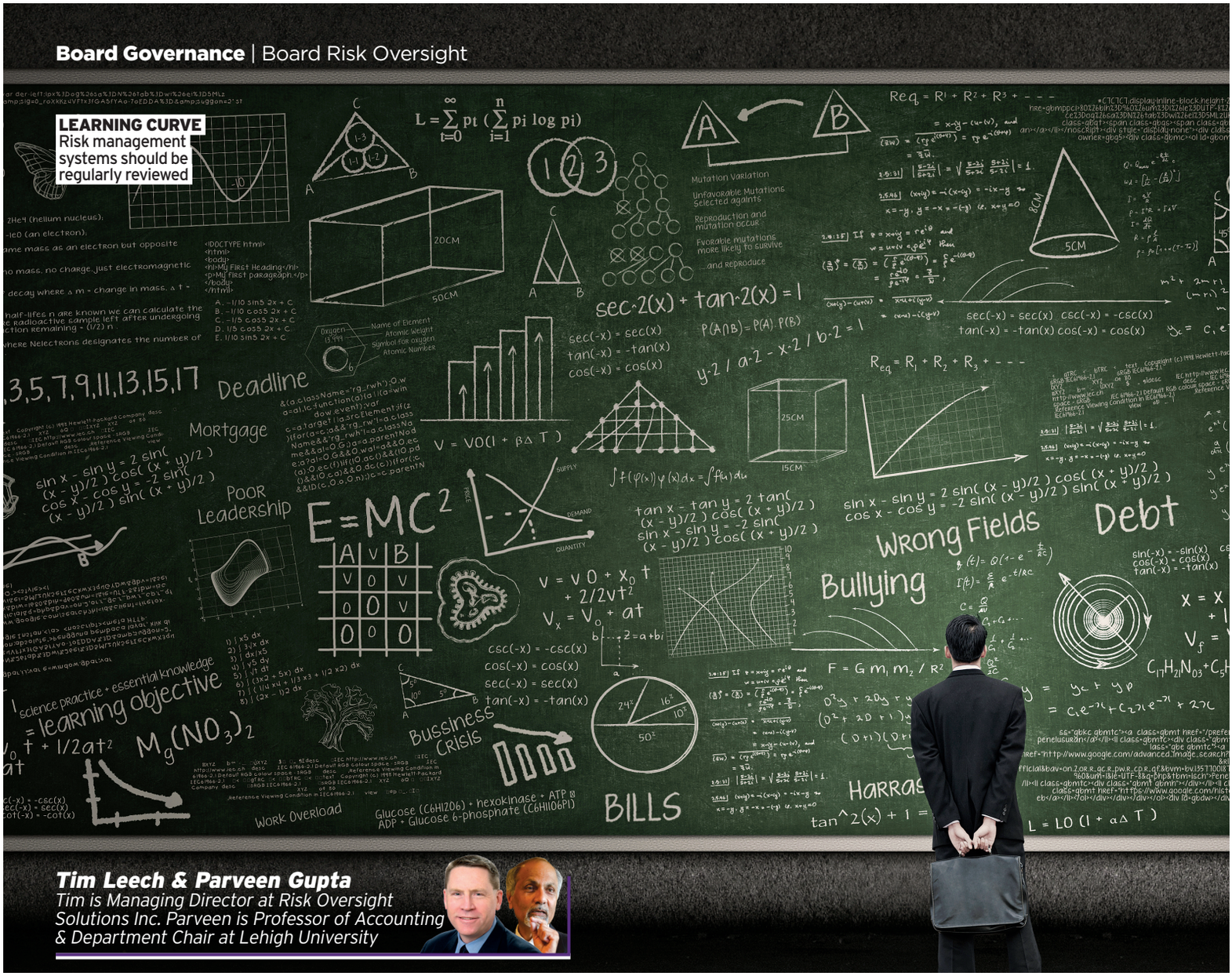


Tim Leech & Parveen Gupta
Tim is Managing Director at Risk Oversight Solutions Inc. Parveen is Professor of Accounting & Department Chair at Lehigh University

What knowledge and skills do directors need?

This article provides an overview of the risk oversight knowledge and skills required to equip directors to better drive value creation, prevent significant corporate value erosion and, perhaps most importantly, help directors protect their personal reputations as guardians of stakeholder interests.

When considering what new knowledge and skills a person needs it is generally accepted in the education and learning community that it makes sense to start with what are called 'learning outcomes' or, more simply stated 'what levels of knowledge, skills and abilities does a person need to do their job better?'.

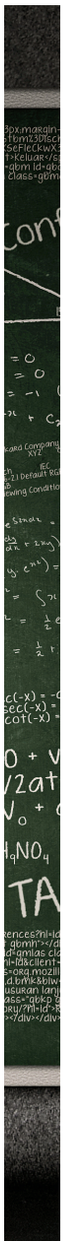
This article first reviews emerging requirements for directors of US public companies and then discusses the considerably more codified and advanced 2015 UK public company board requirements. It is expected that other countries, including the US, will follow the UK's lead in this emerging area of board risk oversight.

Today's board risk oversight requirements require new tools and new ideas

SEC raises the bar in 2009

Most experts agree that the roots of the 2008 global financial crisis, started in the US. Following the crisis the US Securities and Exchange Commission (SEC) issued new proxy disclosure rules as part of US reform efforts. The SEC Final Rule[1] released in the fall of 2009 summarised the SEC requirements in this area as follows:

"The final rules also require companies to describe the board's role in the oversight of risk. We were persuaded by commenters who noted that risk oversight is a key competence of the board, and that additional disclosures would improve investor and shareholder understanding of the role of the board in the organisation's risk management practices. Companies face a variety of risks, including credit risk, liquidity risk and operational risk. As we noted in the Proposing Release, similar to disclosure about the leadership structure of a board, disclosure about the board's



involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company. This disclosure requirement gives companies the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example. Where relevant, companies may want to address whether the individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee or how the board or committee otherwise receives information from such individuals."

Distilled, this paragraph says some thought should be given to what the board is currently doing in the area of risk oversight and what it should communicate to investors about its role. Given the way the SEC has written it, one could argue that a company's disclosure could legally disclose that a board does very little of substance in the area of risk oversight and leave it to stakeholders to decide if they are satisfied or dissatisfied with that decision. Reports and studies by Deloitte,[2] PwC[3],and others have documented in detail what the US listed companies have actually been doing and disclosing in response to the 2009 Rule.

Given no documented reaction from the SEC on status quo board risk oversight disclosures and the sufficiency of the 2009 disclosure requirements, it appears that the SEC is generally satisfied with letting market forces do the work. While the formal duty of care expectations relating to the board risk oversight in the US is currently much lower than the new 2015 requirements in the UK, we expect it will evolve to the next level over the next five years. Directors of US-listed companies that want to voluntarily improve their board risk oversight in the interim and directors of large and medium-size US financial institutions being pressured by their regulators to change will play leadership roles in influencing and driving change.

UK sets a higher bar in 2014

Since the 2008 financial crisis the Financial Reporting Council (FRC), the UK public company regulator, has been steadily increasing the codification and clarity related to board risk oversight expectations.

The recently revised UK Corporate Governance Code released in September 2014 provides the clearest and most stringent set of board risk oversight expectations issued to-date globally. Effective for fiscal years starting after 1 October 2014 all UK listed public companies must include statements from the board of directors in their financial statements covering the following areas:

Statement on risk management and internal control

57. Provision C.2.3 of the Code states that the board should report in the annual report and accounts on its review of the effectiveness of the company's risk management and internal control systems. In its statement the board should, as a minimum, acknowledge that it is responsible for those systems and for reviewing their effectiveness and disclose:

- That there is an ongoing process for identifying, evaluating and managing the principal risks faced by the company
- That the systems have been in place for the year under review and up to the date of approval of the annual report and accounts
- That they are regularly reviewed by the board
- The extent to which the systems accord with the guidance in this document

58. The board should summarise the process it has applied in reviewing the effectiveness of the system of risk management and internal control. The board should explain what actions have been or are being taken to remedy any significant failings or weaknesses.

Where this information has been disclosed elsewhere in the annual report and accounts, for example in the audit committee report, a cross-reference to where that information can be found would suffice. In reporting on these actions, the board would not be expected to disclose information which, in its opinion, would be prejudicial to its interests.

59. The statement should incorporate, or be linked to, a description of the main features of the company's risk management and internal control system in relation to the financial reporting process, as required under the Disclosure and Transparency Rules.

60. The report on the review of the risk management and internal control systems is normally included in the corporate governance section of the annual report and accounts, but this reflects common practice rather than any mandatory requirement and companies can choose where to position it in their report. In any event, companies should consider whether and how to link reporting on the review of the risk management and internal control systems to the information on principal risks in the Strategic Report and material uncertainties relating to the going concern basis of accounting in the financial statements.

The formal duty of care expectations relating to the board risk oversight in the US is currently much lower than the new 2015 requirements in the UK

The new risk oversight learning outcomes required by directors of UK-listed companies and directors in other countries that want to improve their risk oversight capabilities, are summarised in the box below.

BOARD RISK OVERSIGHT 'LEARNING OUTCOMES'
Directors need to be able to competently:

1. Assess whether the risk management framework in place that provides the information on risk status they receive is capable of identifying and escalating the status of the 'principle risks faced by the company'
2. Decide if the risk management framework is 'in accord with the guidance in the September 2014 UK Code' and related guide[4]
3. Assess whether the risk management framework in place is, or is not, 'effective'
4. Understand what constitutes 'significant failings or weaknesses' in a risk management framework and be able to competently assess what would be an appropriate 'remedy' to rectify the identified weaknesses
5. Assess whether the risk management systems specific to external financial reporting are 'effective'

Learning outcome #1

Decide whether the board is getting a materially complete report on risk status

The first learning outcome relates to completeness of information boards receive on the status of residual risk. Leading up to the 2008 financial crisis, more than a few boards were shocked to learn that the company they oversaw was technically insolvent and required massive government support to survive. Many of those companies had implemented annual/semi-annual processes to populate their Risk Register and provided colour-coded 'risk lists' and 'risk heat maps' for their boards to review. They simply didn't work very well. Boards need to start by asking the CEO what he or she does to ensure the board receives a materially complete report on the state of residual risk related to all business objectives key to the company's long-term survival and success.

Boards should consider 1) insisting that Risk Register be replaced with an Objectives Register to improve completeness of coverage; 2) taking steps to satisfy themselves that the Objectives Register includes the top value creation and potential value erosion objectives; 3) requiring a regular report from the CEO/CRO on the residual risk status of those objectives[5]; and 4) requiring an opinion from the Chief Internal Auditor on the completeness and reliability of the Objectives Register information.

Another step recommended by the Financial Stability Board[6] (FSB) that appears eminently practical is to require that the CEO be formally »

assigned responsibility for designing and implementing an effective risk appetite framework and providing the board with regular and materially reliable reports on residual risk status.

In essence, a consolidated report on the entity's residual risk status akin to the status report provided by a balance sheet.

Learning outcome #2

Know how the risk management framework measures up against emerging expectations

In order for a board to meet the UK expectation that the risk framework is in accord with the UK Corporate Governance Code requirements they need to clearly understand the expectations laid down in the Code and how current practices measure up to those expectations. We believe the UK expectations currently represent global best practices in this area.

Learning outcome #3

Assess whether the risk management framework is 'effective'

This is quite likely the most challenging expectation since there is considerable lack of agreement globally on what constitutes an 'effective' risk management framework. Although much remains to be done, we believe that the spirit of this requirement seeks to answer one simple question: 'Is the risk management framework that the company has adopted capable of identifying, assessing, and escalating to the board key risks that threaten the achievement of most important objectives and providing the board with materially reliable and timely information on the residual risk status on those objectives?'

To gain important background/context information on what regulators think constitutes an effective framework, we recommend that directors read the UK September 2014 Corporate Governance Code and related risk guidance and the FSB Principles For An Effective Risk Appetite Frameworks. Directors should also follow the ongoing work of the Committee of the Sponsoring Organisations (COSO) in the US to update the very dated 2004 COSO ERM framework. COSO has announced a target release date of 2016. A stated objective of the COSO ERM update is to help companies and boards cope with the rapid escalation in risk management and risk oversight expectations.

Learning outcome #4

Assess whether the risk management framework has significant failings/ weaknesses and how to best remedy those failings/ weaknesses

In 2000, following a host of corporate governance scandals including Enron, WorldCom, HealthSouth, Parmalat and others, the Institute of Internal Auditors (IIA) changed its International Professional Practice Framework (IPPF) standards and introduced a new standard that stated internal auditors should assess and contribute to the improvement of risk management processes. In 2010, following the 2008 global crisis, the wording was modified and the word 'should' was replaced with 'must'.[7] Unfortunately, five years later, global surveys indicate that only a minority of Chief Audit Executives (CAEs) have provided boards with a formal, comprehensive opinion on the effectiveness of their company's risk management framework and only a minority have taken formal training on how to complete the required assessment.

Boards of companies that have internal audit functions that have not provided them with a formal opinion on the effectiveness of the company's risk management framework should require it. They should request briefings from their CAE on the training they or those hired by the CAE to assist them, have taken and the audit criteria they have used to complete the assessment. Boards of companies that have no internal audit function should consider retaining qualified risk assurance specialists to provide them with an opinion on the current effectiveness of the company's risk management framework, including its ability to produce materially reliable consolidated reports on residual risk status linked to top value creation and potential value erosion objectives.

Directors may believe they have the luxury to watch and learn from others but may suffer negative consequences

Learning outcome #5

Assess whether risk management processes related to financial reporting are effective

Traditional approaches to improve reliable financial reporting imposed by regulators, including those implemented in response to Sarbanes-Oxley section 404 in the US, have focused on producing opinions from the CEO/ CFO/internal audit/external audit on whether they believe internal controls are 'effective'. Instead of accepting this binary and subjective verdict on the whole set of internal controls over external financial reporting, boards should ask for a detailed report on which specific line items of the balance sheet, income statement and note disclosures have the highest composite uncertainty after considering risk treatments/ controls in place. Or, stated another way, the highest composite residual risk that the line/note disclosure may not be reliable[8].

The UK and international auditing standards have already moved in this direction with new external audit disclosure standards[9]. In the US, the Public Company Accounting Oversight Board (PCAOB) has proposed similar changes in this area[10] but is meeting with strong resistance from the audit and business communities. Regardless of whether new external audit reporting standards are approved in the US, audit committee members should proactively ask for this information to assess if management's risk appetite/tolerance related to the objective of issuing materially reliable financial disclosures is aligned with their risk appetite/tolerance.

Some boards will learn faster than others

In this article we have provided an overview of what we believe directors who want to proactively meet the new risk oversight expectations should do now. Boards of UK-listed companies currently have the highest regulatory bar to clear [11] but it is likely that other countries, including the US, will follow as the old adage says, sooner rather than later.

If another well-known adage 'necessity is the mother of invention' is true, boards of public companies in the UK and large financial service companies globally whose regulators have been influenced by the Financial Stability Board recommendations will be the first to respond in a significant way. Directors of public companies in other parts of the world where regulators have not yet moved decisively in this direction, including Canada, may believe they have the luxury of being able to watch and learn from the experiences of others, but may suffer a range of negative consequences in the marketplace in the interim. What is absolutely clear is that the new board risk oversight requirements and expectations necessitate new methods, new tools and new skills. The changes necessary won't come easy.

[1]SEC RELEASE NOS. 33-9089; 34-61175; IC-29092; File No. S7-13-09] RIN 3235-AK28 PROXY DISCLOSURE ENHANCEMENTS, 2009. https://www.sec.gov/rules/final/2009/33-9089.pdf. [2]See http://deloitte.wsj.com/cfo/2014/03/07/proxy-disclosures-indicate-growing-risk-oversight-by-boards/. [3]See www.pwc.com/en_GX/us/point-of-view/assets/pwc_pointofview_risk_disclosure.pdf. [4]Guidance on Risk Management, Internal Control and Related Financial and Business Reporting, Financial Reporting Council, September 2014. [5]For more details See http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-Solutions-Tim-Leech-Objective-Centric-vs-Risk-Centric-ERM-Risk-Spotlight-Webinar-March-23-2015.pdf (current as of April 2015). [6]See FSB Principles for an Effective Risk Appetite Framework, 2013, page 9. [7]International Standards for the Professional Practice of Internal Auditing (Standards) 2013 page 11. https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf. [8]See Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act, Tim Leech & Lauren Leech, International Journal of Disclosure and Governance, September 2011. [9]See PwC Auditor Reporting: Momentum Builds Toward More Informative Reporting http://www.pwc.com/en_GX/gx/audit-services/publications/assets/pwc-auditor-reporting-momentum-builds-june-2014.pdf (as of April 2015). [10]See http://journalofaccountancy.com/news/2014/jan/20149360.html for more details. [11] *It is important to note to readers that the UK operates on a 'comply or explain' basis of corporate governance. There are no regulatory sanctions for not complying provided the deviation is disclosed and explained.*