UPS AND DOWNS
Companies need to rethink their growth strategies

Building businesses for the long-term

Investors, particularly institutional investors, representing in excess of a billion future pensioners, are flexing their muscles and calling on companies around the globe to significantly change their approach to value creation.

Focussing ERM and internal audit on what really matters: long-term value creation and preservation

Tim J. Leech
Managing Director at Risk Oversight Solutions Inc

A letter dated 1 February 2016 from Larry Fink, CEO of BlackRock (the largest money manager in the world with more than $5.1trillion of assets under management) to thousands of CEOs of the biggest companies in the world is a good proxy for the movement.

In it he said "We are asking that every CEO lay out for shareholders each year a strategic framework for long-term value creation. Additionally, because boards have a critical role to play in strategic planning, we believe CEOs should explicitly affirm that their boards have reviewed these plans. BlackRock's corporate governance team, in their engagement with companies, will be looking for this framework and board review."[1]

Fink goes on to add a stern caution and then a caveat: "Those activists who focus on long-term value creation sometimes do offer better strategies than management. In those cases, BlackRock's corporate governance team will support activist plans. During the 2015 proxy season, in the 18 largest US proxy contests (as measured by market cap), BlackRock voted with activists 39 per cent of the time."

"We recognise that the culture of short-term results is not something that can be solved by CEOs and their boards alone. Investors, the media and public officials all have a role to play."[2]

The recent launch in February 2017 of the Investors Stewardship Group (ISG), representing more than $17trillion of assets, is expected to add fuel to this movement.[3] The release of the 2016 Principles of Corporate Governance by the Business Roundtable with CEO signatories from US investment companies with more than $7trillion in annual revenues laid a solid foundation for the formation of the ISG.[4]

The International Corporate Governance Network (ICGN), a global not-for-profit representing companies with assets under management totalling more than $26trillion, calls on investors to start by focussing their attention on the boards of investee companies: "The risk oversight process begins with the board. The unitary or supervisory board has an overarching responsibility for deciding the company's strategy and business model and understanding and agreeing on the level of risk that goes with it. The board has the task of overseeing management's implementation of strategic and operational risk management."[5]

On the long-term value preservation front, Institutional Shareholder Services (ISS), the leading proxy advisory firm, has laid out its position quite clearly. It says "

ISS will recommend voting 'against' or 'withhold' in director elections, even in uncontested elections, when the company has experienced certain extraordinary circumstances, including material failures of risk oversight. In 2012, ISS clarified that such failures of risk oversight will include bribery, large or serial fines or sanctions from regulatory bodies and significant adverse legal judgments or settlements."[6]

This article calls on boards and CEOs to demand something Larry Fink has not explicitly asked for to date – that senior management, internal auditors and ERM specialists radically change their risk management and internal audit methods and provide substantially more and better information to boards on the true state of retained risk, linked to top value creation and preservation objectives.

Broadly, the criticism is this:

Traditional approach to risk management – populate a risk register, update it once or twice a year and produce risk lists and heat maps for the board - is not up to the task As investors call for greater focus on long-term value creation and board oversight of that process, advocates, including Larry Fink, the Business Roundtable, ICGN and ISS, need to recognise that focussing on long-term value creation and, by extension, avoiding major erosion of entity value, requires a lot more than some changes to the annual strategic planning exercise and more rigorous board review of that plan.

A large percentage of the risk assessment work done during the strategic planning process in companies around the world today has not used generally accepted risk assessment methods, often relying on 'brain storming' and intuition, or been subjected to independent review by ERM specialists or internal audit. Based on annual risk oversight surveys,[7] assumptions made by the authors of the 2016 COSO Enterprise Risk Management (ERM) exposure draft and the author's 30 years of work in the ERM space globally, the vast majority of companies have interpreted calls to enhance enterprise risk management (ERM) to mean constructing a corporate 'risk register', developing lists of the top 10/20/30 risks and providing boards with nice colour 'risk heat maps'.The focus of these efforts has predominantly been on hazard avoidance, not long-term value creation objectives. Most importantly, in the majority of companies, it has not meant documenting the top value creation and value preservation objectives being considered and implemented; assigning responsibility for those objectives to specific senior managers; requiring those managers to demonstrate they have taken reasonable steps to identify and assess risks that threaten the achievement of those objectives; and providing reliable reports to the board on the true state of retained risk linked to the company's top value creation/preservation objectives.

Traditional ERM and internal audit – a bad case of paradigm paralysis and ill-equipped to support long-term value creation strategies A 2016 study produced by the AICPA and North Carolina State University[7] reported that only 30 per cent of the organisations surveyed have boards that 'mostly' or 'extensively' review the top risk exposures facing the organisation when the board discusses the organisation's strategic plan. Investors are not only demanding more details on the organisation's long-term value creation plans, they want more and better information on the risks that threaten the achievement of those plans and they want board review of those risks. In large organisations with revenues in excess of $1billion, 87 per cent of respondents want more information from senior executives on risks impacting core growth strategies (see Figure 1).

Demands for more information on risk

At the same time as heightened calls from investors for more and better board oversight of risks to key strategic value creation objectives, there is strong evidence that implementation of risk-centric approaches to ERM, which typically use risk registers as a foundation with annual/semi-annual updates, are stalled globally. They have not been embraced by the C-suite or boards as a useful tool to help the organisation create long-term value – see Figure 2.

Risk-centric ERM stalled

Coincident with the surveys disclosing major problems with traditional approaches to enterprise risk management (See Figure 3), stakeholders are signalling they want far more from internal auditors than the traditional 20-50 spot-in-time internal audits each year with internal auditor opinions on the effectiveness of 'internal controls' on a small fraction of the risk universe. A study done by the Institute of Internal Auditors released in 2016 is indicative of the new demands.[8]

Calls for change in internal audit focus

In that 2016 IIA report on stakeholder expectations one CEO identified what most needed to change: "We need to better define how we link internal audit objectives to the achievement of strategic objectives'"[9]

A majority of the senior managers and board members surveyed around the world want to see internal auditors shift from their traditional heavy focus on financial accounting controls and hazard areas, such as cybersecurity and business continuity, to one that includes providing management with assistance identifying and assessing risks to the company's most important strategic objectives – see Figure 4.

What's wrong with ERM/internal audit?

Unfortunately, both the ERM and internal audit communities have strong, even emotional attachment to traditional risk management and internal audit methods, methods that are increasingly demonstrating they are not equipped to help organisations with today's rapidly changing environments and demands. One only needs to recall the demise of companies, such as Kodak, Xerox, Blackberry and others to see what happens when a paradigm shifts but companies don't.

FIGURE 1: EXTENT THAT EXTERNAL PARTIES ARE APPLYING PRESSURE ON SENIOR EXECUTIVES TO PROVIDE MORE INFORMATION ABOUT RISKS AFFECTING THE ORGANISATION

	Full sample	Largest Organisations (Revenues >$1B)	Public companies	Financial services	Not-for-profit organisations
Extensively	11%	17%	18%	24%	5%
Mostly	26%	34%	30%	35%	22%
Somewhat	29%	36%	33%	23%	27%
Combined	66%	87%	81%	82%	54%

FIGURE 2: COMPLETE ERM IN PLACE: FULL SAMPLE

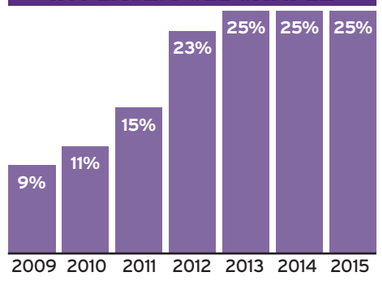


FIGURE 4: DO YOU BELIEVE INTERNAL AUDIT SHOULD BE MORE ACTIVE WITH ASSESSING STRATEGIC RISK?

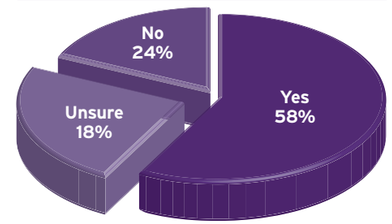
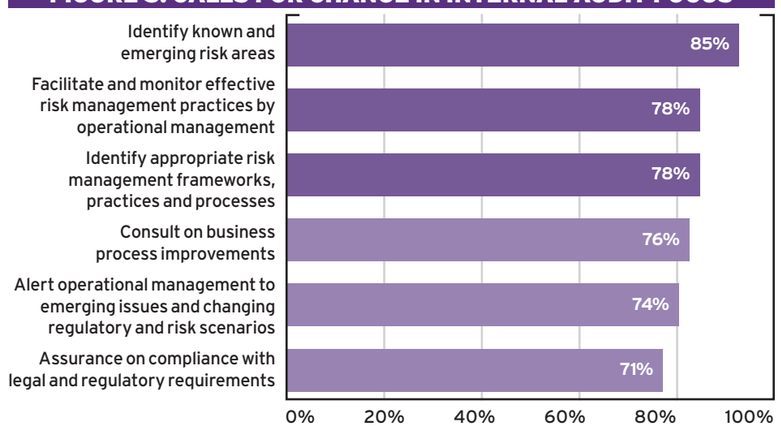


FIGURE 3: CALLS FOR CHANGE IN INTERNAL AUDIT FOCUS



» Readers who want more details on the 'paradigm paralysis' afflicting ERM specialists and internal audit should refer to the Summer 2016 *Ethical Boardroom* article *Paradigm paralysis in ERM and internal audit.*

What needs to change to increase focus on long-term value creation and preservation?

1 The process senior management uses to define and document the organisation's top current and proposed value creation and preservation objectives should be transparent and overseen by the company's board of directors. The company's top long-term value creation and preservation objectives, should be documented in an entity's objectives register.

2 Each objective that has been deemed important/dangerous enough to warrant the cost of formal risk assessment and board oversight included in the objectives register should be assigned an owner/sponsor. That person should be responsible for identifying and assessing risks to those objectives and reporting upwards to the board on the true state of residual risk, linked to those objectives.

3 The company's CEO or his/her designate should be assigned responsibility for providing the board with regular reports on the evolution of the company's top value-creation and preservation objectives and the current state of residual risk linked to those objectives.

4 Management personnel, particularly those that are owners/sponsors, need to be provided with sufficient training to prepare reliable risk assessments on the organisation's top value creation and preservation objectives.

5 Risk specialist groups, in companies that have them, should be assigned responsibility for helping the company build and maintain its objectives register; helping owners/sponsors assigned to those objectives complete risk assessments; and facilitating reporting upwards on residual/retained risk status linked to top objectives to the board of directors. Boards should hold ERM specialist groups responsible for providing regular reports on the reliability and maturity of the process used to report to them on the true state of residual risk, linked to the organisation's top value creation and preservation objectives.

6 Internal audit should be assigned formal responsibility for providing independent reports on the reliability of the company's enterprise risk management process and the consolidated report provided to the board of directors on the state of residual risk, linked to top value creation and preservation objectives.

Investors representing literally trillions of dollars of pension funds and billions of individual investors and pensioners are calling for major change. Companies and their boards will have to decide if they are willing to make the changes necessary

What are the top barriers to increasing the focus on long-term value creation and preservation?

Misaligned reward systems One only needs to scan the amount of work the Financial Stability Board has dedicated to reforming compensation practices following the 2008 financial crisis, post-mortems done on major governance failures, and recent examples, such as Wells Fargo, to realise that misaligned reward systems represent a top risk to the goal of long-term value creation and preservation.[10] The reward misalignment related to both the short-term focus objectives that were being remunerated by organisations at the core of the 2008 financial crisis, as well as how well senior management evaluated and reported to boards on the risks to those objectives. The AICPA/NCSU 2016 annual risk oversight survey provides insight into current compensation practices.[11] It is important to note that if the survey question shown in Figure 5 used to poll current remuneration practices linked to risk management was revised to ask about something more specific than 'risk management activities' –such as 'providing reliable reports on the true state of retained risk linked to top strategic objectives to the board' – the negative numbers you see below would be much higher.

Linkages between risk management and remuneration

It is important to note that I believe a key element of reward system evaluation has been missed by these post-crisis regulator post-mortems – the reward systems of Chief Audit Executives (CAEs) and Chief Risk Officers (CROs). All too often, CAEs are remunerated on whether they have achieved their annual internal audit plan reporting on whether they believe internal controls are 'effective' or 'ineffective' on a small percentage of the total risk universe. But there is often little or no coverage of top strategic value creation and preservation objectives (see Figure 5 below).

CROs are often hired and paid to create and maintain risk registers and provide lists of risks and risk heat maps for senior management and the board. If long-term value creation is to be the new focus, there needs to be a unified focus on developing the right long-term value creation and preservation objectives and assessing and managing the risks that threaten the achievement of those objectives. CROs should be measured on the amount of help they provide to senior managers in identifying long-term value creation and preservation objectives and assessing and managing risks to the most important of those objectives. CAEs should be measured on the quality of their reports on the process used to report to boards on top value creation and preservation objectives and the reliability of the information the board is receiving on the true state of risk linked to them.

Managers at all levels often lack the skills to identify and treat risks to top strategic objectives If boards are to receive reliable reports on the top value creation and preservation objectives, surveys indicate quite clearly that management at all levels will need substantially more training. This is necessary if they are to evolve from informal/ad hoc risk management methods to structured risk management capable of providing reliable reports on the status of risks to top value creation and preservation objectives. The 2016 AICPA/NCS survey of risk oversight practices disclosed a very telling fact – 63 per cent have not provided or only minimally provided training and guidance on risk management.[12]

Risk specialists often don't link risk assessment work done by management to top value creation objectives – a large percentage of ERM efforts today do not explicitly focus on assessing the risks to top value creation and preservation objectives. The majority of ERM efforts use risk registers, not objectives registers as the foundation for their efforts. Figure 6 from the 2016 AICPA/NCSU survey of risk oversight practices provides an indication of the extent organisations integrate strategic planning and work done to identify and assess the risks to the company's strategic plan.

FIGURE 5:TO WHAT EXTENT ARE RISK MANAGEMENT ACTIVITIES AN EXPLICIT COMPONENT IN DETERMINING MANAGEMENT PERFORMANCE COMPENSATION?

	Full sample	Largest organisations (revenues >$1B)	Public companies	Financial services	Not-for-profit organisations
Not at all	29%	10%	12%	19%	46%
Minimally	26%	28%	27%	21%	18%
Combined	55%	38%	39%	40%	64%

FIGURE 6: EXTENT TO WHICH TOP RISK EXPOSURES ARE FORMALLY DISCUSSED BY THE BOARD OF DIRECTORS WHEN THEY DISCUSS THE ORGANISATION'S STRATEGIC PLAN

	Full Sample	Largest Organisations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organisations
"Extensively"	9%	18%	18%	15%	7%
"Mostly"	21%	28%	32%	31%	17%
Combined	30%	46%	50%	46%	24%

How many are linking risk management and the strategic plan?

The majority of internal auditors today have not received much training on formal risk assessment methods The focus of the majority of internal audit departments in the world today has been on doing spot-in-time audits of topics drawn from what is commonly called internal audit's 'audit universe'. They opine on the effectiveness of 'internal controls' on a small percentage of the total risk universe, not on whether the true state of residual risk linked to top value creation and preservation objectives is being reported upwards to the board.

Few audit universes have, at least to date, included their organisation's top value creation objectives. Most don't include specific end result objectives at all, focussing instead on processes, business units, topics, or audit themes. The harsh truth is that the majority of internal auditors today have received very little training on how to complete formal risk assessments on value creation and preservation objectives that use the type of methods promoted by the world's global risk management standard, ISO 31000, or even the more risk-centric risk assessment methods outlined in the 2016 COSO ERM exposure draft. A major global retraining effort will be required if internal auditors are to help their organisations reliably assess and report to boards on the retained risk status linked to top value creation and preservation objectives.

Majority of boards in the world have not been demanding strategic plans be accompanied by high-quality risk assessments Last, but certainly not least, is the fundamental truth that board members around the world have received little or no training on risk oversight. This is necessary if they are to help them assess whether formal risk assessments they receive, if any, linked to the company's strategic plans are likely reliable; and often have not demanded that management's strategic plans be accompanied by formal structured risk assessments that clearly show the company's residual risk status position. This isn't particularly surprising as a large percentage of board members are, or were previously, senior executives, executives that often used intuitive and informal risk assessment methods in running the business and they didn't use/require formal risk assessment methods when developing their strategic plans. It is important to note that boards globally should be excused on this issue as the professional risk management and internal audit communities, including the current COSO project team to update the 2004 COSO ERM guidance scheduled for release in mid-2017 and the ISO 31000 technical committee charged with updating the 2009 global risk management standard, are in a state of confusion and division on the best way forward for ERM. Both COSO and ISO are vacillating over whether to advocate 'objective-centric ERM' that uses objectives registers as a foundation for all risk management efforts with a heavy focus on strategic value creation objectives, or stick with what has been largely risk-centric/risk register/hazard-focussed approaches to ERM.[13]

Focus on what really matters – long-term value creation and preservation

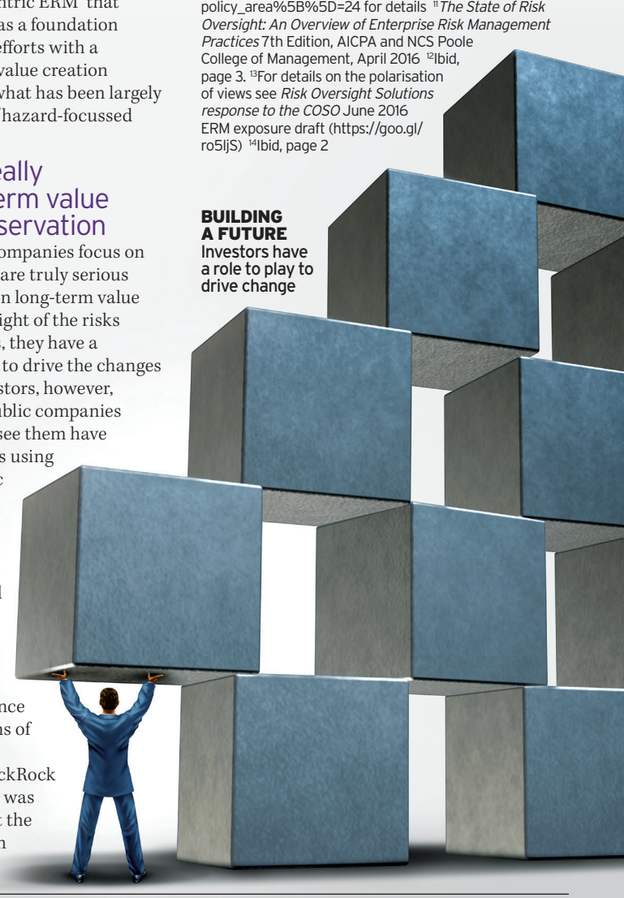
If investors demanding companies focus on long-term value creation are truly serious about putting the focus on long-term value creation and board oversight of the risks linked to those strategies, they have a tremendous opportunity to drive the changes needed. Those same investors, however, need to recognise that public companies and the boards that oversee them have been conducting business using largely the same strategic planning, internal audit and ERM assurance methods that have been used for decades. If the changes being demanded by investors are to occur on a wide scale, radical changes will have to be made to planning, risk management and assurance methods in use in millions of public companies today.

Larry Fink, CEO of BlackRock in his 2016 letter to CEOs was correct when he said that the lack of focus on long-term value creation and short-termism is a problem that will require a concerted effort from multiple parties. To quote Fink: "We recognise that the culture of short-term results is not something that can be solved by CEOs and their boards alone. Investors, the media and public officials all have a role to play."[14]

ERM specialists and internal auditors need to be added to Mr Fink's list.

Investors representing literally trillions of dollars of pension funds and billions of individual investors and pensioners are calling for major change. Companies and their boards will have to decide if they are willing to make the changes necessary to truly make long-term value creation and preservation their focus and reality.

[1]Text of Larry Fink, CEO of BlackRock's 2016 Corporate Governance Letter to CEOs, February 1, 2016, page 1 [2]Ibid, page 2 [3]https://www.isgframework.org/ [4]*Principles of Corporate Governance 2016*, Business Roundtable [5]*ICGN Guidance on Corporate Risk Oversight*, Third Edition, 2015 [6]Martin Lipton, *Risk Management and the Board of Director*, Harvard Law School Forum on Governance and Financial Regulations, Feb 15, 2017. [7]*The State of Risk Oversight: An Overview of Enterprise Risk Management Practices* 7th Edition, AICPA and NCS Poole College of Management, April 2016 [8]*Relationships and Risks: Insights from Stakeholders in North America*, IIA Research Foundation, A CBOK Stakeholder Report, 2016, page 4. [9]Ibid, p. 5. [10]See http://www.fsb.org/publications/?policy_area%5B%5D=24 for details [11]*The State of Risk Oversight: An Overview of Enterprise Risk Management Practices* 7th Edition, AICPA and NCS Poole College of Management, April 2016 [12]Ibid, page 3. [13]For details on the polarisation of views see *Risk Oversight Solutions response to the COSO* June 2016 ERM exposure draft (https://goo.gl/ro5ljS) [14]Ibid, page 2



BUILDING A FUTURE
Investors have a role to play to drive change