Board oversight of strategy & risk

Directors need better information to meet rapidly escalating expectations

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

A February 1, 2016 letter from Larry Fink, CEO of BlackRock the largest money manager in the world with over $5.1trillion assets under management, to CEOs of the biggest companies in the world is a good indicator of a growing institutional investor sentiment.

He wrote:"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]

The International Corporate Governance Network (ICGN), a global not-for-profit that represents 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," it says. "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."[2]

On the long-term value preservation front, Institutional Shareholder Services (ISS), the leading proxy advisory firm, has also laid out its position quite clearly: "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." [3]

The most powerful institutional investors in the world are signalling quite clearly that they want boards to better oversee strategy and value creation; as well as the effectiveness of the company's risk management processes linked to value preservation.

Two main findings from the American Institute of Certified Public Accountants (AICPA)/North Carolina State 10th annual 2019 risk oversight survey provide insight on the limited progress made to date in integrating strategic planning and enterprise risk management (ERM):[4]

- **External stakeholders expect greater senior executive involvement in risk management.** External parties (59 per cent) are putting pressure on senior executives for more extensive information about risks, and 65 per cent of boards are calling for 'somewhat' to 'extensively' increased management involvement in risk oversight. Strong risk management practices are becoming an expected best practice. These pressures are increasing for large organisations and public companies, particularly
- **Few organisations perceive their approaches to risk management as providing important strategic value.** Less than 20 per cent of organisations view their risk management process as providing important strategic advantage. Only 26 per cent of the organisations report that their board substantively review top risk exposures in a formal manner when they discuss the organisation's strategic plan (See Table, opposite)

The harsh reality is that strategic planning, the annual/semi-annual ERM risk register update processes, and internal audit in the majority of companies around the world are largely standalone silos with very limited real integration.

Since the globally accepted definition of the word 'risk' is 'affect of uncertainty on objectives', why are ERM frameworks, internal audit and strategic planning frameworks not better integrated?[5]

Really big reason #1

Heavy focus on risks and internal controls, not objectives, impedes integration. The majority of ERM frameworks in the

world today are risk centric, focussed on building and maintaining risk registers; not objective centric, focussed on assessing the certainty that top value creation and preservation objectives will be achieved. The majority of internal audit work done today, largely because of its external audit roots, is control centric, compliance centric, and process centric; not objective centric.

The diagram below shows the 10 main assurance methods in use today. For those that want to better understand the evolution of thinking and methods, a longer explanation of the 10 main assurance methods is available.[6]

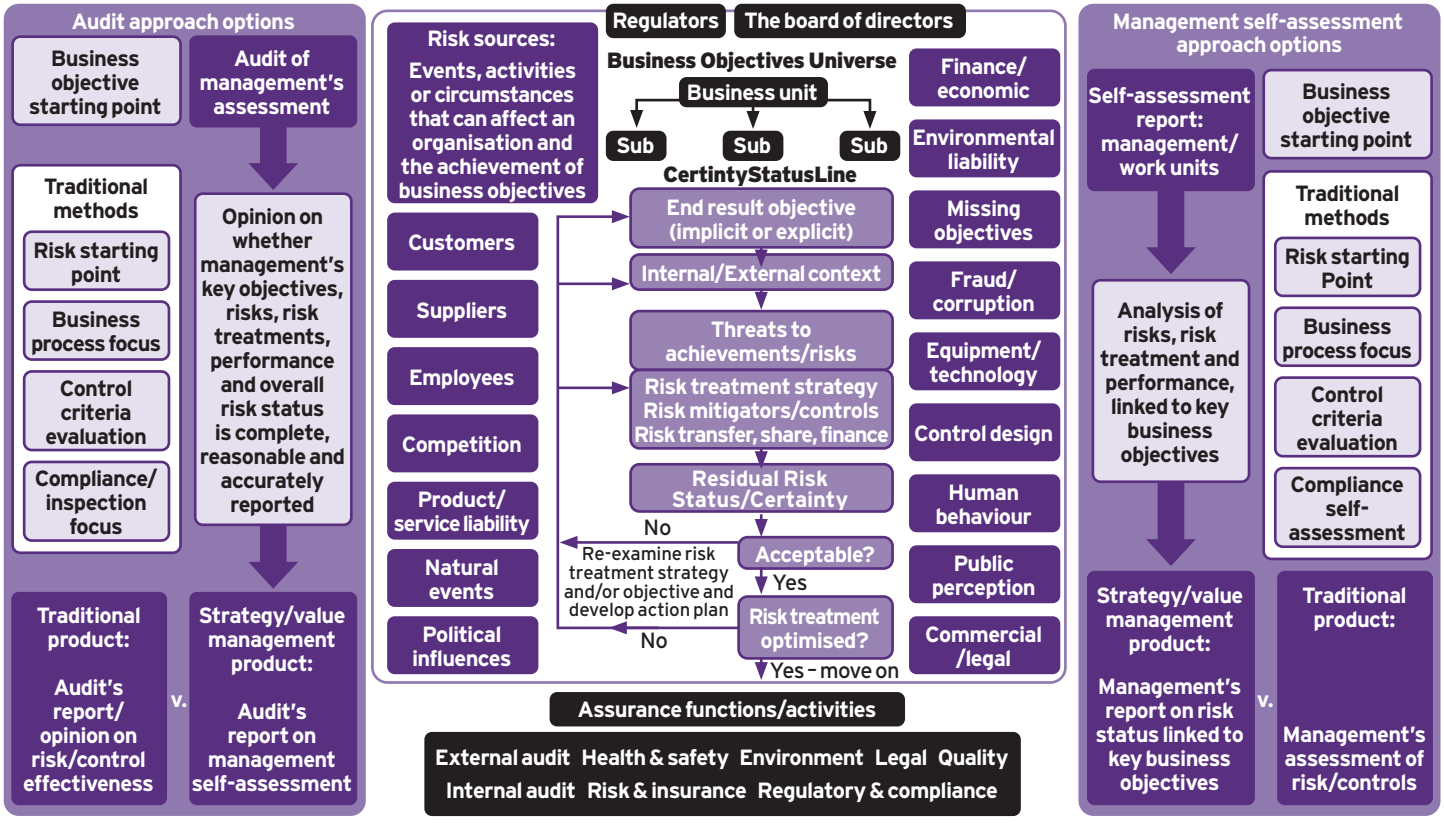
The largest percentage of internal audit work done in the world today is done from the left side of the diagram. Internal auditors, most often using some combination of what is labelled traditional methods in the diagram, provide opinions on whether internal controls are effective. Internal auditors receive little, or sometimes no training at all on the full range of risk treatment methods in spite of often claiming to do 'risk-based internal audits' (i.e. risk transfer, risk share, risk finance, risk avoid, risk mitigate and risk accept). The focus is on evaluating internal controls, linked mainly to traditional value preservation objectives, such as reliable financial statements, data security, continuity of operations and asset safeguarding.

Following the 2008 global financial crisis, public companies, particularly companies in the financial sector, were pressured by regulators to create ERM frameworks. The majority of ERM frameworks in the world today are risk centric. The focus is on building risk registers and showing boards of directors the company's 'risk profile' and risk maps. Direct links to strategic objectives and current performance are rarely made. Few risk functions or internal audit departments analyse the composite effect of multiple risks that effect achievement of top objectives. The current risk oversight survey done by North Carolina State and the AICPA, now in its tenth year, still assumes most organisations are using risk centric/risk register-based ERM frameworks, not objective-centric ERM. »

AICPA/NORTH CAROLINA STATE 10TH ANNUAL RISK OVERSIGHT SURVEY

Percentage of respondents saying 'mostly' to 'extensively' Extent that	Full sample	Largest organisations (Revenues >$1B)	Public companies	Financial services	Not-for-profit organisations
Existing risk exposures are considered when evaluating possible new strategic initiatives	40%	39%	42%	46%	35%
Organisation has articulated its appetite for or tolerance of risks in the context of strategic planning	28%	26%	28%	40%	20%
Risk exposures are considered when making capital allocations to functional units	30%	32%	29%	38%	21%

STRATEGY & VALUE OVERSIGHT ERM/AUDIT OVERVIEW



The majority of ERM frameworks in the world today are risk centric', focussed on building and maintaining risk registers; not objective centric, focussed on assessing the certainty that top value creation and preservation objectives will be achieved

Really big reason #2:

The three lines of defence model works against integration of strategy and ERM. Following the 2008 global financial crisis, there was enormous regulatory pressure globally on financial institutions to create risk management departments.

Risk functions, not surprisingly given regulatory focus and expectations, focussed on identifying risks and creating risk registers, risk maps, risk profiles and risk appetite statements. Internal auditors continued to focus on providing subjective opinions on internal control effectiveness, primarily linked to traditional value preservation objectives. The assessment methods and terminology used by the two groups, with the full endorsement of regulators, were quite different.

As a result of growing confusion, the IIA in Europe started to popularise what has become widely known as the three lines of defence (3LoD) model to try to explain the role of risk groups and role of internal audit. A visual of the original European Confederation of Institutes of Internal Auditing (ECIIA)/Federation of European Risk Management Associations (FERMA) framework is shown in The Three Lines of Defence Model Table below.

Financial regulators around the globe quickly seized on the IIA framework and popularised it by legislating/regulating the use of the framework.[7] The IIA accelerated the adoption of the 3LoD model with the release of a guidance paper in 2013. This 2013 development had the effect of further emphasising that risk functions (part of the 'second line of defence') should focus their attention on risks; and internal audit (the 3LoD) was to report on the first line of defence's use of management controls and internal control measures. How an organisation creates value and exploits opportunities is not discussed. The governing body/board/audit committee and senior management are depicted and described in the framework as process oversights, not active participants/'lines.

In June of 2019, the IIA announced its intention to update the 2013 3LoD guidance. To kick-off the process, the IIA published an exposure draft for comment.[8] The comment period closed on 19 September 2019. The authors made it very clear that, in spite of strong criticism from multiple expert sources, significant changes should not be expected.

The model has attracted criticism over the years, highlighting its limitations in addressing the complexity of modern organisations. In addition, the familiar graphic, developed and promoted to illustrate the model, is seen as reinforcing these limitations. A number of variations to the model have been proposed, but none has gained significant adoption.

Rather than needing a complete overhaul, the current model has strengths that can be extended and enhanced to serve organisational needs even more successfully.

My top criticisms of 3LoD and recommendations made to the IIA working group in September 2019 to increase integration of strategic planning, ERM, and internal audit follow:[9]

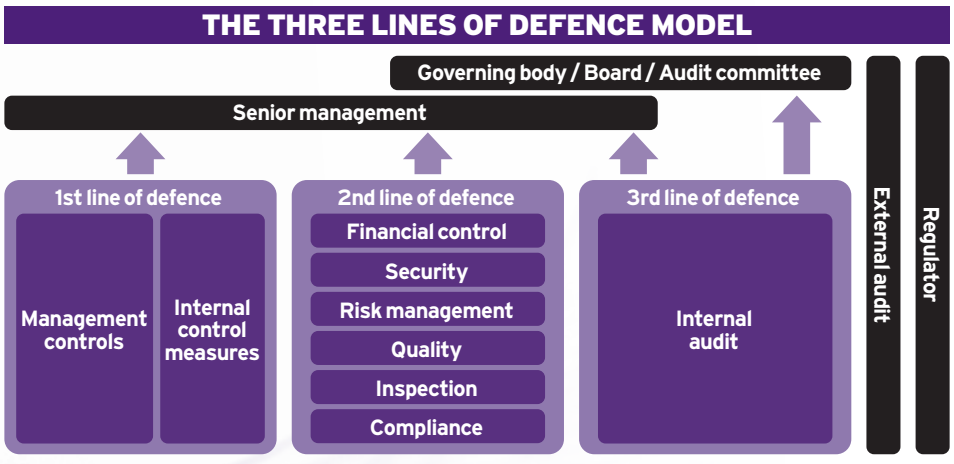
Use of the word 'defence': While I like the notion of 'lines' in the name of the framework, I am strongly against retaining the word 'defence'. It implies that the primary purpose of all the lines, particularly risk specialists and internal audit, is defence. This marginalises the role of all the lines and implies the framework has no role in value creation or strategic planning. This is not consistent with the direction of COSO ERM 2017 for risk management or what Richard Chambers, IIA CEO/president sees for the IA profession. A LinkedIn post where I comment on this issue is available.10 The June ED mentions the issues raised by the word 'defence' but does not address the huge damaging impact of the word 'defence'.

Recommendation: Replace the word 'defence' with 'accountability' or 'assurance'.

Role of management – the first line: Page eight of the ED describes the role envisioned for management. It does not indicate that management is/should be responsible for learning how to self-assess the acceptability of the current state of risk, linked to top value creation and preservation objectives. It also does not state that the first line should be responsible for regularly reporting on the state of risk-linked top objectives upwards to the CEO and board. This suggests to me that the working group has accepted/endorsed a weak first line governance model and described the roles of all other lines assuming a weak first line that is not responsible for assessing and reporting on the state of risk linked to top objectives. This is very akin to endorsing manufacturing operations decades back that relied on the inspection department to identify and correct flaws from production. The framework should distinguish between weak first line models and strong first line models and provide an overview of what the roles of all the lines are in a weak first line model, and the quite different role of all the lines in a strong first line model. More comments on the weakness are available on my LinkedIn post.[11]

Recommendation: Provide readers with an overview of the roles of all the lines, assuming a strong first line model where management is the primary risk assessor/reporter linked to top value creation and value preservation objectives. The current draft provides the role descriptions of the lines for a weak first line model. The guidance could describe the differing roles of the lines to illustrate the differences between a strong first line model and a weak first line model.

Assurance method(s) being used: There are five primary assurance methods organisations use to get assurance. These



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, Article 41*

DRAWING THE LINES
A strong first line with five lines of accountability is the best model

assurance methods are broadly defined as objective centric, risk centric, process centric, control centric, and compliance centric. These methods can be done by the second and third lines directly or performed by management and quality assured by the second and third lines. These different assurance methods are described in an overview.[12] There are significant differences between the different methods.

When a company uses an objective-centric assurance method applied to top value creation and value preservation methods, it significantly elevates the role and stature of the second and third lines and helps governing bodies meet escalating expectations that boards oversee the company's strategic planning process. The ED makes no reference to the technical assurance method(s) being used by an organisation, in spite of the fact that roles of all the lines are significantly impacted. For example, in most organisations that use a risk-centric/risk register-based ERM framework, few internal audit departments today provide much formal assurance to the board that the information it is receiving from the second line/risk group is reliable.

Recommendation: Provide an overview of this issue in the guidance, which describes the impact on the lines when different combinations of assurance methods are used.

Number of 'lines': The ED is about three lines of defence but introduces a fourth line – governing body. It isn't clear if the current three lines in the IIA three lines of defence model is going to become four lines in the final guidance document. The ED does not envision the CEO and C-Suite as a line in spite of the fact that, in my experience, the role of the CEO is absolutely key to the long-term success of an assurance framework.

Recommendation: Endorse the five-line approach that many have advocated since the IIA 3LoD was introduced that elevates the roles of the CEO and C-Suite and the board of directors.

It is ironic that the IIA, when it popularised 3LoD to try to define the roles of overlapping assurance groups, has consciously or unconsciously popularised and reinforced what I regularly call 'a weak first line risk governance framework'. Even more ironically, regulators around the world have picked up on the IIA 3LoD model and further reinforced and encouraged the use of a weak first line model that depends heavily on the second and third lines (risk and other second line groups and internal audit) to identify and report areas of major weakness and excessive risk emerging from the first line. In simple terms, the IIA and regulators have endorsed and elevated a framework that is much like the auto production lines of the 60s and 70s in North America; an approach that relied heavily on inspection departments at the end of the line to identify and correct production flaws from the main production line.

The IIA is now considering the feedback that it has received to date on the June 2019 3LoD exposure draft. I am not optimistic the IIA will make major changes to this badly flawed model.

Really big reason #3:

CEOs and boards don't think risk groups or internal audit have much to offer in the area of strategic planning.

As a direct result of really big reasons #2 and #3 described in this article, CEOs and boards, quite naturally and rationally, see risk functions (one of the second line of defence), and internal audit (third line of defence) as being primarily about defence, with little to contribute to the strategy development and implementation process. Risk oversight surveys done in the US by the AICPA and North Carolina State for the past 10 years, and in Canada most recently by Conference Board and CPA Institute continue to confirm this fact.

Risk groups focus on building and maintaining risk lists with an emphasis on value preservation. Internal audit focusses on giving opinions on internal control effectiveness with a heavy focus on value preservation objectives. In the majority of organisations, neither group starts the process by agreeing a set of the organisation's top value creation and value preservation objectives, including top strategic objectives. Management (the first line) is rarely responsible for learning how to assess and report on the state of risk/certainty linked to top strategic value creation or the more traditional value preservation objectives. Few chief risk officers or chief audit executives or their staff are asked to participate directly in the strategic planning process or oversight of its implementation.

Going forward

If I am correct that the IIA has little appetite for radical change and quite likes internal audit's regulatory endorsed role as 'defence specialists' and that the associations that represent the risk profession (e.g. IRM, GARP, PRIMIA, RMA) are largely silent and content with their role as second line 'defence specialists', the onus will fall on CEOs/senior management (what I and many others label 'the fourth line') and boards of directors, (what I and many others label 'the fifth line') to demand change.[13] The fourth and fifth lines responsible for oversight of strategic planning, ERM and IA must demand that the companies they oversee transition from the seriously flawed 3LoD model, a model focussed heavily on value preservation that depends heavily on inspection and rework identified by the second and third lines, in favour of an objective-centric/strong-first-line/five-line accountability model with active roles for senior management and the board.

Boards, and the associations that represent them, also need to clearly signal to the IIA and regulators around the world that at least some boards of directors want major changes in the deliverables from risk groups and internal audit to better meet what boards, society and powerful institutional investors need in today's fast-changing, disruptive world.

Footnotes will be run in full online.