Board & C-Suite Driven Assurance: The Dawn of a New Era

Tim J. Leech CIA CCSA CRMA FCPA

tim.leech@riskoversight.ca

Many years ago I wrote a seminal article titled "Control & Risk Self-Assessment: The Dawn of a New Era in Corporate Governance". That article, and the ideas in it, played a significant role launching my first company in 1991, and had a significant impact on the profession globally. Almost 25 years later this article describes recent developments and forces that will almost certainly see the onset of an even more profound and significant transformation – truly the dawn of a new era in internal auditing.

Traditional/Historical Internal Auditing

I joined the profession as an internal auditor in the summer of 1981. Since that time the profession has evolved and advanced in many positive ways, but continues to be bound by some fundamental and confining paradigms. Those paradigms include:

1. Internal auditors plan, execute and report results of point-in-time audits.
2. Internal auditors assess "internal controls" and report opinions on whether they believe controls are "effective".
3. Internal auditors report what they believe to be "control deficiencies", "material weaknesses", "significant deficiencies" or "opportunities for improvement".
4. "Direct report" auditing is the primary approach used globally. In a direct report engagement the auditor directly evaluates the subject matter for which the accountable party is responsible. The accountable party does not make a written assertion on the subject matter they are responsible for.
5. The profession has been primarily "supply driven" not "demand driven".
6. Internal audit does not usually know, or require that management and boards define the type and amounts of risk the company and its board are prepared to accept.
7. A majority of internal audit departments have not, for a variety of reasons, assessed and reported on risks to the organization's top strategic/value creation objectives, or the effectiveness of the entity's entire risk management framework.

The traditional/historical direct report approach to internal auditing described above is now under attack. Evidence collected globally in 2014[1] indicates dramatic drops in internal audit customer satisfaction.

Key Developments Globally

Board responsibility to oversee management's risk appetite and tolerance significantly elevated - Following the 2008 global financial crisis commissions were convened around the world to try and understand what had gone wrong and prevent similar destabilizing events in the future. A unanimous conclusion was that boards of directors and, to a lesser degree, regulators, had not adequately discharged their duty to oversee what is increasingly being called management's "risk appetite and tolerance".

Creation of the world's first preeminent regulator guidance body – Financial Stability Board ("FSB") – Shortly after the onset of the global financial crisis a decision was made to create a new super regulatory power, the Financial Stability Board ("FSB"). This organization, currently chaired by Mark Carney, Governor of the Bank of England, with representation from governments and financial sector and securities regulators from around the

[1] IIA Pulse on the Profession, Enhancing Value Through Collaboration: A Call to Action, IIA AEC, July 2014.

world, has, with unprecedented speed, formulated and disseminated what is most aptly termed paradigm shift guidance with an overarching, albeit, unstated goal of reengineering corporate governance globally. One of the FSB's most significant contributions to date is a November 2013 guide for national regulators, companies, and auditors titled **"Principles for an Effective Risk Appetite Framework"**.

The authors of the FSB guidance took the bold step of defining new and bold mandates for management, boards of directors and, most significantly for readers of this article, internal auditors. Details of the new role envisioned for internal auditors is shown in the box below. The FSB is, in essence, calling on internal audit to transition from providing spot-in-time, direct report, subjective opinions on "control effectiveness" on a small percentage of an entity's risk universe, to reporting on the reliability and effectiveness of an organization's entire RAF, including, but not limited to, reporting on the reliability of risk status reports provided to the organization's board of directors by management.

4.6 Internal audit (or other independent assessor) should:

a) routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;

b) 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;

c) independently assess periodically the design and effectiveness of the RAF and its alignment with supervisory expectations;

d) assess the effectiveness of the implementation of the RAF, including linkage to organisational culture, as well as strategic and business planning, compensation, and decision-making processes;

e) assess the design and effectiveness of risk measurement techniques and MIS used to monitor the institution's risk profile in relation to its risk appetite;

f) report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and

g) evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.

Source: Financial Stability Board, Principles for an Effective Risk Appetite Framework, November 18 2013.

Codification of board responsibility to oversee management's risk appetite and tolerance – In parallel with the FSB, regulators around the world have started to enact regulations that reflect key FSB recommendations, particularly the need to assign primary responsibility for risk management and reporting to management, and risk appetite/tolerance oversight to boards of directors. One of the most graphic illustrations is the new UK

Governance Code issued in September 2014. It positions responsibility for risk oversight squarely with boards of directors; calls on management to design, implement and maintain effective risk governance frameworks; and calls on boards to seek independent assurance that management has, in fact, designed, implemented, and maintained effective risk governance frameworks. It is expected other major countries that want to improve the integrity of their capital markets will follow the UK's lead.

Internal audit customer satisfaction plummets – as these regulator driven developments gain traction globally a summary of customer satisfaction surveys done by 3 major consulting firms and the Institute of Internal Auditors was reported in the July 2014 IIA Pulse on the Profession Report referenced earlier. The report paints a graphic picture of a significant and very recent decline in board and senior management satisfaction with traditional/historical direct report internal audit services.

What This Means to the Internal Audit Profession Going Forward

Need to Transition from "Direct Report/Spot-in-Time" Auditing to Attestation Reporting on Management Representations on Risk Framework Effectiveness and Risk Status – the FSB has defined roles for the board, senior management, and internal audit that call for a fundamental accountability shift - a shift that requires management continuously assess and report upward on risk status, and for internal audit to assess and report opinions to the board how well management is discharging their assigned risk governance responsibilities. This new paradigm requires radical and fundamental shifts in existing IIA certification curriculum and training offerings. IIA IPPF professional practice standard 2120 was modified in 2010 specifically to provide support the shift and the Certification in Risk Management Assurance ("CRMA") launched globally. Internal audit departments will need to evolve from the business of performing traditional spot-in-time direct report audits and providing subjective opinions on "control effectiveness" on a small percentage of the risk universe and, instead, focus substantially more resources on providing assurance to boards that senior management is creating and maintaining effective risk management and reporting frameworks.

Educate Boards of Directors on Evolving Expectations - the evolution of these expectations is likely to evolve at varying speeds and intensity in different countries. Not all senior management and board members have been actively following the evolution of these new expectations, and not all national regulators have codified risk governance expectations with the clarity and simplicity of the September 2014 UK Governance Code to spur the needed transition. It is also important to note that not all CEOs and CFOs are likely to welcome direct responsibility for creating and maintaining effective risk appetite frameworks and providing formal reports on residual/retained risk status to their boards.

Look for Opportunities to Gain the New Knowledge and Skills Required - If internal auditors are to accept and assume the type of responsibilities defined by the FSB earlier in this article, they must "retool" their knowledge and skills. Instead of the traditional internal audit focus on providing subjective opinions on "control effectiveness", internal auditors now need to acquire the knowledge and skills to assess and report on the reliability of management's risk appetite frameworks, including management's reports to the board on retained/residual risk status. This means learning the type of vocabulary defined by the FSB in its *Principles For An Effective Risk Appetite Frameworks* guidance and ISO 31000 and ISO Guide 73, and gaining the knowledge and skills necessary to identify the full range of risks, "risk treatments", and a picture of residual risk status, not the much narrower assessment of traditional "internal controls" internal audit has historically focused on. More importantly, internal auditors need to continuously assess and report on whether the current residual risk status related to key strategic and foundation objectives is currently within the board and senior management's risk appetite and tolerance.

Closing Remark - Recognize that aversion to change is a human condition – this short article outlines events and drivers that call for radical and quantum change in the current internal audit paradigm. A natural human trait is to resist radical change and favour smaller and more incremental steps. The dramatic drops in customer satisfaction

statistics described in the IIA July 2014 Pulse on the Profession report have led to the IIA literally issuing – A CALL TO ACTION to internal auditors around the globe. Addressing rapidly evolving and escalating customer and regulatory expectations will require the profession globally make rapid and radical changes if it is to ensure it remains fully relevant to key customers in the years to come. There is a well-known adage that states "necessity is the mother of invention". The need for radical and rapid change in the traditional internal audit delivery model is real. It's time the internal audit profession to literally reinvent itself to meet the needs of key customers – particularly boards of directors. No small task to be sure, but a job that absolutely needs to be done. Best wishes for success as the profession decides whether it welcome, or resist, the dawn of a new era in internal auditing.

Tim J. Leech CIA CCSA CRSA FCPA is Managing Director Global Services at Risk Oversight in Canada. He is recognized globally as a thought leader, innovator, trainer and advisor in the risk and assurance field. He can be reached at tim.leech@riskoversight.ca