Better board oversight

A guide to where boards of directors can look for useful insight

Tim J. Leech
Managing Director, Global Operations at Risk Oversight Solutions

Board risk oversight expectations continue to escalate. In a global world, where directors have limited time for professional development, where can/should directors look for practical information, advice and guidance?

For the last 30 years of my career I have focussed on helping organisations around the world and their boards meet escalating risk oversight expectations. Those expectations accelerated rapidly following the 2008 global financial crisis and continue to accelerate as new colossal corporate governance failures, such as Wells Fargo, Boeing, Nissan and many others, come to the forefront. To stay current over the past three decades I have looked to a range of sources for updates on new developments, legal jurisprudence precedents re director standard of care, and practical 'how to' advice. This article gives an overview of where boards of directors that want to stay current on board oversight of risk can look for useful guidance.

Staff in the company you oversee

Boards have tremendous power to demand information they want. I regularly recommend boards assign responsibility to the corporate secretary to update directors on important corporate and risk governance developments. Quarterly board updates on this subject are appropriate, given the rate of change in the world. The company's corporate secretary should, in turn, assign responsibility to the chief internal auditor and chief risk officer, where one exists, to provide the corporate secretary, or the board directly, with updates on relevant corporate and risk governance developments. The updates should be short (under two pages) with links to more details for those board members who are interested.

Boards need to make it very clear to the board secretary that this is information they want each quarter to help them meet their corporate governance and risk oversight expectations.

The information-seeking process should start by the board director(s) with primary responsibility for oversight of internal audit and risk management asking the chief audit executive (CAE) and/or the chief risk officer (CRO) a few simple questions:

1. Does the company use a strong first-line risk management approach where management is the primary risk assessor/reporter on important objectives, or do we rely on second- and third-line assurance groups to identify and report problem areas to the board?
2. Does the company provide formal training to management responsible for important objectives on how to identify and assess risks and assess acceptability of residual risk linked to those objectives? If yes, how much and how often?
3. Which assurance approach or approaches does the company use as a primary methodology to obtain assurance – objective centric, risk centric, process centric, control centric or compliance centric? Why has it selected the mix of assurance methods it uses?

More details on the 10 primary assurance methods available can be sourced online.[1]

Professional publications

I have been writing in the area of board oversight of risk now for many years. Many others I have great respect for write regularly for influential platforms, such as the *Harvard Law School Forum on Corporate Governance*, and journals targeted specifically at board directors like *Ethical Boardroom* in the UK, Conference Board Director Notes, Conference Board Governance Blog and the National Association of Corporate Directors in the US. I encourage you to subscribe to and monitor these sources.

After 30 plus years of monitoring director-focussed publications globally, my vote for top corporate governance advisor is an American – Martin Lipton and his colleagues at Watchell, Lipton, Rosen and Katz who regularly publish in the *Harvard Law School Forum*. You can access a sample of their work online.[2] The posts do a great job overviewing legal standard of care for directors who are subject to US law and, more recently, other global developments and resources. Since the US represents the country that the majority of the biggest and most successful corporations in the world use to access capital, these periodic updates are relevant to board members around the globe. In addition to the legal perspective on evolving director duty of care that Lipton's posts provide, they offer candid and well-researched views on what good directors should be asking their companies for. While some of his advice may seem like overkill to directors carrying a heavy work burden, these posts are the best I have seen. They cover the broad corporate governance space, as well as the more granular subset of risk governance.

Best new board risk oversight guidance

A new not-for-profit organisation has emerged in the UK called The Risk Coalition. Its founding members

MANAGING BOARDROOM OVERSIGHT EXPECTATIONS
Directors should keep informed of the latest developments in risk governance

include board associations, risk associations, internal auditors and more. It has the visible support of UK regulators.

In December of 2019, after releasing an exposure draft and receiving input from a broad range of stakeholders, including board members and board associations, The Risk Coalition released in final a new guide titled *Raising The Bar: Principles-based Guidance For Board Risk Committees And Risk Functions In The UK Financial Services Sector.*[3]

Although the report cover specifically states this guidance is intended for financial sector organisations in the UK, the recommendations are, in my opinion, the best I have seen for boards in all business sectors, including not-for-profit and government functions with boards, that want to do a better job overseeing risk functions and risk governance. The Risk Coalition has indicated that it may issue another report specifically tailored to address risk oversight in other business sectors. Its 2019 guidance assumes all organisations have a risk function, which is often not true in sectors outside of the financial sector.

In the foreword of this guidance there is a short paragraph that has disproportionate importance. It states: *"The separate guidance of 'eight principles' for board risk committees and 'nine principles' for risk functions is helpful. The emphasis on first-line responsibility and accountability for risk management is overdue. Hopefully, the three lines of defence model benefits from extra clarity."*

Boards have tremendous power to demand information they want. I regularly recommend boards assign responsibility to the corporate secretary to update directors on important corporate and risk governance developments

This is the first authoritative guidance I have seen that specifically recommends boards call on the companies they oversee to move away from traditional internal audit and risk management and reporting methods which are, in essence, weak first-line risk governance models, to a stronger first-line risk governance approach. Strong first-line risk governance is an approach where accountability of the first line/management to regularly assess and report upwards on the state of risk linked to top value creation and preservation objectives to boards is clear; accountability to assess and report upwards rests squarely with management responsible for important value creation and preservation objectives; and management is provided with adequate training to fulfil that expectation.

Paragraph 27 of Principle 5A for boards in the guide and paragraphs 29 to 33 of Principle 6 are illustrative of the emphasis on this dimension in this new guidance (see box-out, right).

On page 26/36 of the report, the authors take the bold step of proposing what the Institute of Internal Auditors should do when they update IIA guidance on what is generally known as the three lines of defence model (3LoD)– an update expected in the first half of 2020: "First line management should manage risks through the disciplined application of the organisation's risk management framework. The aim is to help the organisation achieve its strategic objectives while remaining within risk appetite. Consequently, first-line management should be the principal source of (non-independent) risk information presented to the board risk committee." »

27 Seek appropriate assurance on the completeness, accuracy and fairness of first-line management's reporting of the organisation's:
- principal and emerging risks (including emerging categories of risk) and their impact on the likely achievement of the organisation's strategic objectives in both the short- and medium-term
- proposed or actual risk responses
- significant incidents and near-misses, actual or likely breaches of risk appetite, overall risk profile and risk capacity

In meeting this principle, the board risk committee should:

29 Assess the quality and appropriateness of board-level risk information and reporting from each of the lines of defence, including whether significant matters are escalated sufficiently promptly and the overall quality of supporting narrative and analysis

30 Challenge whether first- and second-line board-level risk information and reporting adequately leverage risk data aggregation and analysis techniques to identify latent patterns of risk and predict emerging risk trends and themes

31 Consider whether board-level risk information and reporting is both comprehensive and comprehensible, enabling non-executive directors to understand, probe and challenge executive management effectively

32 Seek appropriate assurance on the quality and reliability of the organisation's risk information governance and reporting arrangements, including the adequacy and appropriateness of executive management procedures for deciding what risk-related information to present to the board and its committees

33 Confirm that risk information reporting between group entities (where relevant) and with regulatory authorities is complete, accurate and timely

The statement in the foreword of The Risk Coalition guidance that states 'the emphasis on first-line responsibility and accountability for risk management is overdue' may be the biggest single understatement in board guidance documents that I have seen in my 35 years monitoring the space.

From international professional associations like the IIA

In late 2019, the Institute of Internal Auditors released a study titled *OnRisk 2020: A Guide To Understanding, Aligning, And Optimising Risk*. While the authors of the guide clearly assume that enterprise risk management is fundamentally about creating risk registers/risk lists, not assessing certainty important objectives will be achieved (an assumption I have written at length on and take huge exception to), it does contain some incredibly important conclusions that point to major problems in the quality of information on risk status that boards are receiving:

- **Boards are overconfident** Boards consistently view the organisation's capability to manage risks higher than executive management – evidence of a critical misalignment between what executive management believes and what is communicated to the board
- **Boards generally perceive higher levels of maturity in risk management practices** Board members' perceptions of risk knowledge and capability place them ahead of executive management and chief audit executives, relative to risk maturity, therefore making them more likely to believe those risks are better managed
- **'Acceptable misalignment'** on risk is a prevalent and dangerous mindset. A majority of respondents believe some misalignment on risk perception should be expected, with some viewing it as 'healthy'. While misalignment around individual knowledge of a risk may be acceptable, based on varying roles, misalignment on the perception of the organisation's capability to manage a risk is a serious concern

The authors go on to say on page 9/40 of the report: *"One reason for this misalignment may be the quality and completeness of information flowing to boards. Boards need information that is complete, accurate, and timely, and must establish proper oversight practices to ensure this. This challenge is not unknown to boards. According to the National Association of Corporate Directors (NACD) report,* 2019 Governance Outlook, *'Directors struggle to keep up with a rapidly evolving business landscape. For the second year in a row, NACD's public company governance survey found that a large majority of directors, almost 70 per cent, report that their boards need to strengthen their understanding of the risks and opportunities affecting company performance.'[2] The cited public company governance survey also found boards are spending twice as much time reviewing information from management than from external sources, 'revealing a heavy dependence on management views and analysis in fulfilling their oversight duties'. What's more, more than half (53 per cent) of directors indicated that the quality of information from management must improve, 'suggesting the board needs better, not more, information from management'."*[3]

Although I am strongly against the reports and studies that have an underlying assumption that enterprise risk management means creating risk lists, and don't think the new IIA report OnRisk identifies the real reasons boards are not getting the information they require to meet risk oversight expectations, it does shine a spotlight on a really big problem – boards are not getting the information they need to do a good job of overseeing risk.

From the Americans

In 2017, the US Committee of Sponsoring Organisations, commonly known as COSO and comprised of five accounting/finance-related organisations, released a new guidance document, on *Enterprise Risk Management (ERM)*. Its biggest shortcoming in terms of being useful is that the full guidance is a daunting 202 pages. Unlike the clarity in the principles-based' The Risk Coalition guidance from the UK, COSO ERM messaging to board members on what they should be doing to oversee risk governance is obfuscated and some have labelled it 'consultant speak'. Although it has important messages, only incredibly persistent board members are likely to have attempted to onboard key COSO ERM messages.

On the positive side, COSO ERM 2018 guidance's major contribution to better risk governance is that it stresses that risk should be seen and assessed in direct relation to the company's strategy and objectives, and risk management should be integrated with performance. In my experience, only a small minority of companies today have integrated their ERM frameworks with top strategic objectives or performance. Although there is much to be critical about in this 2017 US guidance, the executive summary does call on boards to ask management some really important questions.

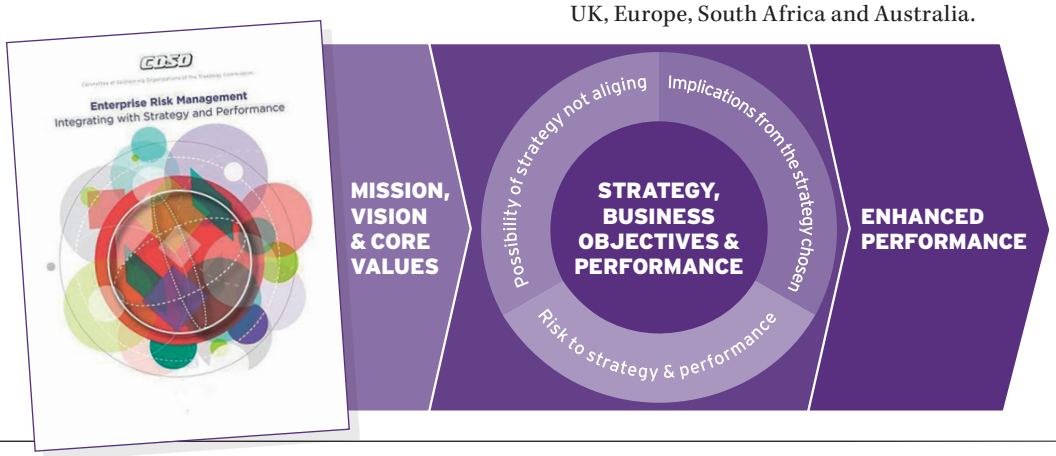
Questions for management

Can all of management – not just the chief risk officer – articulate how risk is considered in the selection of strategy or business decisions? Can they clearly articulate the entity's risk appetite and how it might influence a specific decision? The resulting conversation may shed light on what the mindset for risk taking is really like in the organisation.

Boards can also ask senior management to talk not only about risk processes but also about culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the risk culture, and how has that changed? As things change – and things will change, whether or not they're on the entity's radar – how can the board be confident of an appropriate and timely response from management?

Best regulatory approach

Driven by the countries where my clients operate, I have had to stay up to date on what national regulators believe, in the opening words of The Risk Coalition, 'good looks like'. The most notable regulators I track are regulators in Canada, the US, UK, Europe, South Africa and Australia.



After working globally, my pick for the most useful national regulatory guidance goes to the Financial Reporting Council (FRC) in the UK. Overall, the UK Governance Code is a useful and principles-based guide. FRC has also been doing some ground-breaking research on the impact of corporate culture on corporate performance and behaviour. I believe at a high level the UK Governance Code, when combined with the new The Risk Coalition guide *Raising the Bar* provides a fairly comprehensive view of what boards need to be doing.

Two big cautions on FRC guidance

In spite of the FRC being my national regulator guidance of choice, the FRC may well be a primary cause of companies globally adopting ineffective risk registers/risk listing as a foundation for their ERM frameworks. This UK-led movement to create risk lists, which came to the fore when the UK initially launched the UK Governance Code, has had the unfortunate effect of creating the illusion of effective risk management. Paragraph 28 in the 2018 Code and earlier versions is likely the main culprit:

28. The board should carry out a robust assessment of the company's emerging and principal risks. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated.

These words in the 2018 Code and earlier versions have caused companies to believe that they need to compile lists of 'principal risks' and adopt 'risk-centric' ERM frameworks. Unfortunately, boards have been receiving little information on the affect of the risks in these risk registers/risk lists on the certainty of achieving important strategic/value creation and value preservation objectives. The FRC would do well to rewrite the Governance Code in the area of risk oversight as soon as possible.

The other main area over which I have raised concerns with the FRC in the past, is their lack of guidance for boards on how to assess the effectiveness of internal audit functions. Audit committees are responsible for overseeing the effectiveness of internal audit but little is provided to help boards know 'what good looks like'. The Risk Coalition *Raising The Bar* guidance does not address this dimension of board oversight in a useful way.

25. The main roles and responsibilities of the audit committee should include:

- Monitoring and reviewing the effectiveness of the company's internal audit function or, where there is not one, considering annually whether there is a need for one and making a recommendation to the board

In summary, while there are some significant areas for improvement, particularly the two areas noted above, the FRC UK Governance Code is still the best risk governance guidance out there right now from a national regulator.

Powerful institutional investors

A relatively new phenomenon that boards need to be aware of is the increasingly strident risk governance expectations of institutional investors. The biggest and most powerful institutional investors in the world are calling on boards to do a better job overseeing risks that have potential to impact corporate strategy and corporate solvency.

While these players that control literally trillions of dollars of capital, including behemoths like BlackRock and Vanguard, provide few practical details on 'what good looks like' in terms of strategy and risk oversight, they do make it abundantly clear that want to hear persuasive stories about how boards and senior management of companies they have invested in are satisfying themselves that the companies they oversee have effective risk frameworks, linked to top strategic/value-creation objectives, as well as potentially fatal value-preservation objectives, such as complying with laws, publishing reliable financial information and data security.

Those interested in a quick primer on the rise in power and expectations of institutional investors can access my fall 2019 article in *Ethical Boardroom* titled *Board Oversight of Strategy and Risk*.[4]

The biggest and most powerful institutional investors in the world are calling on boards to do a better job overseeing risks that have potential to impact corporate strategy and corporate solvency

Going forward

What is abundantly clear is that boards and directors that ignore the rapid escalation in risk oversight expectations do so at their peril. Corporate, as well as personal, reputations are 'at risk'. Best wishes for success with your risk oversight work in 2020. I hope you and the companies you oversee find this advice useful.

[1]http://bit.ly/2mkJW0I [2]https://corpgov.law.harvard.edu/contributor/martin-lipton/ [3]http://bit.ly/2QTIP4X
[4]https://riskoversightsolutions.com/wp-content/uploads/2011/03/EB_Autum2019_TimLeech_Board-Oversight-of-Strategy-and-Risk.pdf

RISKY BUSINESS
It needs improving but the FRC's UK Governance Code is still the best