Internal audit
Trends and challenges

Terry Hatherell
Global Internal Audit Leader
Deloitte

Now, more than ever, the internal audit department is recognised as a key pillar in an organisation's overall governance structure. Unfortunate past incidents of corporate wrongdoing and, more recently, risk failures have again served to highlight the critical role that internal audit plays and have shone the spotlight squarely on internal audit to step up and deliver on increasing expectations.

Traditionally, the internal audit function focused on providing core assurance around business process risk and controls. But, with increasing market volatility and complexity, internal audit is being asked to deliver deeper insights and value beyond assurance, particularly in the areas of strategy execution, emerging risk, and increasing the use of analytics. Delivering on these new and increased expectations presents many challenges for internal audit departments today.

An ongoing challenge for internal audit relates to multiple stakeholder expectations which, at times, may differ. It is generally considered that, to ensure the independence of the function, internal audit should report functionally to the Audit Committee of the Board of Directors. Audit Committees, however, have a very clear fiduciary and governance responsibility with respect to value preservation and ensuring that principal business risks are effectively managed across the organisation. These responsibilities translate directly into an expectation that internal audit provide assurance to the Audit Committee (and more broadly to the Board of Directors) that key risks are identified and managed effectively. Without question, this independent assurance role is a basic expectation for all internal audit departments and is at the core of internal audit's mandate. Other stakeholders, including regulatory bodies for regulated entities, have similar expectations of internal audit. Management, as one key stakeholder, looks to internal audit for similar assurances; however, increasingly, management expectations extend beyond this core assurance role in search of greater value—in effect, a greater return for the organisation's internal audit investment. As context for this expanded expectation, one needs to look no further than what is transpiring in many organisations today—a laser focus on creating shareholder value in an uncertain and often challenging business climate.

The expectation of enhanced value is not a new challenge for internal audit departments. What is different today is the confluence of factors—greater complexity which creates new and emerging risks, significant risk failures leading to reputational, regulatory and financial impacts; and an uncertain and challenging economic environment in many regions which has created the need in many organisations to 'do more with less' in order to drive greater shareholder value.

To respond to these challenges and to deliver on multiple and increased stakeholder expectations, highly effective internal audit departments are employing a number of strategies and tactics.

As the business landscape for most organisations becomes increasingly complex and fast-paced, there is a movement towards leveraging business analytic techniques to refine the focus on risk and derive deeper insights into the organisation. Leading internal audit departments are moving beyond the use of ad-hoc analytics that have traditionally provided hindsight and into areas of continuous auditing, sustainable analytics, the application of exploratory and predictive methods and sophisticated data visualisation techniques—all of which deliver profound fact-based insights and foresights. Leveraging analytics allows internal audit departments to produce deeper insights and conclusions that help decision-makers take action quickly and make more effective, timely decisions. At the same time, the use of analytics allows internal audit departments to be more efficient and 'do more with less' by analysing entire populations of data rather than reviewing and assessing samples of transactions. Advanced analytics capabilities also incorporate a predictive element to provide foresight into risk events before they occur. Examples of high-value areas where analytics is being embedded into internal audit activities include predictive project analytics to assess the effectiveness of project risk management and the likelihood of project success as well as vendor cost recovery reviews to identify duplicate and inappropriate billings and to assess related vendor governance and expenditure controls.

Increasingly, internal audit departments are also including a specific focus on emerging risk. Some internal audit departments have even allocated a defined percentage of internal audit resources to focus exclusively on the evaluation of emerging risk areas. With the explosion of new technologies and the ever-accelerating pace of technological innovation, it comes as no surprise that many of these emerging risks are technology-related. Threats posed by cybercrime, for example, have increased faster than the many organisations' ability to cope with them. Today's cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile and long-term presence within information technology environments. And many organisations risk leaving themselves vulnerable to cybercrime due to a false sense of security, perhaps even complacency, driven by non-agile security tools and processes. Cloud computing is another example of an emerging technology risk and represents a major change in information technology architecture, sourcing, and services delivery by giving businesses on-demand access to elastic and shared computing capabilities. The adoption of cloud computing creates new risks beyond the more obvious security-related risks such as those associated with regulatory, privacy, data integrity, contractual clarity, business continuity and vendor management issues, to name just a few. Other emerging risks include mobile payments, social media, big data and risks related to the extended enterprise created by virtue of the increased use of outsourcing and third parties in businesses today.

With the onslaught of regulations impacting organisations and the expectation that the regulatory environment will become even more stringent, internal audit departments are focusing proportionately more time on assessing compliance with regulations. One such critical area relates to anti-corruption. Beyond the steep regulatory, legal, and financial consequences of non-compliance with anti-corruption legislation, reputational impacts can have severe and long-lasting effects. The Foreign Corrupt Practices Act (FCPA) (which makes it illegal for U.S. citizens or companies to attempt to bribe foreign officials in order to gain a business advantage) and the UK Bribery Act of 2010 are two such examples of regulations with an impact on a global scale. Given the significant risks involved, it is imperative that organisations have anti-corruption programmes in place to ensure compliance. Key elements of an effective anti-corruption program include board oversight, written standards and policies, risk assessments, communications and training, monitoring and auditing, incident reporting, corrective actions, and discipline. Leading internal audit departments are reviewing the design and effective operation of their organisation's anti-corruption programme and are providing independent assurance to management and the audit committee that key anti-corruption risks are managed to an acceptable level.

The recent financial crisis in many regions has highlighted the extent to which a risk and control culture can shape, for better or for worse, the awareness, attitude, and behaviour of employees toward internal and external risk and the management of risk within an organisation. An organisation's culture has a pervasive impact on how its individual members behave. As a result, organisations as well as regulators and government bodies have realised the crucial role that risk and control culture plays in the way risks are managed. In the 'people, process, and technology' trinity of risk management infrastructure, it is indeed people who ultimately make process and technology work. Furthermore, how people manage risks largely depends on the culture prevailing within the organisation. Increasingly, boards and senior management are considering actions to foster a stronger risk and control culture within their organisation. Leading internal audit departments are designing culture assessment frameworks and are executing internal audit activities to assess whether the prevailing risk and control culture and related processes, actions, and 'tone at the top' align with the organisation's values, ethics, risk strategy, appetite, tolerance, and approach.

As the risk landscape becomes more complex and specialised, internal audit departments are challenged to keep up in terms of having the skills necessary to competently assess critical risks impacting their organisation. Increasingly, leading internal audit departments rely on third-party expertise to provide specialised skills to supplement existing in-house resources. Information technology skills are the most common area where third parties support internal audit departments in bringing much-needed expertise in areas such as security, analytics, information technology governance and enterprise system-specific skills and experience. Additional non-technology specialised skills that internal audit departments frequently seek from third-party partners include regulatory, supply chain, anti-corruption and fraud-related competencies.

Stakeholder recognition of the importance of internal audit has never been greater. As a result, the expectations of internal audit with respect to risk assurance and the provision of insights continue to increase in lock-step. The challenge for the internal audit department, today, is to seize this unprecedented opportunity to cement its value proposition and position itself as a critical element in the overall governance ecosystem.

The recent financial crisis in many regions has highlighted the extent to which a risk and control culture can shape, for better or for worse, the awareness, attitude, and behaviour of employees toward internal and external risk and the management of risk within an organisation