EDPACS

The EDP Audit, Control, and Security Newsletter

ISSN: 0736-6981 (Print) 1936-1009 (Online) Journal homepage: http://www.tandfonline.com/loi/uedp20

Board Oversight of Management's Risk Appetite and Tolerance: Regulators Claim they Expect it but Change will Not Come Easy

Tim Leech & Parveen Gupta

To cite this article: Tim Leech & Parveen Gupta (2015) Board Oversight of Management's Risk Appetite and Tolerance: Regulators Claim they Expect it but Change will Not Come Easy, EDPACS, 51:4, 9-14, DOI: 10.1080/07366981.2015.1038159

To link to this article: http://dx.doi.org/10.1080/07366981.2015.1038159

Published online: 16 Apr 2015.

Submit your article to this journal

Article views: 53

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=uedp20

Download by: [Murdoch University Library] **Date:** 04 October 2017, At: 18:17

BOARD OVERSIGHT OF MANAGEMENT'S RISK APPETITE AND TOLERANCE: REGULATORS CLAIM THEY EXPECT IT BUT CHANGE WILL NOT COME EASY

TIM LEECH AND PARVEEN GUPTA

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

Abstract. In the aftermath of the 2008 global financial crisis post-mortems were convened in countries around the world to identify what went wrong. A unanimous conclusion was that boards of directors of public companies in general, and financial institutions in particular, need to do more to oversee "management's risk appetite and tolerance" if future crisis are to be avoided. This finding represents a significant paradigm shift in role expectations while introducing a new concept the Financial Stability Board (FSB) has coined effective "Risk Appetite Frameworks" (RAFs).[i] Regulators around the world are now moving at varying speeds to implement these conclusions by enacting new laws and regulations. What regulators appear to be seriously underestimating is the amount of change necessary to make this laudable goal a reality.

CODIFICATION OF BOARD RISK OVERSIGHT

Immediately following the onset of the 2008 global crisis a group called the Senior Supervisors Group (SSG), and later, the FSB the world's first global super regulator, went to work at record speed to publish, seek comments to exposure drafts, and issue guidance to national bank and securities regulators around-the-world. Excerpts from FSB's radical and far-reaching November 2013 guidance on RAF follows.

The Board of Directors Should...

1. approve the financial institution's RAF, developed in collaboration with the CEO, CRO, and CFO, and ensure it remains consistent with the institution's short- and long-term strategy, business and capital plans, risk capacity as well as compensation programs;
2. hold the CEO and other senior management accountable for the integrity of the RAF, including the timely identification, management, and escalation of breaches in risk limits and of material risk exposures.

The CEO Should...

1. establish an appropriate risk appetite for the financial institution (in collaboration with the CRO and CFO) that is consistent with the institution's short- and long-term

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom

strategy, business and capital plans, risk capacity, as well as compensation programs, and aligns with supervisory expectations;
2. be accountable, together with the CRO, CFO, and business lines for the integrity of the RAF, including the timely identification and escalation of breaches in risk limits and of material risk exposures

Internal Audit (or Other Independent Assessor) Should...

1. routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;
2. identify whether breaches in risk limits are being appropriately identified, escalated, and reported, and report on the implementation of the RAF to the board and senior management as appropriate

In 2010, in response to some of the initial SSG/FSB post-mortem analysis, the Securities and Exchange Commission (SEC) in the United States introduced new proxy disclosure rules[ii] that require a general broad acknowledgment in the annual proxy that the board is responsible for risk oversight. Since then, the Commission has not taken any steps to provide more granular guidance to clarify what they expect.[iii] Perhaps in anticipation of new U.S. disclosure requirements the Committee of Sponsoring Organizations (COSO) announced in October 2014[iv] that it is embarking on a two-year plan to update the now dated 2004 COSO Enterprise Risk Management (ERM) framework. A primary stated reason for the update is to assist companies and boards report on the effectiveness of their risk appetite frameworks.

In September 2014 in the United Kingdom, the Financial Report Council (FRC), the United Kingdom equivalent of the SEC, became the first national security regulator to codify and elevate the expectation that boards of directors of all UK-listed public companies must oversee management's risk appetite and tolerance.

Securities regulators in other countries are working to codify new expectations requiring boards visibly, and more effectively, oversee management's risk appetite and tolerance.

CHANGE WILL NOT COME EASY

The core idea that boards of directors should oversee management's risk appetite and tolerance appears to be a logical extension of their role and, at least on the surface, would appear easy enough to implement if boards and management are both willing. However, the reality is that there must be a major paradigm shift on the part of regulators, boards, senior management, risk specialists, internal and external auditors, and other risk "silos," including safety, environment, compliance, IT security, and others, to make this regulatory aspiration a reality. Some of the major roadblocks are discussed below.

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom

Roadblock #1: Regulators Themselves

Following a "perfect storm" of corporate malfeasance the United States enacted the Sarbanes Oxley Act of 2002. Section 404 requires that CEOs, CFOs, and external auditors form binary opinions whether they believe internal control over financial reporting is, or is not, "effective" using criteria drawn from a "suitable" control framework. The dated 1992 COSO internal control framework was deemed "suitable" by the SEC. The 1992 COSO control framework was recently replaced with the marginally better COSO 2013 control framework. Canada and other countries directionally followed the U.S. lead. The problem is, this approach does nothing to train senior management or auditors to assess and report on the state of "residual risk," the risk that remains after considering controls and other important risk treatments; or for boards to assess whether they are comfortable with management's risk appetite and tolerance. This results in the boards receiving little in the way of reliable information on the line items in the company's balance sheets and income statements with the highest composite uncertainty (or, stated another way, the highest likelihood of being materially wrong).

Roadblock #2: Internal Audit "Direct Report" Audit Methods

A large percentage of public companies maintain internal audit functions that complete spot-in-time audits and report "material weaknesses," "control deficiencies," areas needing improvement, and the like. What these audit opinions represent using a risk lens, is an opinion whether the auditors like, or dislike, the controls in place, and by extension, whether they like, or dislike the current state of retained/residual risk. How they have formed their like and dislike opinions on the state of residual risk is often unclear. More importantly, all agree, including the global Institute of Internal Auditors (IIA), that in spite of the apparent contradiction with current practices, it is management and the board's job, not internal audit, to decide how much retained risk is acceptable in pursuit of an organization's business objectives.

Compounding the problem, internal auditors in a large percentage of companies today do not use risk assessment methods designed to identify and assess the current state of residual/retained risk. Most do not know how to appropriately use recognized risk frameworks[v] or risk vocabulary[vi] in their daily work. Very few internal auditors have received much, if any, training on how to identify and consider the full range of risk treatments.[vii] It simply is not part of the current core curriculum or training offerings. The focus has been on identifying "internal controls," often without linking these controls to specific risks. It has not, with few exceptions, been on providing a consolidated entity level report on the current residual risk status related to key objectives for senior management and boards.

In the absence of reliable information on state of residual risk from business units and assurance specialists, senior management and, most importantly, boards of directors, are handicapped in their efforts to oversee management's risk appetite and

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom

tolerance. Regulators globally continue to support this "direct report/control centric" audit approach, while at the same time calling on boards of directors to oversee management's risk appetite and tolerance—a regulatory imposed recipe for confusion and future governance failures.

Roadblock #3: Traditional "Risk Centric" ERM Methods

The idea that management and boards should be actively and transparently involved in "risk management" is not a new one. Australia was the first country to pioneer a risk management standard in the mid-1990s (AS/NZ 4360). Gradually, over the next decade, other countries followed suit. In the U.S., COSO released its own ERM framework in 2004. ISO, the world's international standards setter, released the world's first global risk management standard in 2009. For a variety of reasons, including support from the consulting sector and resistance from management, the world has generally interpreted ERM to mean an annual exercise (with limited time and efforts) to build and maintain "risk registers," now increasingly being referenced less charitably as "risk lists." These risk registers are accompanied by color coded "heat maps" showing which risks had been rated as RED, based on the likelihood and impact of each risk and controls in place. Boards receive lists of the top 10/20/50/100 risks. Often these are stand-alone lists with no linkage to related business objective or a clear map showing how the top risks impact which business objectives. The fact that most important business objectives have 10 or more significant risks that create uncertainty the objective will be achieved has been, and is still today, largely ignored.[viii]

Roadblock #4: Practical Advice How to Actually Do It

In 2009, not long after commissions globally started to report their conclusion that weak/deficient board oversight of management's risk appetite and tolerance was a central root cause of the global crisis, the National Association of Directors (NACD) in the United States released its seminal Blue Ribbon Commission report, "Risk Governance: Balancing Risk and Reward." This report calls on boards to increase their focus and attention in this area and proposes six key board risk oversight duties. What is missing in that report, and is still largely unaddressed by the NACD and other director associations and regulators globally, are the practical steps and major changes companies must make, including the training and new tools necessary to help boards fulfill their new fiduciary duty to oversee management's risk appetite and tolerance.

Roadblock #5: Human Aversion to Radical Change

Last, but certainly not least, major changes are needed in regulatory attitudes and the corporate functions and processes that create and provide information on the state of retained risk. It is

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom

likely that not all CEOs want their boards of directors to know all the areas of high retained risk. For a variety of reasons, there may also be more than a few boards that do not want to know "the whole truth and nothing but the truth." Unfortunately, more than a few C-suites have kept boards in the dark in the past as management pursued strategies more aligned with maximizing their personal goals than the long-term success of their organizations. Major changes are needed in internal audit charters, training, certification, and methods. ERM specialists need to focus on developing new methods and tools that provide ethical senior management teams and boards with a consolidated report on the state of retained risk across the enterprise, including risks that threaten the achievement of the organization's top strategic objectives, as well as foundational objectives relating to legal compliance, reliable financial statements, data security, business continuity, and the like.

In summary, an old adage applies. Regulators should practice what they preach. if regulators truly want boards of directors to be more effective overseers of management's risk appetite and tolerance they should complete formal risk assessments on their stated objective of legislating better and more effective board risk oversight. Once they have properly identified the full range of significant risks to this objective, with the support of groups like the NACD, FEI, IIA, and the myriad of risk associations, they need to develop risk treatment strategies to reduce the very real likelihood that senior management and boards will not embrace this new regulatory imperative. Regaining the trust of investors and the public around the world is a goal that's worth the effort.

Notes

i. See Principles for an Effective Risk Appetite Framework November 2013, Financial Stability Board.
ii. U.S. Securities and Exchange Commission, "Final Rule on Proxy Disclosure Enhancements," Release Nos. 33-9089 and 34-61175, effective February 28, 2010, p. 44 (www.sec.gov/rules/final/2009/33-9089.pdf). Last accessed September 5, 2013.
iii. See Tim Leech and Lauren Leech, "Preventing the Next Wave of Unreliable Financial Information: Why U.S. Congress Should Amend Section 404 of the Sarbanes Oxley Act." *International Journal of Disclosure and Governance* advance online publication, 8 September 2011; doi: 10.1057/jdg.2011.18 http://riskoversightsolutions.com/wp-content/uploads/2011/10/PreventingTheNextWaveofUnreliableFinancialReportingWhyUSCongressShouldAmendSOX404LeechandLeech.pdf
iv. See COSO press release at http://www.coso.org/ermupdate.html
v. The two primary recognized risk frameworks are the 2009 ISO 31000 Risk Management standard and the 2004 COSO ERM framework.
vi. The most accepted risk management taxonomy is ISO Guide 73 Risk Management Vocabulary 2009.

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom

vii. Per ISO 3100 Risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the **risk source**; changing the **likelihood**; changing the **consequences**; sharing the risk with another party or parties (including contracts and risk financing); and retaining the risk by informed decision.
viii. See Leech, "The High Cost of ERM Herd Mentality," unpublished white paper, for more details on deficiencies of traditional ERM. http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk_Oversight-The_High_Cost_of_ERM_Herd_Mentality_March_2012_Final.pdf

Tim J. Leech, FCPA, CIA, CFE, CRMA is Managing Director Global Services at Risk Oversight Solutions Inc. He has over 25 years of experience in the board risk oversight, ERM, internal audit, and forensic accounting fields, including expert witness testimony in civil and criminal proceedings and global experience helping public and private sector organizations with ERM and internal audit transformation initiatives and the design, implementation and maintenance of integrated GRC/ERM frameworks. Leech has provided training for tens of thousands of public and private sector board members, senior executives, professional accountants, auditors and risk management specialists in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. He has received worldwide recognition as a pioneer, thought leader and trainer. His newest innovation, "Board & C-Suite Driven/Objective Centric ERM and Internal Audit", a new approach to ERM and internal audit, has been licensed by the IIA for global deployment in 2015.

Parveen Gupta is the chair and professor of accounting at the College of Business and Economics at Lehigh University in Bethlehem, Pennsylvania. He is a recognized expert in Sarbanes-Oxley, internal control, risk management, financial reporting quality, and corporate governance. He has published numerous research papers and monographs in these areas. He is the recipient of many awards in teaching and research. During 2006–2007, he served as an academic accounting fellow in the SEC Division of Corporation Finance, where he worked closely with the division's chief accountant and participated actively on Sarbanes-Oxley-related projects. He is a frequent speaker at academic and professional conferences both at a national and international level. He is often quoted in the media.

Downloaded by [Murdoch University Library] at 18:17 04 October 2017

© Copyright 2014 by Ethical Boardroom strictly reserved. No parts of this material may be reproduced in any form without the written permission of Ethical Boardroom