What does your audit committee know about risk?

Overview

One of the key factors to a successful partnership between chief audit executives and the board is risk maturity. Here, we explore this idea and things you can do to build a more powerful partnership with your board, audit and risk committees.

UK governance for listed and private companies makes it clear that the board has responsibility for an organisation's risk management system regardless of its delegation to a board committee for oversight. Without sound knowledge and understanding, this is like putting a passenger in the pilot seat of an aircraft and turning off the autopilot. Does your board know enough about risk?

Who owns risk?

One of the key principles of corporate governance is that "the board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives."

It goes on to state that the board "should establish an audit committee of independent non-executive directors." One element of their remit is to review "the company's internal financial controls and internal control and risk management systems, unless expressly addressed by a separate board risk committee

composed of independent non-executive directors, or by the board itself."

Whilst chief audit executives will report to the audit committee chair, they may also be asked to report on risk to any or all of the board committees depending on the resourcing of risk management. Internal audit has legitimate roles within risk management, as defined by the Chartered IIA.

In the financial services sector risk committees are mandated.

Why is risk maturity so important?

Risk maturity is all about taking informed risk, knowing when to seize an opportunity and when to say stop. For the board and particularly the non-executive directors it is much more than casting an eye over a risk register or heat map. It can be the difference between hitting the headlines positively or negatively aka Carillion, Patisserie Valerie, Interserve and Facebook, to name but a few.

A board member might perceive themselves to be risk aware. They look at a risk report, debate a position on a heat map, know about the latest cyber headlines and the regulations the organisation must comply with….but do they understand risk appetite, the potential of modelling and simulations, active oversight of risk mitigation and assurance mapping. As with any demographic there will be differences, those with exceptional knowledge and those that are essentially faking it.

The Chartered IIA risk maturity model is a good reminder for auditors of an organisation's progress through the different stages.

It can be challenging for audit leaders to have meaningful conversations with their AC if they have limited awareness of the subject being discussed. For example, where boards have shied away from defining their risk appetite, internal auditors can be locked in subjective debate with management as to what constitutes *taking too much risk*; what is a high finding, a red report, a priority action. How can the AC effectively support audit leaders without the right tools and knowledge?

Risk maturity comes from knowledge and understanding. The commitment to develop skills, processes and reporting that promotes effective risk management and the achievement of objectives. Taking informed risks rather than avoiding risk or taking subjective decisions.

Surely all directors have good risk awareness…

In one of his blogs, IIA President and CEO Richard Chambers said: "risk defines the world of the internal auditor [it] shapes our audit plans, directs our stakeholders, and determines our success or failure."

Risk is a complex subject and it is natural that understanding varies considerably. It is also a fairly recent concept in the boardroom having been first introduced via the Turnbull report in 1999 although its uptake was at a slow pace until the financial crisis in 2008.

In real terms, even experienced directors have had a limited time to get their heads around the detail of formal risk management. There is a big difference between applying a common-sense approach to risk and the level of formality now required to satisfy stakeholders including regulators.

Think about your own organisation:

- How have you sought to understand the risk knowledge of your board?

- What experience do they bring?
- Are they competent to sit in the pilot seat of sub-committees?

Expectations of the audit and risk committees

All that aside, there is a job to be done. Audit leaders are not unreasonable in expecting to have more than a passing awareness of risk management. After all, it is a key component of corporate governance.

The FRC's Guidance on Audit Committees states that new members should receive an induction including "an overview of the company's business model and strategy, identifying the main business and financial dynamics and risks." It also suggests "ongoing training, including the role of internal and external auditing, and risk management." The FRC being principle based does, however, *assume* a level of knowledge rather than make explicit statements.

Specific governance principles for banks outline the requirements for the audit and risk committees. This is a useful guide for audit leaders in all sectors if their organisation has or is considering introducing a risk committee.

The Institute of Directors goes further and addresses risk management within their director competency framework detailing various attributes re knowledge, skills and mind-set.

Competency	Knowledge Area	Consideration points for directors
Governance	**Risk Oversight**	Risk appetite and the role of risk in growth and value creation
		The structures and systems which enable your organisation to effectively identify, assess and manage risks and crises
Strategic Thinking	**Considering the Impact of decisions**	Identify the potential impact of decisions and offer contingency plans and risk mitigation
Decision Making	**Taking appropriate risks**	Take calculated risks in the context of the organisation's strategy and the appetite of the board

Think about your response to the earlier questions:

- Have you been lenient in your judgement?
- Does your audit/risk committee demonstrate an appreciation and understanding of risk?
- What role did you have in the induction programme for all of your NEDs?
- What role did your risk colleagues have in the programme?
- When is the last time the audit committee agenda allowed time for training/updates?

Partnership impact

The partnership between chief audit executives and the audit committee has a major impact on the

organisation. It is a critical relationship.

Audit and risk committees lacking sufficient awareness and the tools associated with risk maturity are unable to provide the direction and support that facilitates internal audit functions to deliver their full remit. Issues can easily arise regarding the importance of audit reports, lack of commitment to mitigation plans, resourcing challenges, quality of the audit plan and the value of the profession.

An appreciation of concepts such as risk appetite makes the job of providing assurance so much easier and more constructive for the organisation. Risk mature directors are more likely to welcome root-cause analysis and see the value-add of a cultural audit due to their understanding of enterprise-wide rather than silo risk.

Constructive challenge, from the audit committee, of the audit plan is imperative to drive continuous improvement and stretch internal audit functions; as is sponsorship to audit the right risks even when it can be contentious.

Partnerships bring value to both parties, a powerful alliance to protect the organisation. For some years now audit leaders have known that strategic risk is where shareholder value is lost. Research by the Corporate Executive Board in 2014 confirmed that the trend away from non-strategic risks in the drivers of value decline is continuing

Strategic Risk	Operational Risk	Legal & Compliance Risk	Financial Risk
86%	**9%**	**3%**	**2%**

The Chartered Institute's 2019 Risk in Focus report includes a feature on auditing the 'right risks'. It shows that internal auditors spend most of their time auditing compliance, financial controls, data security and protection, cybersecurity and regulatory change. Strategic risk doesn't even feature as a category!

What does this say about audit plans, risk maturity and the effectiveness of the relationships between CAEs and their audit committees?

Tips for building risk awareness (and maturity)

Sadly there are no silver bullets for board members especially those chairing audit and risk committees. Organisations and people are unique so what works for one might not work for another. You need to use your own insights to work out what could be beneficial, if it doesn't land just try something else.

Talk

Instinctively you know how risk mature your audit committee is. Think about ways to open discussion on the topic that allow individuals to open up without feeling pressured.

Here are some ideas to get you started:

- How confident are you that the organisation has got all its risks identified?
- Life is rarely linear and straightforward, which combination of risks happening at the same time worries you the most?
- Risk appetite is a bit of a complex subject how do you think about it from a practical point of view?
- When you think about our strategic goals and the things the organisation is doing today - are we being too cautious about getting there or too maverick?

- What is your secret to thinking about the unknown unknowns that could come at us from left field?
- Which board reports do you enjoy reading and why? Are there any that you always learn something new from?

Risk management audit

Back to basics. If maturity needs to be improved, where better to start than with an audit of risk management. Be brave - it might mean asking the CEO to sponsor actions such as board training or endorsing policy. Think about whether the risk information provided to the board/audit/risk committee encourages them to discuss the right things. For instance, if risk reports major on process, they become repetitive and a waste of valuable time, the focus should be on strategic and emerging risks, interdependencies, risk mitigation plans, priority risks and the results of research and risk analysis.

Shake up the audit report

Take a fresh look at the language you use and the format of reports.

- Are the reports interesting?
- Is the relevance of risks clearly communicated?
- Do they tell a story about risk management or are they more a succession of fragmented facts?
- Regardless of whether your organisation has useable risk appetite statements do you talk about risk appetite?

Lead by example to drive risk awareness. Provoke questions. Provide answers.

Relevant reporting

Think about how the audit committee report can build risk maturity. Work with the risk function if there is one. Your report could include a risk section, an audit/risk dashboard or a feature 'opinion' on topics such as culture, risk, governance etc.

Education

Find a way to bring risk education into the boardroom. Find allies to work with such as the company secretary, an audit committee member, a 'get-it' director or external audit partner. Make it interesting, interactive and personal; avoid papers, PowerPoint and preaching! Address why risk maturity is this important for them; personal success, achieving rewards, protecting their reputation and enhance experience. Think about a balance between process and behavioural/cultural training.

Embed risk disciplines

In an ideal world the board and senior management will lead by example with risk as a key part of their decision-making. To help embed risk and make it part of everyday discussions and activities use audit engagements as an opportunity to heighten its visibility in audit topics such as capital requests, budgeting, project management, strategy, performance management and operations.

Authorities audit

If an audit of risk management seems daunting or has met with resistance, try an innocent audit of authority levels. Most organisations have delegated authority levels for financial risk but what about other risks? This could be a good introduction to raising awareness using the familiar backdrop of financial controls.

Reduce compliance

Whenever the opportunity presents itself remove barriers to risk maturity such as ‘tick-box compliance’. Maturity cannot be achieved with a checklist mentality. Routine risk assessments and focus on regulatory requirements can lead to complacence. Make compliance checks meaningful, engage people with the risk they are managing not just the control itself. Spice it up a little – make people think!

Closing Thoughts

Audit leaders have a responsibility to promote good risk management. It begins in the boardroom with strategy and permeates through the organisation to the cleaner noticing sensitive data in a rubbish bin. This level of risk maturity takes time and effort. It is forged out of a blend of knowledge, collaboration and values. Partnerships are critical to its development and success. Which partnerships are you part of in your organisations journey towards risk maturity?

"Risk management is the most important thing to be well understood"

Bruce Kovner, hedge fund manager and philanthropist