Board Risk
Article by John Plender
Pages 04-07
This article explores the board’s role in overseeing non-financial risk and examines whether audit committees can take on non-financial risk oversight and whether there is a risk that the audit’s committee’s core work on financial risk would be lost.

Recent events at Bell Pottinger and various reported cyber-attacks (there are many more not reported) have highlighted the range of non-financial risks to which modern day organisations are exposed to on a daily basis. The Bell Pottinger example serves to illustrate the importance of an entity’s reputation and how quickly, given the speed of modern day communication, this can be severely damaged. It also illustrates the importance of the culture within an organisation and the threat that an inappropriate culture presents. In terms of mitigating cultural risk, there is a need to ensure that directors and employees align themselves with the mission, goals and values of the organisation including behaving ethically.

The cyber risk is particularly prevalent in modern day society – the global attack by a strain of ransomware, “WannaCry” in May 2017, impacted on the operational capabilities of various organisations across the globe including the National Health Service in the UK. Additionally, the reliance by organisations on their IT systems...
exposes them to far more non-financial risks than just cyber. When things go wrong, as happened to BA earlier in 2017, this can have a major impact on an entity and its customers. Ryanair’s recent flight cancellation announcements further illustrate the risks to which such entities are exposed. Pilots are currently a key “off-balance” asset to airlines. This may change in the future but currently having pilots, whether employed or contracted, to fly planes is an operational necessity of an airline. An inability to make use of such key assets, whether caused by error or by legal restrictions e.g. a limitation on flying hours, presents a risk to such businesses. Therefore, given the diversity of non-financial risks, how do companies ensure that there is appropriate oversight of such risks including that appropriate safeguards are in place to mitigate their impact and that the level of threat is commensurate with an entity’s risk appetite?

The risks that companies face are both financial and non-financial and increasingly the latter category, though not new, appears to becoming more prevalent and significant. Although, there is no generally accepted definition of what is a non-financial risk and indeed, what is a financial risk, risks are commonly split into these two categories. There is however a common consensus that financial risks are those which relate to the integrity of financial systems and the related risk of presenting misleading financial information. Furthermore, risks of a treasury nature such as credit risk, exchange rate risk, and market risk may also be viewed to be within scope. Therefore, non-financial risks would be perceived to be any risk other than a financial risk, thus encompassing risks associated with compliance, conduct, economic uncertainty, health and safety, protection of intellectual property, operational, political, reputational, strategic, and technological et al.

Regardless of the types of risk to which an entity is exposed, ultimately, an entity’s risk profile and risk appetite are owned by the board and it has responsibility for overseeing the implementation of appropriate risk assessment systems and processes to identify, manage and mitigate the principal risks to the entity’s business. The key, therefore, is to ensure that the board is appropriately balanced i.e. it is composed of the right individuals with the relevant skills, diversity, experience, knowledge and competences and that those individuals are utilised to best serve the needs of the company. This balance is also a dynamic concept and should naturally change over time as the size, strategy and lifecycle of the company changes – e.g. the current focus on ensuring directors have or gain appropriate digital skillsets is a good example of how the needs of a board change over time. Both the directors and senior management need to focus on not just the short but also the longer term in relation to risk management and internal controls which play an important part of stewardship and are key to ensuring the long-term viability of the business.

The board has to ensure that it covers all of the bases when it comes to risk management, and in many cases at least certain aspects of the oversight of risk management will be delegated to a board committee. The Board may also take some confidence in situations where there are specific management risk committees.

**Audit committees**

Just as with the size and composition of boards, there is no one-size-fits-all-approach to the oversight of risk. Traditionally, the audit committee has generally been tasked by the board with oversight of the risk management function including an entity’s non-financial risks. Despite this, in many instances the primary focus of the audit committee has been the oversight of financial risks as highlighted by the terms of reference of various audit committees of listed entities. This is also evidenced by the need in certain jurisdictions for the audit committee to contain a member who has had recent and relevant financial experience, highlighting the importance of the “financial” expertise to the work of the committee. That said, the audit committee...
will also normally be responsible for the oversight of an entity’s internal audit function the scope of which will cover non-financial as well as financial risks. Internal audit, however, in many instances will not be the primary source of assurance over non-financial risks like health and safety but will rather provide an additional layer to that provided by specialists. Companies may use Safety, Health and Environment auditors (SHE) to visit plants to check on compliance to company processes and procedures etc and they will provide primary assurance to the board. However, the board may want further comfort that this assurance is fit for purpose and might ask internal audit to review the way the SHE audit function is run. Such an approach illustrates how an audit committee can take more responsibility for non-financial risk but there are limits and if this role is significant it can lead to the need for a different approach.

**Separate risk committees**

This need has been recognised by some businesses, particularly larger and more complex entities, possibly due to an increased awareness of the entity’s exposure to risks, increased focus by governance experts as well as a possible concern that audit committees are not best placed to broaden their remit. They have responded by establishing a separate committee or in some cases committees to look after many non-financial risk-based matters. This has been particularly prevalent in the aftermath of the financial crisis as the importance of risk management was clearly highlighted, particularly in the financial services sector. Where a separate risk or equivalent committee is established, this should have responsibility for the company’s most critical non-financial risks and risk management capabilities. Naturally, the directors who form this committee must have the appropriate skills and competencies to provide effective oversight over the risks falling within the committee’s scope. The use of a risk committee encourages an integrated, organisational-wide approach to the identification and management of risk whilst also providing a stimulus in relation to the quality of the monitoring of and reporting on, risk, for both management and the board. Such an approach should help the board focus on the entity’s overall position.

Having a separate risk committee also benefits the audit committee and other board committees by allowing them to focus on their respective core responsibilities. However, where there are separate committees looking after different aspects of risk it is also essential to ensure that nothing falls between the cracks i.e. there is a real danger that the use of various committees can result in a fragmented and silo-driven approach, which can result in critical risks being omitted from consideration. This risk can be mitigated by having some degree of overlap of membership and ensuring appropriate communication between the committees involved e.g. the audit committee and the risk committee. Furthermore, it is essential that there is absolute clarity over the respective terms of references, so that the board and committees are clear who is responsible for what. It also illustrates why it is essential that the risk oversight approach should be carefully orchestrated at the full board level as the board can’t delegate responsibility for risk and the establishment of committees does not detract from or diminish in any way the collective responsibility of the board.

**Board skills**

However a board decides to proceed in organising risk oversight, knowledge of the industry or an adjacent one and its critical risks should be prerequisites for at least the majority of the board and in certain sectors will be a necessity for all board members. An effective induction process will also help newly appointed directors get up to speed with the business, its operations and the risks it faces. Other skills are also important such as an enquiring mind and a challenging mindset. Where the audit committee has responsibility for oversight of non-financial risks the need to reskill the audit committee will first and foremost depend on the need to reskill the board. This will
depend on various factors such as the nature, complexity, scale and reach of the business and its operations; the skill sets of the current audit committee members; and the perceived key risks that the entity is currently subject to and indeed, is likely to be subject to, in the foreseeable future. Given the changing political and societal landscape this of itself is leading to change in board composition. Gender diversity quotas for instance have been introduced in certain jurisdictions to ensure that there are more women on boards. Another current key factor is the speed of technological advances including the availability of big data and the related associated risks of such. This presents a case to have an expert on such matters on the board itself and potentially someone from a younger generation to ensure that appropriate consideration is given to any demographic issues. That said there are other ways to involve such individuals, possibly by them serving on a specific management committee or to have experts who are non-board members sit on the audit committee. However, the latter approach is not generally viewed favourably by UK companies. This is partly due to confidentiality reasons, collective responsibility and that any such individuals would suffer from not having access to the same level of information as board members. Furthermore, consideration could be given to increasing the size of a board. The more board members, the easier it is to then allocate such individuals to their respective committee(s). However, having too large a board also creates its own problems.

In conclusion, the overriding criterion to ensure that a company can have an effective system for the oversight of both financial and non-financial risk is that the board must be appropriately balanced. Ultimately, it will be a for each company to determine the most appropriate governance structure, including board and committee composition, to meet the challenges that the organisation faces. Investors should also play their part by engaging on such matters with their investees. Ultimately, a board’s composition, the oversight of risk and risk management will evolve over time as business reacts to the changes which shape society, of which the impact of the 4th Industrial Revolution will undoubtedly be one.