Are we using weak first line risk governance?

The single most important question boards and CEOs should be asking internal auditors and risk officers

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

There is growing consensus around the globe that boards and CEOs are responsible for overseeing the 'effectiveness' of risk governance in organisations they oversee. Regulators, powerful institutional investors and credit rating agencies expect it. Even the courts and regulators are increasingly holding directors to account when massive risk oversight failures occur during their watch.

Unfortunately, there isn't much practical guidance available to CEOs or directors that defines how to discharge these emerging risk oversight expectations in real life. The dominant risk governance framework, defining roles and responsibilities of boards, CEOs, management, chief risk officers (CROs) and chief internal auditors ((CAEs), to have emerged is one developed by the Institute of Internal Auditors (IIA), widely known as 'three lines of defence' (3LoD). Regulators around the world, particularly in the financial sector, seized on 3LoD when it was released in 2013, and many have legislated its use. Consultants have helped hundreds of thousands of companies implement it. Hundreds of thousands of public companies have made representations in their annual reports and/or to regulators that they use the IIA's 3LoD framework to guide their risk governance efforts.

The big news this fall is 3LoD was updated in July of 2020 with a new IIA guide – *IIA's Three Lines Model*. Although the IIA has downplayed the significance of changes made, this new risk governance framework should cause all board directors to ask CEOs, CROs and CAEs a simple question:

Are we using a weak first line risk management model with a focus on assessing/managing risks, or a strong first line risk management model focussed on assessing/managing the risk/certainty of achieving our top value creation and preservation objectives?

This article provides a quick overview of the origins of the 2013 IIA 3LoD model; describes its major weaknesses; introduces the new 2020 three lines model; and describes core elements and major benefits that flow from implementing objective-centric/strong first line risk governance.

Origins of the 2013 IIA three lines of defence model

Following the 2008 global financial crisis, commissions were convened in countries around the world to try to identify what went wrong with the risk governance frameworks in place in financial institutions.

One of most comprehensive and in-depth evaluations of risk management practices was undertaken by the highly influential Senior Supervisors Group (SSG). SSG is a forum composed of financial regulators from Canada, France, Germany, Japan, Switzerland, the UK and the US. The SSG published two reports examining how weaknesses in risk management and internal controls contributed to industry distress during the financial crisis. On 21 October 2009, in a transmittal letter accompanying the second report, the SSG highlighted areas of weakness that required further work by financial firms[1]:

- The failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm
- Compensation programmes that conflicted with the control objectives of the firm
- Inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement
- Institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel

Findings of this SSG forum, and scores like it around the world, resulted in regulators legislating that companies create and fund risk management departments and risk management frameworks. The mandate was to respond to the failings identified by the SSG; and address the growing expectation that boards need to better oversee the effectiveness of risk management processes.

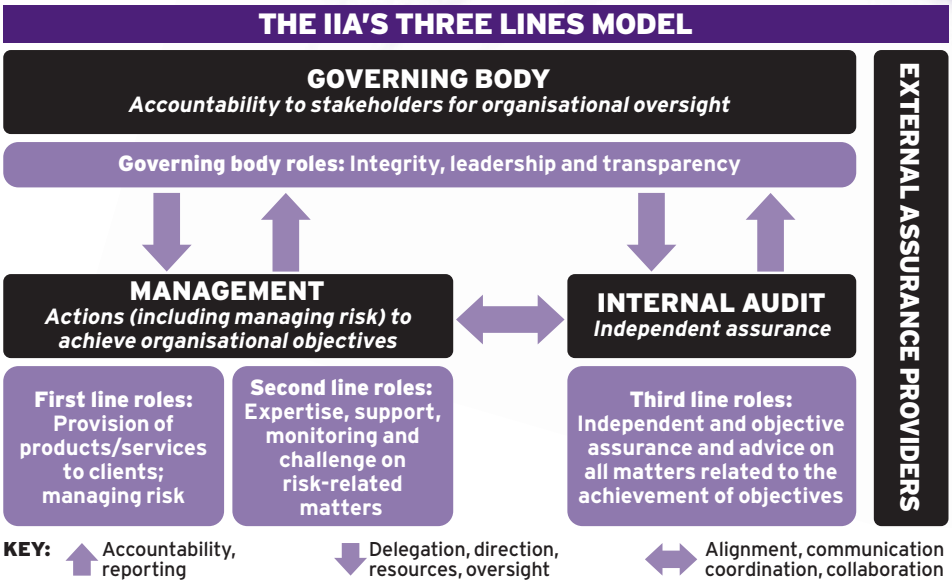
In practice, the new risk departments responded by building and populating what is widely known as 'risk registers'. In many companies, new CRO positions were created to lead these efforts. The newly populated risk registers were used to present 'top risks' to boards, often with the aid of 'risk heat maps' that showed top risks, often with the very popular traffic light red/amber/green

colours assigned. Internal audit departments were encouraged by the IIA to 'chase the risks' and 'audit at the speed of risk'.

Regulators had demanded risks be better managed. New processes were created and designed to demonstrate to regulators that risks were being managed. Unfortunately, little attention was paid to assessing and reporting on the risk/certainty of achieving the top strategic, value-creation and preservation objectives. This is in spite of the generally accepted definition of risk as 'the effect of uncertainty on objectives', and the fact that a large percentage of major governance failures over the past two decades have been linked to value creation objectives and CEO/board-endorsed strategic plans.[2]

What these developments resulted in was growing confusion about the roles and boundaries of the new risk management functions and existing internal audit departments. In 2012, Article 41 of a paper titled *Guidance on the 8th Company Law Directive*, issued by the Institute of Internal Auditors, proposed the three lines of defence framework, using the diagram below. That diagram formed the foundation element of a 2013 IIA global guidance paper titled *The Three Lines of Defence in Effective Risk Management and Control*.

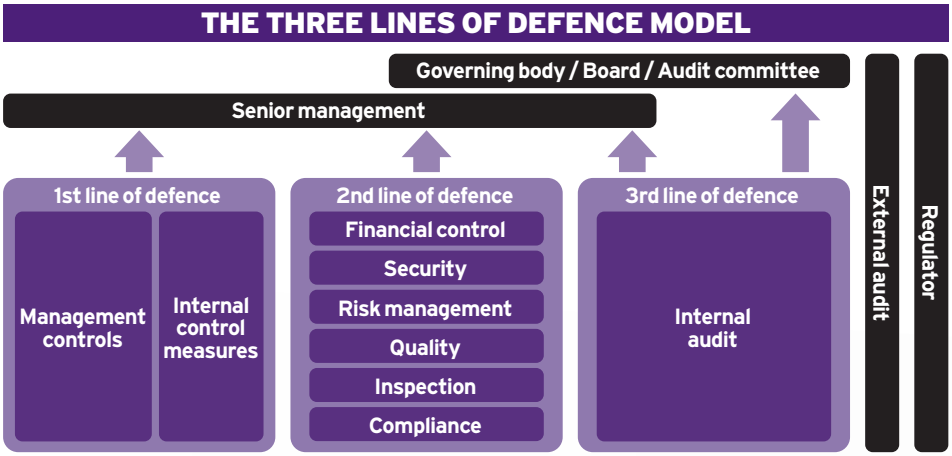
Following the release of the IIA three lines of defence in 2013, regulators all over the globe began to demand regulated companies in the financial services sector and others adopt it.



Weaknesses of the 2013 IIA three lines of defence

A chapter in Wiley's Governance Handbook titled *Three Lines of Defence versus Five Lines of Assurance: Elevating the Role of the Board and CEO in Risk Governance* describes key weaknesses in the 2013 IIA 3LoD framework.[3]

At a summary level, the two most significant deficiencies in 2013 three lines of defence are the heavy focus on managing risks, not managing certainty/risk top objectives will be achieved; and that management, the first line that 'own and manage risks', is not responsible for formally assessing and reporting upwards on the risk/certainty objectives will be achieved.



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

The 2020 update: the new IIA three lines model

In 2018, the IIA announced plans to update the 2013 *Three Lines of Defence* guidance. Major changes were not planned or expected as the IIA stated that it believed the framework was generally working well. In mid-2019, the IIA released a *Three Lines of Defence Exposure Document* and invited comments. The changes to the 2013 3LoD guidance being considered by the IIA were minor. The implicit assumption in 3LoD that management/the first line was not expected to assess and report on risk/certainty of achieving objectives remained. The notion that the primary focus should be on individual risks, not certainty/risk of achieving top value creation and preservation objectives, remained. Although the IIA does not share comments received, there were many comment letters, including one from this author, calling for major, not minor/incremental, changes.

In July 2020, the IIA released the final updated guidance. The name of the framework was changed from IIA's three lines of defence to the IIA's three lines model. The primary visual is shown above: »

The three 'lines' are distinguished at a high level in the IIA paper as:

- Functions that own and manage risks
- Functions that oversee risks
- Functions that provide independent assurance

Later in the paper this is further defined as:

- Risk owners/managers
- Risk control and compliance
- Risk assurance

The first line's responsibilities are summarised on page three as 'operational management identifies, assesses, controls, and mitigates risk'. It isn't clear why, but the paper does not see the first line formally reporting upwards on risk status.

The second line includes staff functions that are involved in some way with what management does on an ongoing basis. The second line's primary purpose is summarised on page two as 'management establishes these functions to ensure that the first line of defence is properly designed, in place, and operating as intended'.

The role of the third line of defence, internal audit, is defined on page five as follows: 'Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defence achieve risk management and control objectives.'

The word DEFENCE is gone. The underlying theme of the new guidance is on achieving 'organisational objectives', including value creation and value preservation objectives. The first line is to focus on managing risk to achieve organisational objectives. The second line is to provide 'expertise, support, monitoring and challenge on risk-related matters'. The third line is to provide independent and objective assurance on 'all matters related to the achievement of objectives'. I outlined my major concern with the new framework in a LinkedIn blog post and an email to the IIA global chair and president/CEO.

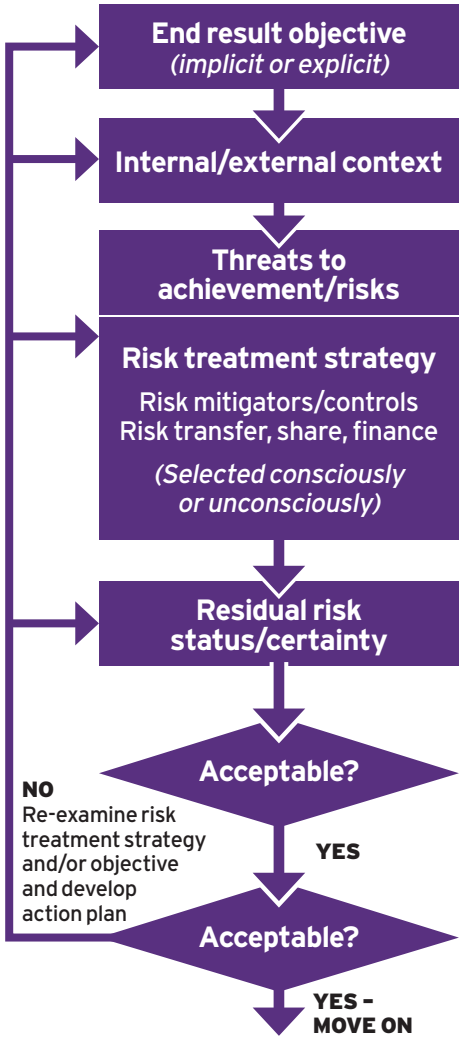
"If I was asked, my only serious concern is one word in the sentence used to describe first line's role – 'Maintains a continuous dialogue with the governing body, and reports on: planned, actual, and expected outcomes linked to the objectives of the organisation; and risk.' I would have recommended replacing the word 'risk' in that sentence with 'risk/certainty of achieving objectives'. This change ripples through to roles of second/third lines. Just too big a leap, I guess."

In an email on 6 October 2020, this author asked Jenitha John, the chair of the IIA 3LoD update working group and IIA's 2020 global chair to clarify whether the new IIA guidance means the first line should report on certainty/risk of achieving top objectives; or did they mean the first and second lines should continue the widespread practice of maintaining risk registers, reporting lists of top risks, and providing risk heat map reports to CEOs and boards. No response.

How do you know if a company is using a weak first line risk management model? You are using a weak first line risk management model at your organisation if:

- Senior management has not clearly defined and communicated the organisation's top value creation and value preservation objectives
- Management receives little or no training how to formally assess/report on certainty/risk of achieving top strategy/value creation/preservation objectives
- Management is not expected to report on certainty/risk status linked to top value creation and preservation objectives to the CEO and the board
- The board rarely receive reports from management on certainty/risk status linked to top value creation/preservation objectives, risk appetite and corrective plans when current risk/certainty status is seen as outside of the organisation's risk appetite

If you answered 'TRUE' to these questions for your organisation, you are have a lot of company. The majority of organisations in the world today are using a weak first line/risk-centric risk management model that relies heavily on second and third lines compensating for deficiencies of a weak first line risk management model.



Statement of an end result objective
e.g. customer service, product quality, cost control, revenue maximisation, regulatory compliance, fraud prevention, safety, reliable business information and others

External and internal environment
The organisation seeks to achieve its objectives

Threats to achievement/risks
These are real or possible situations that create uncertainty regarding achievement of the objective

Risk treatments Manage uncertainty that the objective will be achieved by mitigating, transferring, financing, sharing or accepting risk

Residual risk/certainty status
Information helps decision-makers assess the acceptability of the retained risk position and the level of **certainty** that the objective will be achieved. (Status data includes performance data, potential impact(s) of not achieving the objective, impediments and any concerns regarding risk treatments in place)

Is the **residual risk status** acceptable to the work unit? Management? The board? Other key stakeholders? (i.e. managed within risk appetite/tolerance)

Is this the lowest cost of combination of risk treatments given our risk appetite/tolerance?

FIVE CHANGES TO YOUR RISK MANAGEMENT FRAMEWORK

STEP 1
Populate 'objectives register' with top value creation and value preservation objectives

STEP 2
Assign objective owner/sponsors and identify risk assessment rigour (RAR) and independent assurance level (IAL) targets

STEP 3
Confirm decisions made in steps 1&2 on objectives register, risk assessment rigour and independent assurance levels with the board

STEP 4
Owner/sponsors complete CertaintyStatusline™ and internal audit/other assurance groups complete independent assurance work

STEP 5
Consolidated report including 'composite residual risk ratings' prepared for senior management and the board

1 2 3 4 5

©2017 Risk Oversight Solutions Inc.

What does an objective-centric strong first line risk management framework look like?

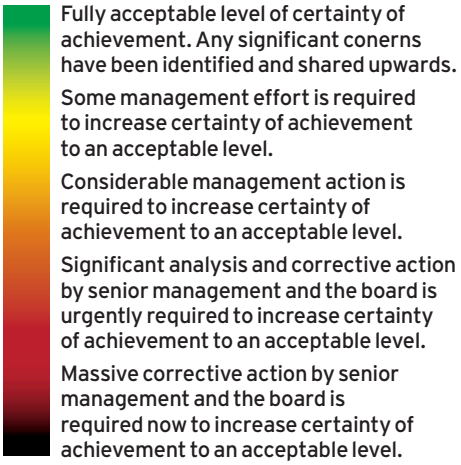
Moving from traditional, weak first line risk-centric risk management and internal audit to strong first line/objective-centric risk management is simple, but the amount of change required to the roles of all the 'lines' is huge. Most importantly, someone, be they internal or external, must champion and successfully sell the business case for change to senior management and the board.

Once an organisation buys the business case for change, the diagram left (Five Changes to your Risk Management Framework) captures what's required in five simple steps. The most important step is senior management with board oversight agreeing what the organisation's top strategic/value creation and preservation objectives are important enough to warrant formal, as opposed to informal, risk management/certainty assessment processes.

The core building block of the system starts, not surprisingly, with what is, ideally, a clear end result objective, using the simple flow diagram above.

'OBJECTIVE CERTAINTY' RATINGS

EXAMPLE CORE OBJECTIVES	OWNER	CERTAINTY
Achieve eight per cent return on private equity investments in excess of the sector	Mary Brown	
Increase customer retention by 15 per cent year over year	Chuck Smith	
Increase customer satisfaction ratings from 3.2/5.0 to 4.0/5.0 by year end 2020	Mary Brown	
Reduce lost time due to accidents by 30 per cent year over year	Paul Stevens	



Senior management and the board receive concise reports on the company's top value creation and preservation objectives with supporting detail with simple to understand 'objective certainty' ratings. Green ratings do not mean there are no significant residual risks/certainty. Significant concerns/ uncertainties have been communicated upwards (See chart, above).

Top benefits of objective-centric strong first line risk & certainty management

The benefits are many and persuasive. They include:

1 The focus is on an organisation's top value creation and value preservation objectives. Efforts of all lines, including senior management and the board, is integrated and focussed on increasing/managing certainty that objectives will be achieved while operating with a level of residual risk/ certainty acceptable to the CEO and board.

2 The work of all lines is integrated and rationalised using the simple step of agreeing the value creation and preservation objectives that are key to long-term success, and defining the roles all lines and the governing body will play managing risk/ certainty that those objectives will be achieved. This reduces the massive 'assurance burden' imposed on the first line when second and third line functions use unintegrated methods and terminology in their work.

3 The roles of the lines is driven by a logical requirement that the people that have primary responsibility to achieve key objectives are also responsible for assessing/ reporting upwards to the CEO and board on the current residual risk/certainty of achieving those objectives. Second line groups help the first line do that and provide a separate report to CEOs and boards on the effectiveness of the risk management processes and information that the first line is reporting to the CEO and board. The role of the third line, internal audit, is to provide an independent report on how well the first and second lines are doing.

4 Objective-centric risk assessment is aligned with reward and motivation systems. People are not usually paid to 'manage risks', but are often paid to achieve objectives. The people with the most to gain by achieving objectives are paid to learn how to formally assess, monitor, report on and manage the certainty/risk that those objectives will be achieved. Experiential/ intuitive risk management used everyday by people all over the world is elevated to a more structured and rigorous process.

5 Strong first line risk governance provides significantly better information to senior management and the board to help them discharge escalating risk oversight expectations. This aligns with five years of survey results from the annual 'risk oversight' surveys conducted by North Carolina State University, sponsored by the American Institute of Certified Public Accountants. Those surveys indicate that boards around the globe have been asking for significantly more visible senior executive engagement in risk management and risk oversight. Results of that survey are shown in the chart below for 2015 to 2019.

A key issue central to the business case for objective-centric/strong first line risk management is captured in a simple question: how can management effectively manage risks to objectives they are responsible for if they aren't expected to know how to formally/transparently assess the acceptability of the current risks/ certainty linked to those objectives?

What the future holds – the jury is still out

The majority of organisations in the world today use weak first line/risk-centric risk management processes. The new IIA 2020 three lines model is a huge step forward that hints at, but doesn't clearly state, there is an urgent need for companies to transition from a focus on 'risks' to a focus on managing certainty that top value creation and preservation objectives are achieved. Organisations don't need more clarification/ endorsement from the IIA to endorse objective -centric/strong first line risk management. The framework meets core regulatory requirements to demonstrate the existence and functioning of an 'effective risk appetite framework'. The business case for focussing all lines on risk/certainty of achieving objectives is strong. The only really big question is 'are companies willing to embrace and move to a significantly better approach to risk governance?'

[1]See Observations on Risk Management Practices during the Recent Market Turbulence, Senior Supervisors Group, March 6, 2008 (last accessed on September 5, 2013 at www.newyorkfed.org/newsevents/ news/banking/2008/SSG_Risk_Mgt_doc_final.pdf), and Risk Management Lessons from the Global Banking Crisis of 2008, Senior Supervisors Group, October 21, 2009 (last accessed on September 5, 2013 at www.sec.gov/news/press/2009/report102109.pdf). [2]International Standard, *ISO 31000 Risk Management Guidelines 2018.* [3]*Three Lines of Defense vs Five Lines of Assurance: Elevating the Role of the CEO and Board,* Wiley Governance Handbook, Chapter 19, Tim Leech and Lauren Hanlon, 2016

EXTENT TO WHICH BOARDS ARE ASKING FOR MORE SENIOR EXECUTIVE INVOLVEMENT IN RISK MANAGEMENT