RISK OVERSIGHT, MANAGEMENT, AND CONTROLS

Rajiv Jaitly

Risk management as a board subject has emerged from the shadows of theory to become a practical way of setting and managing corporate objectives for those charged with the oversight and governance of organisations. Risk management means different things to different people, and many categories of risk have been defined and encompass different types of corporate concern, whether extending to enterprise, investment, liquidity, operational, or other forms of risk management.

“Doing the right thing,” defined as conduct risk, has become a prescribed form of risk categorisation, particularly for financial services’ firms. The conduct or behaviour of firms and its employees has been pushed to the forefront. Providing the right outcome for customers and meeting their needs is now an important focus for boards. A spotlight is being shone on how effective boards are in assessing information and statistics to determine whether firms are meeting and delivering value to their customers. If firms are falling short, the board needs to take decisive action and track this until they are back on track.

Risk management is of course not always the avoidance of risk. Enterprises do need to balance risks with rewards, but may take the view

that some types of risks are accepted and managed whilst other risks are avoided altogether. The removal of all risk would also eliminate all opportunity and in any event would never be a practical or sustainable strategy for a business. Indeed, managed risk may be good for a business.

Risk and risk management, boards, and corporate governance, are all topics of ongoing research but the principles articulated by the UK regulator, the Financial Reporting Council, remain applicable to all organisations. The major reports written in 2011 and 2012¹ are summarised as follows:

the board must determine its willingness to take on risk, and the desired culture within the company

risk management and internal control should be incorporated within the company's normal management and governance processes, not treated as a separate compliance exercise

the board must make a robust assessment of the principal risks to the company's business model and ability to deliver its strategy, including solvency and liquidity risks. In making that assessment the board should consider the likelihood and impact of these risks materialising in the short and longer term

once those risks have been identified, the board should agree how they will be managed and mitigated and keep the company's risk profile under review. It should satisfy itself that management's systems include appropriate controls, and that it has adequate sources of assurance

the assessment and management of the principal risks, and monitoring and review of the associated systems, should be carried out as an on-going process, not seen as an annual one-off exercise, and

this process should inform a number of different disclosures in the annual report: the description of the principal risks and uncertainties facing the company; the disclosures on the going concern basis of accounting and material uncertainties thereto; and the report on the review of the risk management and internal control systems.²

The questions we have set out below have emerged from our discussions through the lenses of both executive and non-executive roles on boards whether as chief risk officers, chief operating officers, non-executive chairs

1 Boards and Risk 2011 Financial Reporting Council and The Sharman Inquiry 2012.

2 www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf.

of audit finance and risk committees of boards or as members of boards setting strategy for a business and managing issues as they arise or through the scanning of risk horizons. Risk as viewed by a board encompasses three very broad areas:

1. Strategic – to ensure that risk management is embedded in the corporate objectives of the board
2. Cultural – to ensure that the people in the organisation led by its board have embraced risk management as part of the culture of the organisation
3. Operational – to ensure that the strategic and cultural embedding of risk management is operationalised so that it becomes a practical rather than theoretical tool in managing the risk of the business

The questions on risk management matters that we feel all board members should ask about an organisation they are charged with governing include the following:

- How does the organisation define risk?
- Has the organisation defined what its appetite for risk is?
- Does the organisation have a risk management policy?
- How is risk managed and reported?
- How does the organisation operationalise its risk management policy, and is there a clear risk management framework in place?
- Who is responsible for the executive function of risk management and to whom does it report?
- Is the risk management function independent from the business and able to demonstrate robust challenge on all risk matters?
- How often does risk management appear as an agenda item on matters considered by the board and its committees?
- To whom are the functions of risk management delegated by the board and what authority do they have to manage risk?
- Has the organisation defined what its key risk indicators are?
- How has the organisation defined the key risk indicators?
- Do you understand how these risk indicators are compiled (data quality) and reported (monitoring)?

- Who gets to see, review, and comment on these indicators and how often is this done?
- Are risks categorised and assigned to “risk owners” with the appropriate seniority to demonstrate they are effectively managed and or mitigated?
- How are risk issues escalated within the business?
- How are risks to the business recorded?
- Is there a corporate risk framework and risk register?
- How often is the risk register updated and reviewed?
- How often do the risks on the register change ratings?
- Who owns the risk management process?
- Is the risk management process one for “meting out justice,” or is it a process for a learning organisation?
- Is the risk management framework an insurance-based structure, or is it a framework that is embedded in all organisational processes?
- Who tracks risk events and how are risk issues closed off?
- Is risk management treated as a part of internal audit, or is it treated as a separate function?
- Can people within the organisation articulate what its critical risks are?
- Does the organisation operate a three-lines-of-defence policy?³
- Are the organisations’ corporate objectives and view of risk aligned?
- How are divergences in opinion on matters of risk managed?
- How process driven is risk management?
- Is there a healthy tension between management and the risk and compliance functions?
- Is there a scorecard process for risk management, or is some other process used to rate and manage risks?
- Have the controls that provide for safe ratings on risks been tested? How often are these key controls tested for reliability?⁴

3 These are: First line of defence: Management controls and internal control systems; Second line of defence: Organisational compliance functions such as compliance departments and internal audit; Third line of defence: External assurance such as through independent audit.

4 Also referred to as avoiding the “green-washing syndrome.”

- Are board papers manageable, or are board members expected to read the equivalent of a medium-length novel in preparation for meetings?
- How often are risks stress-tested?
- Does the organisation self-assess and review long-term viability?
- Are there any pressures that would prevent disclosure and dialogue between executives and board members?
- What does the organisation do with its risk management information? How serious are the discussions around risk management at board level?
- What level of transparency does the business demonstrate with its external advisers such as its auditors?
- How transparent is the organisation within its own hierarchy?
- Does the organisation encourage the recording of breaches, errors, and near misses in the pursuit of learning as a way of risk management?
- Are the financial, taxation, and business regulatory requirements understood and complied with?
- How seriously does the organisation guard its reputation in its interactions with stakeholders?
- Does the organisation understand who its key stakeholders are and what that means for the organisation and its viability?
- What risks has the organisation dealt with in the past and how likely are those risks to materialise again?
- Does the organisation have the appropriate skills to identify and manage risk to it?
- How are emerging risks captured and considered by the board, particularly if it impacts the firm's risk profile?

In writing such a chapter as this it feels incumbent on us to try and describe what a good risk management environment set by a board might look like and of course, whilst each organisation will have differences in what it does and the culture it creates, some basics remain constant, and so we have tried to frame what good looks like in a brief paragraph with general application.

A good risk framework would exist where an organisation's board has set a clear corporate strategy understood by the entire organisation and reflected in its mapping and management of risks to deliver that strategy. The board will be clear about how the organisation will deal with those risks, whether by instituting controls, conducting periodic reviews,

carrying insurance, or avoiding or, indeed, accepting risks. Risk management would be embedded in the culture of the organisation as something used as a learning tool to improve outcomes, operational safety, and the sustainability of the organisation in delivering its strategic objectives, and would be reflected in the risk outputs of the organisation, which would be practical and used by management to learn and improve its operations beyond being theoretical outputs or something used to mete out punishment. Finally, these risk outputs would be translated into practical operational controls, risk indicators, risk maps, risk registers, and assurance frameworks that were reliable, accurate, complete, operationally useful, and which delivered the strategic objectives of the organisation.