inextricably linked. This makes assessing risk exposure especially difficult because risk is unpredictable and contagious, and connected globally within complex organisational structures.

    Understanding an organisation's true risk profile can be significantly improved by identifying the interrelationships between risk and potential risk contagion. For example, beyond the AI and new technology risks addressed above, an organisation might need to look wider and consider the impact on employment over the medium and long-term. A bank might be writing twenty-five year mortgages for people who appear to be in steady 'white collar' employment and while conventional modelling might predict a positive contribution to the bottom line, things could quickly go awry if (and when) AI and robotics impact employment in sectors traditionally insulated from such advances.

    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

The BLC team
T: 020 7694 8855
E: boardleadershipcentre@kpmg.co.uk