Deloitte.

Internal audit insights— High impact areas of focus

To be truly effective, internal audit departments should ensure that their efforts are targeted at the key risks and issues facing organizations—a task made more difficult in an environment of increasing complexity, uncertainty and change. Within this document, we share several key areas that we believe internal audit departments should consider incorporating into their audit plans.

Ethical and regulatory compliance

New regulations—and enhanced measures aimed at enforcing them—together with increased focus on ethical standards have created a multi-faceted and complex compliance challenge for many companies. Failure to address this challenge adequately may result in significant fines, penalties, and reputational damage. As a result, ethical and regulatory risks are a major discussion point within the C-suite and internal audit has a key role to play. Internal audit departments should consider structuring an assurance framework and build a range of program activities designed to evaluate ethical and regulatory compliance and promote a greater level of understanding, efficiency, and effectiveness in the organization's compliance practices and operations.

Data analytics

The explosion of technology developments and resulting volumes of data generated in many companies today have given rise to a whole new set of business risks that cannot be managed using traditional internal audit methodologies and manual sampling techniques. Data analytics is advancing in a significant way as leading internal audit departments leverage analytics to examine, sort, and transform data into useful and understandable information, which produce insights and foresights into organizational risks. By leveraging the power of analytics, internal audit can address current and emerging risks quickly, and draw conclusions that help company decision-makers take action more quickly, more confidently, and with deeper insights, thereby delivering enhanced value. More specifically, internal audit analytics can help drive a more effective, risk-based planning process by: determining which entities have greater risk and should receive more attention; and improving the efficiency, coverage, and value of discrete audit reviews.

Cloud computing

According to a 2012 global, cloud computing services report released by International Data Corporation, IT spending on cloud services worldwide is expected to exceed $40 billion this year and grow by as much as another 41% over the next four years.[1] Cloud computing represents a major change in information technology architecture, sourcing, and services delivery by giving businesses on-demand access to elastic and shared computing capabilities—thereby transforming how an organization does business. Given the access to online capabilities, cost savings, and overall sourcing flexibility gained, companies—especially small and medium-sized companies—should not ignore the potential value of this new technology. However, the adoption of cloud computing does create new risks. Typically, companies understand the risks associated with security but they also need to understand and manage other key risks the cloud may introduce, such as those associated with regulatory, privacy, data integrity, contractual clarity, business continuity, and vendor

[1] International Data Corporation, *"Worldwide Client and Server Operating Environments 2012–2016 Forecast: The Changing Dynamics and Demographics"* <http://www.idc.com/getdoc.jsp?containerId=236428> (August 2012)

management, to name just a few. Internal audit can play a pivotal role in an organization´s risk-aware migration to cloud computing services, facilitating management discussions on how to mitigate possible risks and participating directly in pre- and post-implementation reviews to assess the extent to which key risks are being appropriately managed.

Social media

Increasingly, business decision-makers are aware of the inherent risks associated with social media use—from privacy issues to hacking threats and potential reputational damage. These are some of the downside risks of social media, but what about the upside risks—that is, the risk of not capitalizing on the many benefits of social media? Appropriate and managed use of social media may enable interactions with stakeholders that foster creativity, innovation, customer loyalty, improved service, and brand promotion. The question becomes, is your company harnessing the potential of social media to achieve your strategic objectives, while also doing all it can to avoid pitfalls and protect valued assets? Internal audit departments should consider a broad social media assessment that has the dual objectives of both protecting and enhancing value for your organization by determining where the organization stands in terms of both upside and downside social media risk-taking.

Cyber crime

The rise of the sophisticated cyber criminal has become one of the fastest growing security threats to organizations. The cyber crime landscape features malware exploits that can routinely evade traditional security controls. The reactive attack and penetration approaches of the past may no longer be sufficient to deal effectively with this level of ingenuity and are being replaced with new forms of cyber intelligence capable of enhancing traditional security programs. Adding a layer of complexity to the issue is the rise of social networking, online communications, and online financial transactions. Internal audit has a significant role to play in identifying exposures and helping management address cyber vulnerabilities.

Software asset management

Software purchases account for a significant portion of many companies' 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. As a result, many companies, during routine audits, are found to be either under-licensed or over-licensed for the software they are currently using. Under-licensing can create significant financial, legal and reputational risk while over-licensing means that the company is paying excessive license costs. Proper management of software assets can help companies pay the requisite amount for their software. Internal audit departments are responding to these risks by executing software asset management (SAM) operational audits. These audits use experienced SAM professionals and include the following components: process risk assessments, software license baselines and software risk assessments, combined with insightful analysis and recommendations, including remediation activities and projects.

Auditing the risk management function

Risk management departments play an important role within organizations as they work with management and Boards of Directors to identify key risks and to manage and monitor those risks in accordance with the organization's risk appetite and tolerances. As the organization's "third line of defense," internal audit is counted on to provide independent assurance with respect to the effectiveness of the risk management program. In fact, the Institute of Internal Auditors Standard 2120 requires "the internal audit activity to evaluate the effectiveness and contribute to the improvement of risk management processes.[2]" Although these processes are assessed through ongoing audit activities, internal audit should also conduct regular and formal audits of an organization's risk management function and program, given the critical role that risk management

[2] The Institute of Internal Auditors, *"International Standards for the Professionals Practice of Internal Auditing (Standards),"* < https://na.theiia.org/standards-guidance/mandatory-guidance/pages/standards.aspx>

plays within the organization. Auditing a company's risk management function encompasses an assessment of the quality and effectiveness of risk management efforts, including the overall approach to risk issues, risk identification, risk reporting, the role of risk owners, methodologies, and supporting tools. Assessments often take the form of a gap analysis leveraging leading industry practices, recognized risk frameworks (such as the ISO 31000[3] or Deloitte's[4] Risk Intelligent Framework[5]), and capability maturity models.

Global IA fraud prevention controls

A number of internal audit departments are increasingly interested in fraud and bribery prevention and detection controls, particularly as they relate to overseas subsidiaries. To say that the enforcement landscape has been stepped up would be an understatement. Prosecutions and fines under the Foreign Corrupt Practices Act (FCPA)[1] (which makes it illegal for U.S. citizens or companies to attempt to bribe foreign officials in order to gain a business advantage) have increased dramatically in recent years. While the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) had only five enforcement actions in 2004, that number rose to 40 actions in 2009 and 74 in 2010. Japan's "J-Sox"[2] requirements and the U.K. Bribery Act of 2010[3] are two other major examples of related regulations on a global scale. In Deloitte's experience, fraud and anti-corruption risks often do not receive proper attention from management which may lead to significant financial, compliance and reputational consequences should unfortunate incidents occur. More and more, internal audit is expected to assess key fraud and anti-corruption risks and determine whether risk exposures exist.

Capital project reviews

Organizations are becoming increasingly aware of the potential impact of poor capital project management and execution on success and the bottom line. For years, capital projects have been behind schedule and fraught with cost overruns. The economic challenges, however, in many markets, has once again shone the spotlight on these projects, causing organizations to scrutinize key elements of capital projects, specifically cost and schedule. Each year, many organizations expend substantial sums of money through various types of contractual agreements; however, the contracts underpinning these arrangements are often vague, misinterpreted, or inadequately monitored. Frequently, risks exist such as erroneous or duplicate contractor charges, excessive contractor time and inadequate processes associated with the monitoring of capital costs. Given the significant value at stake and the associated risks, Internal Audit functions should play a key role in contract risk and compliance activities to identify opportunities for cost recovery and to provide valuable insights and recommendations to improve processes and controls. Traditional vendor and/or contract compliance reviews can be tedious, time-consuming, and potentially ineffective in identifying root cause issues associated with cost and schedule overruns. Successful and highly

---

[3] International Organization for Standardization, "ISO 31000:2009, *Risk management—Principles and guidelines,"* <http://www.iso.org/iso/home/standards/iso31000.htm>

[4] As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see **www.deloitte.com/us/about** for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

[5] Deloitte Touche Tohmatsu Limited, " Risk Intelligence: A board imperative," <https://www. deloitte.com/ view/en_US/us/Insights/Browse-by-Content-Type/podcasts/ ab7f8ed50ecfe210VgnVCM1000001a56f00aRCRD.htm>

[1] Congress, *"The Foreign Corrupt Practices Act of 1977* (FCPA)," (Washington, D.C. 1977) <http://www.justice.gov/criminal/fraud/fcpa/statutes/regulations.html>

[2] National Diet of Japan, *"The Financial Instruments and Exchange Act,"* (Japan, June 2006) <http://www.fsa.go.jp/en/policy/fiel/index.html>

[3] Parliament of the United Kingdom, "the Bribery Act of 2010," (London, England 2010) <http://www.legislation.gov.uk/ukpga/2010/23/contents>

effective Internal Audit groups are using advanced tools, such as data analytics, across the end-to-end capital project life cycle to provide the organization with deeper insights and real-time monitoring of key risks to help promote more effective capital project planning and execution.

People Risk

Talent plays a most critical role in driving and sustaining business performance and Human Resources plays a key role in building the talent pool and creating the talent experience for an organization through attracting, developing, and retaining the right talent to execute on the business strategy. In fact, leading organizations consider talent as part of their overall risk management efforts, and are increasingly ranking leadership and talent risks among the top potential threats to success. Talent is one of the hardest assets to put effective controls around. An audit of the HR function and talent management practices may validate whether an effective talent strategy is in place, supports the overall business plan, and is being executed appropriately. Additionally, it can help ensure people-related risks tied to areas like succession, leadership development, talent acquisition, critical workforce segments, talent shortages and workforce planning are identified and proactively planned for and managed before issues occur. Internal audit reviews often include a comparison to leading industry practices, capability maturity models (e.g., Deloitte's Talent Maturity Model), and an assessment of compliance with policies and relevant labor legislation.

Global contacts

Terry Hatherell
Deloitte Canada
Global Internal Audit Leader—Americas
thatherell@deloitte.ca

Porus Doctor
Deloitte India
Global Internal Audit Leader—Asia Pacific
podoctor@deloitte.com

Wim Eysink
Deloitte Netherlands
Global Internal Audit Leader—Europe and the Middle East
weysink@deloitte.nl

Sarah Adams
Deloitte Mexico
Global IT Internal Audit Leader
saraadams@deloittemx.com

Sunita Suryanarayan
Deloitte & Touche LLP
Global Internal Audit Analytics
ssuryanarayan@deloitte.com

Doug Wilkinson
Deloitte Canada
Global Controls Transformation & Assurance Leader
douwilkinson@deloitte.ca