TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 93 | June 2019

Audit Tiptoes the Line Between Audit and Risk Management

Internal audit executives report on all sorts of things, and that's not going to change. To whom all those things should be reported, however, is an open question.

On one hand, audit executives are being asked to do more. They are expected to be trusted advisors, counseling the board about risk. They're to embrace new technologies that allow better analytics and more perceptive monitoring of risk throughout the enterprise.

At the same time, boards are under pressure. Regulators, shareholders, customers, business partners, and others all want them to do a better job at governing risk — not just reviewing it or setting tolerances for it. Stakeholders want to hold boards more accountable, all the time.

Think about what that means. If the audit executive and the board are both being challenged to do better at the same tasks — assessing risk, and building a capability to intervene when a risk stretches beyond the comfort zone — a tangle of questions are raised about corporate governance, risk assurance, and the role of the chief audit executive.

For example, should corporate boards establish risk committees? If so, what issues does the audit executive report to them? If the CAE discusses some issues with the risk committee but other issues with the audit committee, is that wise? Should the CAE's role be split? Or is the converse true: that modern technology is fusing internal audit and risk management into one larger risk assurance function?

"I'm not sure we as a discipline have argued well enough, to those who are not as passionate as we are, as to the benefits of who owns risk," says Tom McLeod, head of risk for the Australian Broadcasting Corp. and a former board director of The Institute of Internal Auditors–Australia.

As a result, audit executives might be drifting into a role nobody quite anticipated, straddling audit and risk management duties. They've always been good at the former, modern technology is making them better at the latter — and, well, somebody has to do it.

"It's that slow journey," McLeod says, "where you don't realize you're more heavily involved in risk monitoring until you are heavily involved in risk monitoring."

That's true of audit executives as much as it's true of corporate boards. So how do both groups channel this evolution productively?

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with more than 200,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit **www.theiia.org/tone** to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to **tone@theiia.org**.

Content Advisory Council

With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

Begin With Board Pressures

According to a 2018 study by the EY Center for Board Matters, reported in the Harvard Law School Forum on Corporate Governance and Financial Regulation, only about 11 percent of boards in the S&P 500 have a risk committee. Even then, the concentration is in financial firms, with 74 percent having risk committees. Outside that sector, the percentage plummets, with only four percent of consumer, industrials, tech, and utilities having risk committees.

But those numbers don't capture the full tale. For example, the Federal Reserve requires publicly traded banks with assets of $10 billion or more to have a risk committee, so it's no surprise that so many do.

Meanwhile, according to that same EY study, 14 percent of consumer firms have a public policy committee, and 38 percent have a corporate responsibility committee. In the health-care sector, 21 percent have a regulatory affairs committee, and 18 percent have a technology committee.

That all makes sense. Consumer firms worry about being perceived as good corporate citizens; hence, more have corporate responsibility committees. Health-care firms are highly regulated, especially around personal health information; as a result, they have more compliance and technology committees. As long as the company has some board committee that watches risks important to the business, who cares what it's called?

James Lam, chair of the risk committee at E*TRADE and a long-time risk management consultant, says any business with more than $1 billion in annual revenue should consider forming a dedicated risk committee.

In Lam's view, that committee should address "technical, granular risks," which could be anything from compliance to sustainability to cybersecurity to anti-money laundering, or whatever else needs attention. The goal is to take those issues off the full board's plate, so it can focus on strategic risks.

"If the full board can do all that, fine," Lam says. "But that's a very full agenda."

McLeod cites the example of Rio Tinto, where he was chief audit executive in the early 2010s. The board had a sustainability committee that looked at land rights, water use, and other environmental concerns — "deep, fundamental risk issues that were rarely touched or considered," he says.

McLeod reported to both the audit committee and risk committee at Rio Tinto, but he knew what he had to discuss with each committee. When risk and audit committees are combined, "there's not a clear understanding of the delineation," he explains.

This could all represent a poor understanding of risk governance more than anything else. Audit committees have been around for decades, and their duties related to strong financial reporting have been clear since the Sarbanes-Oxley Act of 2002. That is, people "get" what audit committees should do.

Risk governance is vague. Outside of the banking sector, specific regulations about what a risk committee does are scarce. Thinking about risk calls for creativity and imagination — traits not generally required of audit committee members.

"The audit committee 'is paid to think inside the box,' in a world of corporate disclosures, financial reporting rules, and SOX testing," Lam says. "There are very specific rules, internal control requirements, and testing."

The risk committee, however, "is paid to think outside the box." So, it's going to view the organization's business activities in a different way than the audit committee does. A risk committee will need different types of information — more types of information — to guide its work.

The Trouble in Splitting the Difference

Well, hold up. Chief audit executives supply information to the board. So, if the board does establish separate audit and risk committees, can the CAE report to both?

McLeod believes so. That's what he did at Rio Tinto. At the other end of the spectrum, however, are voices like Richard Anderson's, chair of the risk committee at Pay.UK in London and a member of that firm's audit committee. He sees risk management as "struggling with the multiple futures that our business might face," and therefore quite distinct from the audit function.

What makes this question so thorny is the arrival of modern technology. Yes, artificial intelligence, robotic process automation, and data visualization all help the chief audit executive identify risk and test internal controls in ways never before possible. That's the good news.

Then again, once the audit team builds those next-generation risk analysis tools, they immediately become risk management tools, which business functions can use to guide their operations.

Action Items

Review committee charters. Audit committees pick up one concern after another, from compliance risk to cybersecurity to corporate culture, and more — all on top of their regular duties of overseeing financial reporting and internal controls. Revisit the board's committee charters to see if those non-financial reporting risks would be better served by a risk committee that could give those issues the attention they demand.

Assess risk assurance duties. Along similar lines, review all the risk assurance duties within the organization to see whether the creation of a chief risk officer role is warranted. Odds are that most First and Second Line of Defense functions already perform some risk management, even if they lack a uniform, disciplined approach. If that is the case, would a CRO help to bring that discipline? Or could a smaller organization adopt a standard methodology to achieve the same thing?

Consider how technology will help risk management. Data analytics, visualization tools, and artificial intelligence all could easily be "dual use" technologies — able to help the audit function assess controls and other functions to manage risk. Does your organization have a technology strategy to guide that, to help senior management and the board make better decisions?

For example, it would be a relatively straightforward exercise for the audit team to build algorithms that find personal data collected before consent was given, or reseller contracts signed before third-party due diligence was completed. Then the marketing or sales teams could use those algorithms to manage their own risks. For global businesses with concerns about privacy or bribery, those are issues a risk committee might want to oversee.

In this analytics-driven world — which is, remember, the world that everyone says the audit function should embrace — where does auditing end and operational risk management begin?

Anderson minces no words about the prospect of internal audit developing algorithms that the business might use for risk management: "They should not be developing or running them." Businesses should build their own models, which audit then can test for effectiveness.

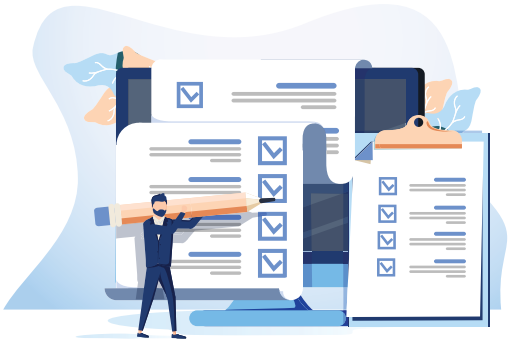
For better or worse, however, many firms don't do that. Rather, they toddle into analytics-driven risk management, and internal audit is asked to lead the way, because it has been honing its skills at data analytics for years while studying financial transactions or T&E spending.

Consider the idea from start to finish: The board begins with an urgency for better risk management, but doesn't define what a committee should do to address it. Instead the board says, essentially, "You, audit function — help us out with this."

That impulse could eventually lead audit and risk management to combine into what McLeod calls a "chief assurance function. ... The role of the future, a merging of the two since they've never been properly delineated."

But, McLeod adds, "What goes by the wayside is the independence aspect."

And, in the end, boards need to understand the uniqueness that internal audit brings and the value derived by having an independent function.



Quick Poll Question

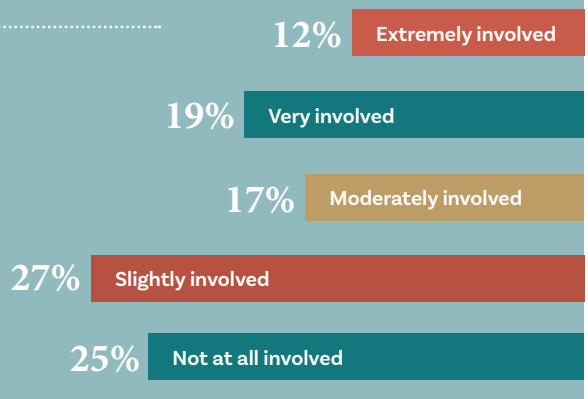
How often does internal audit provide reports to the Risk Committee?

- ❑ On a regular basis
- ❑ Periodically on specific risk issues
- ❑ Only when requested
- ❑ There is no separate Risk Committee

Visit **www.theiia.org/tone** to answer the question and learn how others are responding.

QUICK POLL RESULTS:

How involved is internal audit in assuring accurate and complete information flows to the Board?



Source: Tone at the Top April 2019 survey.