Deloitte.

# CFO Insights

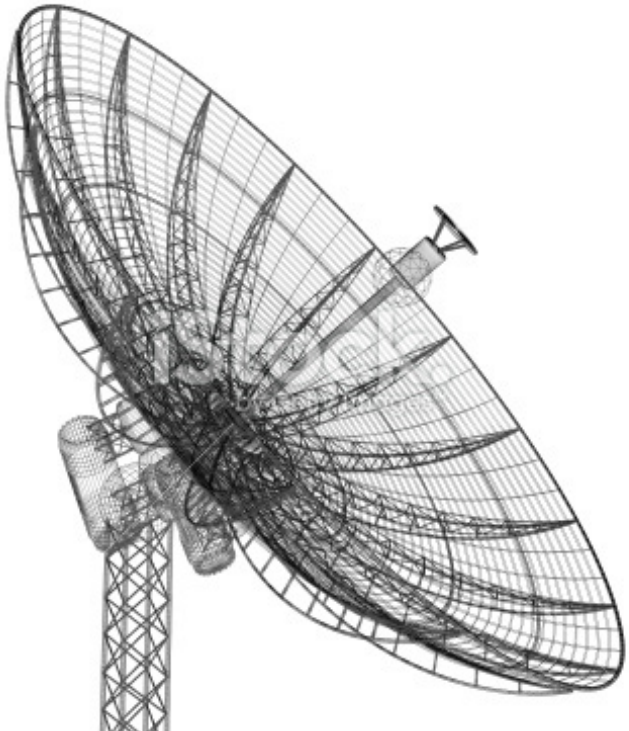
## Can internal audit be a command center for risk?

Traditionally, internal audit (IA) has served as the independent eyes and ears of boards and management, both in terms of risk oversight and compliance. But given the deluge of risks companies now face along with continuously evolving regulation, there is an opportunity for IA to move beyond its scouting role and serve as an integral part of the team for identifying and combating risk.

Given its cross-functional lens, IA is in a position to do just that. To do it effectively, however, requires leveraging innovative techniques, such as data analytics and predictive modeling, to identify emerging risks and allocate resources to maximize coverage. In addition, IA needs the support of management and the audit committee to move to a higher-value role, as well as the talent to deliver more than customary audit findings.

For CFOs, the benefits of a highly evolved IA function are multifold. With IA process costs for the *Fortune* 500 representing between 0.026% and 0.126% of revenue (variable based on company size, industry, and adoption of leading practices),[1] extracting greater value from such an investment is paramount. Moreover, since many chief audit executives (CAEs) still report administratively to the CFO (70% in the *Fortune* 500, according to the 2013 Global Audit Information Network Annual Benchmarking Survey[2]), it behooves finance to equip the function with capabilities to deliver more-informed audit reports. And given the continuing desire of CFOs to play more-strategic roles, having a forward-looking IA department can be a valuable weapon in their arsenal.

In this issue of *CFO Insights*, we'll look at specific areas where internal audit can add additional value, and offer questions that can lead to IA becoming more of a command center for risk.



### Leveraging tools and techniques

Internal audit has undergone several evolutions in recent years. In the mid-2000s, corporate adherence to the Sarbanes-Oxley Act increased demand for many internal auditors—and their focus on compliance testing and financial controls. Since then, though, many companies have tended to see it as both a risk and a business-consulting function. That is not every company's view, of course, but two forces are pushing the transformation forward:

**Technology enablement.** As in most areas of an organization, new technologies are increasing the speed of delivery and allowing better insights. In IA, in fact, the use of technology is increasing the impact of audit findings through, for example, data visualization. In addition, other techniques are making reports more timely and accessible. Continuous auditing, for example, which is an automated approach, enables auditors to continually gather critical data that supports and enhances the audit, rather than the historical norm of examining limited samples. That means executives can pinpoint and act on, say, inventory issues, in real time instead of inferring potential issues and relying on reports based on outdated information.

**Data analytics.** The data captured by new technologies can help IA and the business know where the risks are, how to prioritize them, and how to better focus audits and management's efforts to mitigate risks. For example, regression testing and predictive modeling can allow CFOs and auditors to quickly identify anomalies. Specifically, advanced-analytic and data-modeling techniques that use self-learning algorithms can automatically categorize anomalies within a wide range of variables to identify higher-risk audit entities. Analysis of this nature can then help direct audit activity toward areas of greatest risk. Particularly effective across geographic locations and overseas operations, it has also been used to analyze areas as diverse as revenue leakage, compliance risks, and other enterprise risks.

By leveraging the necessary technology and data, IA can contribute insights such as the following:

1. **Cyber-risk.** In the United States, the average cost of a data breach is $188 per lost or stolen record, or an average of $5.4 million per organization breached.[3] Understanding the risks involved with protecting company assets and containing such costs is obviously top-of-mind for CFOs. In addition to an effective risk management program, which includes cyber-security education programs and monitoring, IA can help the organization better understand its preparedness by using analytics to detect breach patterns and reviewing cyber-controls in a regular cadence.

2. **Strategic risk.** According to a recent Deloitte Touche Tohmatsu Limited (DTTL) global study, strategic risk has become a major focus, with 81% of surveyed companies now explicitly managing strategic risk—rather than limiting their focus to such traditional areas as operational, financial, and compliance risk.[4] But understanding how IA can help flag risks related to strategy is often out of IA's comfort zone. Still, if IA has a seat at the executive table, it is in the position to report when strategy is not well understood throughout an organization, which may lead to decisions that are not in accordance with overall strategy.

3. **Investment risk.** In the most recent *CFO Signals*™ survey, CFOs noted that more than half of their capital expenditures would be slated for growth and innovation (37% and 14%, respectively).[5] Traditional audit techniques to determine whether the related investment projects were successful would favor a historical approach. But by using predictive models, internal auditors today can help teams improve the likelihood of a project being delivered successfully: on-time, on-budget, and meeting the specification and business requirements.

## Strengthening IA's value

When it comes to IA, certain attributes are table stakes. For example, one of internal audit's main jobs is to execute a strong risk-assessment process that drives its audit process and resource allocation. And it is the audit committee's job to make sure IA is properly funded and resourced as effectively as possible. But there are questions finance chiefs can ask to help guide IA to becoming a more value-creating organization, particularly around risk identification and mitigation. For example:

**Are internal audit personnel experts in their field, and can they proactively consult on internal controls and risk management?** With the introduction of Sarbanes-Oxley, IA specialists became some of the most sought-after talent in business. But to add additional value, IA needs to team with others in risk management, including legal and IT, to proactively monitor whether management is tackling risk-mitigation plans. In addition, IA has to have the flexibility—and the resources—to bring in appropriate specialists to supplement their teams as needed.

**Is the internal audit process designed to identify whether the organization is controlling those areas that are important to control and not just what is easy to control?** Because IA is one of the only functions with a companywide perspective, it has the ability to access all aspects of the organization and identify anomalies. By working closely with finance and the business units, IA can prioritize which risks to deal with first and create resource allocation plans to ensure that the most significant risks are properly mitigated.

**Internal Audit in the cloud**

Cloud computing has taken the business world by storm—and with it comes a potential deluge of risks. As confidentiality, security, service continuity, and regulatory compliance become even more critical in the digital enterprise, what role should internal audit (IA) play in addressing these risks?

"Cloud computing presents a new frontier for many organizations—and for IA as well," notes Michael Juergens, principal, Deloitte & Touche LLP. "When a company opts for the speed and convenience of moving to the cloud, for example, it often relinquishes control not only of its own data, but that of its customers. For internal auditors, meeting the challenges of cloud computing may mean stretching beyond their traditional audit roles, adding greater value as they assist the organization in building the required control environment."

Specifically, IA should make sure it understands the organization's current cloud footprint, conducts cloud audits by starting at the procurement process, and recognizes the conditions that prompt business users to bypass the IT shop and sign up for cloud services directly. It should also develop and leverage a customized framework tool to help identify the organization's top cloud risks and drill down to key statements. Such a tool, which is outlined in Deloitte's "Will risk rain on your move to the cloud?" can get to the heart of risks by providing a view on the pervasive, evolving, and interconnected nature of risks associated with cloud computing. "These risks range from governance and compliance to infrastructure security and from data management to IT operations," notes Khalid Wasti, director, Deloitte & Touche LLP.

**Cloud risk framework: A recommended approach**

| Cloud risk framework<br>Incorporating a range of interconnected risks: | | |
|---|---|---|
| Governance, risk management, and compliance | Delivery strategy and architecture | Infrastructure security |
| Identity and access management | Data management | Business resilience and availability |
| IT operations | Vendor management | Business operations |

In addition, there are several proactive steps IA functions should consider as the organization adopts cloud computing initiatives:

* Engage stakeholders in informed discussions about the risk implications of cloud computing.
* Review the current organizational risk framework based on cloud risks that have been identified.
* Develop risk-mitigation strategies to help minimize the risks that accompany cloud computing.
* Review and better understand the organization's data governance program, as this is a key component in the treatment of data in the cloud.
* Evaluate potential cloud vendors from a risk perspective.

"Cloud computing is changing the technology landscape, and the changes are only likely to intensify," notes Charlie Willis, senior manager, Deloitte & Touche LLP. "For many organizations, the question is not whether the cloud should be part of their technology strategy, but when and how." Under pressure to provide solutions, organizations may be tempted to leverage cloud services quickly, without weighing the associated risks. As the third line of defense, IA can help provide the context and risk framework an organization should consider when moving to the cloud.

**Have the audit committee, senior management, and the CAE reconciled their expectations for internal audit?** IA can't evolve into a higher-level organization without support. If the board wants IA to solely focus on financial controls and compliance, and management wants it to focus on finding process improvement, there is obviously a role gap. Consequently, it is important to clarify the role up front—through direct dialogue—so IA knows how much of its time and resources should be spent on basic block-and-tackle activities and how much on consulting-type activities, such as emerging risks and efficiencies.

**Is internal audit focused on the right risk areas?** The internal audit team should go beyond focusing primarily on financial reporting risks and evaluate current and prospective risks, including strategic, reputational, operational, financial, legal, IT, and compliance risks. For example, if the company is planning an acquisition in Bangalore, IA should be involved in assessing risks associated with setting up operations and securing licenses there.

**How does internal audit relate to, and interact with, other risk-related functions, such as enterprise risk management, strategic planning, legal, security, and IT?** To truly create value, IA needs to work cross-functionally and with the right subject-matter specialists related to the particular risk. In addition, IA needs to be aligned with the executive team, the chief risk officer (if the organization has one), and the overall risk management organization. Where IA focuses on assessing—not administering—the robustness and effectiveness of the programs that the organization has around risk, teaming with the appropriate risk function can lead to more-holistic audits and better risk mitigation.

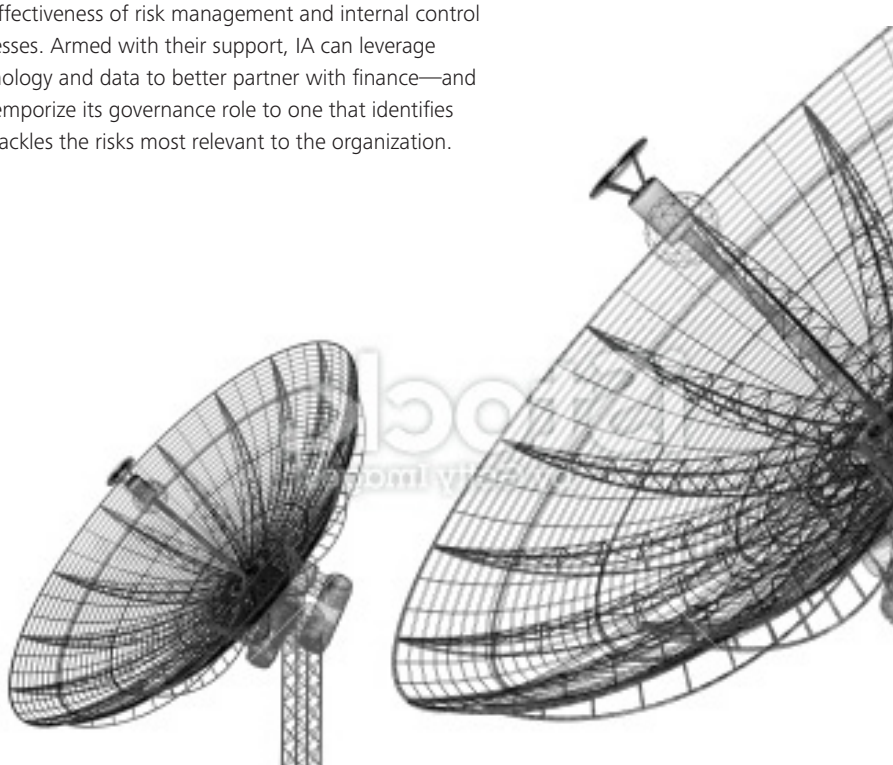
**Is the internal audit department viewed as objective and competent by management and the independent auditors?** Equipped with data analytics and visualization, IA's reputation can only be enhanced. For example, new forms of communication that capture on one page the greatest risks the company faces will be embraced by both boards and senior executive teams. They want to know what the major risks are and which ones to act on—not a 30-page report filled with details that get in the way of action. As for external auditors, working with an IA organization that roots out and controls for emerging risks can lead to more-efficient audits and better working relationships.

### Choosing to be value-creating

In IA, delivering audit "findings" has typically been a measure of success. But preventing those findings from occurring in the first place should be just as valued. To get to that mind-set, however, requires even more than leveraging technology and data to better partner with finance; it also requires added IA skills, and sometimes a culture shift.

Specifically, to be a command center for risk, IA has to add the necessary modeling and analytical skills to its working knowledge of internal controls and risk management approaches. In addition, IA professionals need to move out of their comfort zone and focus on identified risks and resolve not to be satisfied with average performance. Moreover, finance and the audit committee should both expect IA to perform at a higher level and equip it with the resources and the mandate to do so.

Audit committees and senior management rely on internal auditing for objective assurance and insight on the effectiveness of risk management and internal control processes. Armed with their support, IA can leverage technology and data to better partner with finance—and contemporize its governance role to one that identifies and tackles the risks most relevant to the organization.



**Primary Contacts**

**Carey Oven**
AERS Partner
Deloitte & Touche LLP
coven@deloitte.com

**Sandy Pundmann**
AERS Partner
Deloitte & Touche LLP
spundmann@deloitte.com

**Neil White**
AERS Principal
Deloitte & Touche LLP
nwhite@deloitte.com

Deloitte *CFO Insights* are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; and Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP.

**About Deloitte's CFO Program**

The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career—helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's CFO Program, visit our website at: www.deloitte.com/us/thecfoprogram.

**End notes**

1 "Summary information," 2013 Global Audit Information Network (GAIN) Annual Benchmarking Survey, The Institute of Internal Auditors.

2 "CAE Administrative Reporting Line," 2013 Global Audit Information Network (GAIN) Annual Benchmarking Survey, The Institute of Internal Auditors.

3 Data collected from the Ponemon Institute research report: 2013 Cost of Data Breach Study: Global Analysis, 2013.

4 "Exploring Strategic Risk," DTTL and *Forbes Insights*, 2013.

5 *CFO Signals,* Q1 2014; U.S. CFO Program, Deloitte LLP.