Internal audit insights
High impact areas of focus

Internal audit is widely, if not universally, viewed as a key pillar in effective governance with expectations of internal audit greater and more visible than ever. High performance and effectiveness demands that internal audit departments focus their efforts on the key risks and issues facing organizations—a task made more difficult in today's environment of continued complexity, uncertainty, and change. While transactional oversight was once the prime mover, strategic risk has come to the fore, with internal audit becoming increasingly involved in a range of business-critical areas including major projects, cost reduction, cyber, fraud, and third-party risk management.

On an annual basis, Deloitte leverages its global network of internal audit professionals to identify high impact areas of focus that internal audit departments should consider incorporating into their audit plans. As you prepare for your 2015 internal audit activities, we are pleased to provide you with this year's edition of our *High impact areas of focus* series. We hope you find it both thought-provoking and of value.

Predictive project analytics

Studies[1] continue to show that a very large percentage of organizations experience project failure and that almost one-half of all projects fail to meet time, budget and quality goals. Given the high cost and strategic importance of many projects today, internal audit cannot ignore this critical aspect of its audit universe. In order to properly assess what is often greater project complexity and risk, traditional approaches — while important — may no longer be sufficient.

Leading internal audit departments are now taking advantage of advancements in technology, including predictive project analytics (PPA), to address these challenges head on and provide their organizations with much deeper insights and foresight with respect to their project risks. Leveraging advanced analytics, PPA allows internal audit to evaluate the likelihood of project success, identify project strengths as well as key control gaps and enables internal audit to provide actionable recommendations to management. Beyond individual project assessment, PPA is also used by internal audit to evaluate programs or portfolios of projects.

[1] Schlumberger Business Consulting, *Planning & Assurance*, Dave Sivaprasad and Trung Ghi (2011); *Speed Kills*, Ali Klaver (January 2012)

Advanced data visualization

Advanced data visualization techniques help auditors discover meaningful patterns in vast amounts of data. While still considered “advanced” today, data visualization is fast becoming a de facto standard. In business communications, data visualization helps convey complex scenarios and substantiate results.

How can internal audit be more effective through the use of data visualization? Leading internal audit departments are using data visualization to provide deep analytical insights and actionable information. For example, recently, data visualization was deployed by internal audit for a procurement audit within a global construction company. The internal audit team distilled more than one million lines of data to visually illustrate spend by location, individual, and product over time. This approach was instrumental in identifying occurrences of fraud, waste, and abuse, resulting in a positive outcome for the organization and a favorable perception of internal audit.

Continuous auditing

Continuous auditing (CA) and its benefits are well-recognized and have been talked about for a number of years, yet relatively few enterprises have realized its full potential. CA allows internal audit to continually extract key data from business processes to enable its internal audit activities. CA promotes a shift from cyclical or episodic reviews with limited focus to continuous, broader and more proactive reviews. CA also evolves the traditional, more static annual audit plan to a dynamic plan based on the CA results. CA should not be confused with continuous monitoring which is an approach employed by management to determine more quickly where to focus the organization’s resources and attention to improve processes, address risks, or launch initiatives.

The continued proliferation of new and emerging technologies has helped the business case for CA. Further, the business benefits realized by many organizations through the convergence of governance, risk and compliance solutions has helped make CA a reality for a greater number of leading internal audit departments. Internal audit departments, seeing the benefits of incorporating data analytics into their audit activities, are now realizing that the implementation of CA techniques through the extension of analytics is not quite as difficult as it may have been in the past.

Cyber crime

All too frequently, organizations, both large and small and across all industries, are targeted and compromised by cyber criminals. Threats posed by cyber crime have increased faster than the abilities of many organizations to detect, prevent and manage such threats. Any organization dealing with this imminent risk faces potential significant reputational and financial impacts, in addition to regulatory risks, as industry regulators increasingly cite cyber security as one of their top priorities. Today’s cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence within information technology environments. Meanwhile, many organizations may be leaving themselves vulnerable to cyber crime based on a false sense of security, perhaps even complacency, driven by the lack of understanding about the evolving threat landscape, and use of non-agile security tools and outdated processes. Many are failing to recognize cyber crimes in their IT environments and misallocating limited resources to lesser threats.

It is imperative that internal audit takes a leading role in determining whether a systematic and disciplined approach exists to evaluate and strengthen the effectiveness of cyber risk management and determine if appropriate cyber security capabilities (people, process, and technology) are in place to protect against cyber threats.

Software asset management

Software purchases account for a significant portion of many organizations' IT capital spending. However, the full impact of the software license agreements and contracts are rarely understood, and the related internal controls are often found to be lacking or immature. According to a recent Gartner survey[2], over 68 percent of respondents had been audited by at least one software vendor during the past 12 months. As a result, many organizations, during routine audits, are found to be either under-licensed or not licensed optimally for the software they are currently using. Under-licensing can create significant financial, legal and reputational risk, while sub-optimal licensing could mean that the organization is paying excessive license costs. Many organizations do not closely track the procurement, deployment, and use of software, resulting in an increased security risk as well as unnecessary spends in over-licensing and maintenance. Proper management of software assets can help organizations ensure that their software licensing and related costs are commensurate with their usage and needs. Internal audit departments are responding to these risks by executing software asset management (SAM) operational reviews. These reviews often leverage enabling technology and include the following components: process risk and current state assessments, software risk assessments, and software license baseline reconciliations, resulting in insightful analysis and recommendations to address gaps in the organization's software asset management processes. The SAM operational reviews performed by internal audit frequently lead organizations to realize that a robust SAM process should be implemented, yielding potentially significant cost savings and enabling the organization to address future software vendor audits without significantly taxing the organization's resources.

Vendor governance

Many organizations face challenges ensuring that their relationships with vendors yield maximum value for their enterprises. With dependency on multiple vendors to meet their business needs, value lost in the supply chain can result in significant damage to the bottom line. Vendor relationships are often driven by complex and (at times) ambiguous contract clauses, leading to overpayment and/or overbilling in areas related to favorable pricing (often known in the technology industry as "most favored customer"), volume rebates/discounts, mark-ups, subcontractor costs, etc. Such costs are usually undetected due to the volume of transactions, limited operational/financial process controls, and lack of robust analytics tools and capabilities that can holistically monitor activities around vendor spend.

Leading internal audit departments see vendor governance as an important element in their overall audit universe. Vendor audits are being conducted to assess third party risk and also generate financial benefit for their organizations through cost recovery and improved controls to prevent excessive costs moving forward. Highly effective vendor audit programs leverage advanced analytical tools and techniques to address risks and generate unique insights into supply chain inefficiencies. The use of analytics also allows for the deployment of data visualization techniques that can be used both in the internal audit analysis and reporting of results.

[2] Gartner Research, *Survey Analysis: Software License Audit Surveys Show Shift in Focus and Intensity in 2014*, Victoria Barber, Frances O'Brien, Stewart Buchanan (Sept 2, 2014)

Fraud risk management

Fraud affects many organizations and, in today's economic climate, the adage "prevention is better than cure" has never been more accurate. While no organization can be completely immune from fraudulent activity, there is an increasing onus on management to have effective fraud prevention systems in place in order to reduce the exposure to financial loss, reputational damage and service interruption, all of which are common consequences of fraud. An organization's exposure to fraud risk is often heightened during periods of change and uncertainty. Increased financial pressures and reductions in headcount are two examples of why a fraud control environment may weaken.

It is important that organizations have effective fraud risk management frameworks in place, covering areas such as governance and leadership, risk assessment, policies and procedures, due diligence, training and communications, and monitoring and review. Internal audit, in line with its mandate, should play an important role in either assisting management with the implementation of such a framework (for example, facilitation of fraud risk workshops), or with the provision of assurance over key elements of the framework, including design and implementation testing of key anti-fraud controls, the adequacy of due diligence undertaken, or the effectiveness of the monitoring and review process (i.e., is the organization learning from past instances of fraud, both internally and within the industry/sector in which they operate).

Risk and control culture

Shortcomings in risk and control culture continue to underlie many organizational failures that appear in news headlines. Indeed, an organization's risk and control culture—the norms, attitudes, and behaviors related to risk awareness, risk taking, risk management and controls that shape decisions on risk— plays a major role in influencing the decisions of management and employees taken in their day-to-day activities, and has a significant impact on the risks they assume.

Accordingly, regulators increasingly engaged in skeptical conversations with the board and senior management on whether the organization's risk and control culture supports adherence to the board-approved risk appetite, is appropriate for the scale, complexity, and nature of its business and is based on sound, articulated values carefully managed by the leadership of the organization.

As a result, boards and senior management are considering ways to foster a stronger risk and control culture within their organization. Internal audit has a key role to play and should develop a culture assessment framework and execute internal audit activities to assess whether the prevailing risk and control culture and related processes, actions, and "tone at the top" align with the organization's values, ethics, risk strategy, appetite, tolerance, and approach.

Internal audit’s role in mergers and acquisitions

Mergers and acquisitions (M&A) are one of the highest risk activities an organization undertakes. In the past year, the volume and deal value of M&A globally have increased significantly, a trend that’s expected to continue. The principal challenge with M&A transactions is to effectively integrate across multiple dimensions to realize synergy targets, within tight timelines, while relying on resources charged with running the business as usual.

Internal audit, by virtue of its vantage point and deep competencies from a governance, risk and compliance perspective, is ideally positioned to play a key role in an organization’s M&A program. Leading internal audit departments frequently play an important role both in the pre- and post-transaction stages. Pre-transaction roles range from assessments of the overall due diligence program to active involvement in the execution of due diligence procedures. An evaluation of changes to the organization’s risk profile and related risk management activities is also often performed prior to and following M&A transactions. Post M&A activities, internal audit frequently performs activities related to post-acquisition integration and the tracking and validation of synergy capture.

Global contacts

Julie Nyang’aya
Deloitte Kenya
Partner, Enterprise Risk Services
jnyangaya@deloitte.co.ke

Rose Mwaura
Deloitte Kenya
Partner, Enterprise Risk Services
rmwaura@deloitte.co.ke

Adam Sengooba
Deloitte Uganda
Senior Manager, Enterprise Risk Services
asengooba@deloitte.co.ug

Urvi Patel
Deloitte Kenya
Director, Enterprise Risk Services
upatel@deloitte.co.ke

Edwin Odede
Deloitte Kenya
Manager, Enterprise Risk Services
eodede@deloitte.co.ke

Bernard Oketch
Deloitte Tanzania
Manager, Enterprise Risk Services
boketch@deloitte.co.tz