Top 10 in 2013: Internal audit considerations for technology companies
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>New sources of revenue growth</td>
<td>2</td>
</tr>
<tr>
<td>Managing costs</td>
<td>5</td>
</tr>
<tr>
<td>Information technology</td>
<td>6</td>
</tr>
<tr>
<td>Risk management/Regulatory compliance</td>
<td>8</td>
</tr>
</tbody>
</table>
Our annual compilation of internal audit considerations for technology companies, “Top 10 in 2013,” focuses on the critical role internal audit can play in helping companies manage some of their leading risks more effectively in today’s dynamic environment.

As we enter 2013, we continue to see a variety of mixed economic indicators. In response, technology companies are reinventing themselves through multiple means including continued international expansion, outsourcing/shared services, and mergers and acquisitions. Companies are also continuing to invest in new technologies and business models, such as cloud, mobility, and digital products and services. We see a corresponding focus in these transformational areas from an internal audit perspective.

Our selection of risk areas is based on a number of inputs, including:

• Discussions with chief audit executives at technology companies
• KPMG’s Technology Internal Audit share forum
• Insights from KPMG professionals who work with technology companies
• KPMG survey data

You will see that many of the areas of focus are consistent with those in 2012; however, we have seen new emphasis placed in areas such as corporate social responsibility and mobile platform security risks.

The projects on the following pages focus on some of the risks technology companies face as they evaluate their strategies and make investments in the following areas:

• New sources of revenue growth (international operations, third-party relationships, and mergers, acquisitions and integration)
• Managing costs (outsourcing, offshoring and shared services)
• Information technology management (information security and privacy, business continuity management, and IT disaster recovery)
• Risk management and regulatory compliance (Foreign Corrupt Practices Act (FCPA) and anti-bribery and corruption, intellectual property protection, talent management, retention and succession planning, and corporate social responsibility).

These areas highlight the leading exposures companies are working to address as they invest in innovation and pursue revenue growth.
International Operations (high-growth, high-risk areas)

Drivers:

- Enhancing oversight and visibility into international operations
- Achieving greater confidence in the propriety of local business practices and compliance with corporate policies and regulations (e.g., FCPA)
- Increasing consistency of policies and procedures across locations
- Reducing risk of noncompliance with export laws and regulations
- Enhancing controls, and global export and sanctions, compliance processes.

A continued key driver for technology companies is international market expansion. Many technology companies are exploring global opportunities for revenue generation and operational efficiencies. International operations, however, lead companies to have concerns around product quality, protection of intellectual property (IP), and anti-bribery and corruption. Additional risks include inconsistency of business practices, inadequate corporate oversight, and complicated and changing legal and regulatory requirements. Another key challenge technology companies face is complying with myriad sanctions, export laws, and regulations from cross-border trade.

Areas that internal audit can examine during an international operations review include:

- Overall key process areas and control environment, including compliance with U.S. and local requirements (such as import and export regulations)
- Business practices, potential code of ethics, and anti-bribery and corruption issues among a foreign entity or partners
- Communication of the company’s risk and controls to international employees
- Financial processes of business units to ensure consistency with corporate policies and procedures
- Documented policies and procedures for export controls and sanctions compliance
- Export transactions and global trade automation system, and controls to safeguard export-controlled technology.
Third-party relationships (e.g., channel management, vendor management, royalties, etc.)

Drivers:
- Increasing revenue and cost reduction
- Improving contract governance
- Creating more effective contractual self-reporting processes
- Enhancing relationships with business partners.

For many technology companies, revenue can disappear or costs can increase unnecessarily because vendors, distributors, and licensees fail to meet their contractual obligations. Business partners may not mean to do so deliberately, but can fall short due to the complexity of the environment or their agreements. Third parties often work under highly complex contracts in which requirements are not identified clearly or key responsibilities are overlooked. In addition, contracts may not reflect changed circumstances. No matter the reasons, the need to manage risks related to third-party relationships is critical for technology companies to regain full control over their costs and revenue.

Example activities for internal audit to consider include:
- Reviewing third-party identification, due-diligence, selection, and on-boarding processes and controls
- Conducting a leading practices study on the organization’s channel strategy, effectiveness and compliance
- Conducting vendor audits that focus on compliance and effectiveness
- Reviewing the processes and controls over data that is self-reported by third parties
- Developing, implementing and calibrating a continuous monitoring system of self-reported data from vendors and channel partners.
Mergers, acquisitions, and integration

Drivers:

• Implementing a more rigorous and better-controlled M&A program

• Obtaining validation of deal risks and expectations before they are communicated to stakeholders

• Enhancing execution planning, delivery, and performance tracking

• Improving integration processes across all key functions.

A need to manage execution risk more effectively is also leading many companies to design additional rigor into their merger and acquisition programs to help ensure a fact-based and well-controlled diligence, valuation, integration planning, and execution process.

Example activities for internal audit to consider include:

• Performing “post mortem” reviews on prior deals to assess the effectiveness of existing processes and playbooks

• Reviewing M&A playbooks, which document integration processes and should be customized to reflect the existing company culture, business processes, and governance

• Understanding communication processes between finance, internal audit and deal teams to assess control implications of executing business process change during active integrations

• Performing a project risk assessment review of the business integration process, focusing on potential risks, integration success metrics, and information systems.

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International. NDPPS 136331
Outsourcing, offshoring, and shared services

Drivers:

- Transforming and managing business services to operate more efficiently by employing leading industry practices across shared services, outsourcing, and governance
- Improving program governance, decision making, and sourcing relationship performance
- Enhancing delivery models
- Improved monitoring, measuring, and reporting of performance and achievement of expected benefits.

Pressures to reduce costs by either outsourcing (e.g., engaging external service providers to assume activities traditionally performed within the company) or offshoring (e.g., moving processes to centers outside the originating country to be managed by an internal or external service provider) are expected to continue in 2013.

Example areas where internal audit can assist management include:

- Assessing program governance and sourcing partner selection processes, including reviewing RFP content, selection methodology and criteria, parties involved, and other factors
- Assisting and reviewing transition activities, including implementation plans, controls, methodologies, ongoing transition monitoring, and performance results
- Reviewing ongoing key service management factors including service-level agreements, performance metrics, and performance management processes and procedures
- Reviewing postimplementation benefits monitoring and realization to help management determine whether estimated benefits have been achieved.
Information security and privacy

Drivers:
- Enhancing risk mitigation through a more comprehensive and structured information security and privacy management approach
- Improving compliance with regulatory and legal requirements, as well as with Sarbanes-Oxley
- Reducing reputational risk associated with denial of service attacks, privacy breaches and other security-related weaknesses
- Ensuring personally identifiable information (PII) is protected as business models evolve.

As companies manage through the impact of continued globalization and economic recovery, an increased sense of urgency has emerged surrounding information security and privacy. If privacy and security are not addressed, organizations can be exposed to a host of risks ranging from the breach of personal information, which may lead to identity theft and access management issues as well as to availability and company reputation damage.

With the increased use of cloud, mobile, and social platforms, companies need to ensure data is protected. Companies now face an increased security risk, which is why it is important to align controls to the changing environment to protect data.

Areas that would be examined by internal audit during an information security and privacy review may include:
- Security monitoring and detection programs, as well as controls with a focus on Security Incident Event Monitoring (SIEM)
- Programs for data breach notification as required for regulatory and legal compliance
- Access governance program, process, and controls to help ensure inappropriate access is not permitted
- Management sponsorship of security and privacy programs, and level of awareness training (e.g., password protection, information risks, and appropriate handling of confidential customer/employee information)
- Security audits around cloud and social platforms.
Business continuity management and IT disaster recovery

Drivers:
- Mitigating risk due to business interruption
- Mitigating risk to employee safety and the organization’s profitability
- Improving compliance with regulatory and legal requirements.

Business Continuity Management (BCM) is gaining in prominence as the focal point in managing enterprise risks. BCM is viewed by organizations as an effective way to instill resiliency in an organization’s people, processes, and technology infrastructure, and as an effective tool to help ensure the continuity of business operations in the face of a natural or man-made disaster. Companies should consider mitigation plans for situations such as disasters, data security attacks, macro-economic crises, and other potential disruptions.

Areas that could be examined by internal audit during a business continuity management review include:
- The maturity of the business continuity program, including a remediation plan to mitigate risks and a benchmark comparison against companies of similar size and industry peers
- Audit of Business Continuity Program elements such as risk assessments, business impact analyses, continuity strategies, IT disaster recovery, and crisis management plans to determine if plans are current and would be executable in a disaster situation
- The effectiveness of business continuity training and awareness programs
- Business continuity and IT disaster recovery exercises.
Top 10 in 2013: Internal audit considerations for technology companies

Foreign Corrupt Practices Act (FCPA) and Anti-Bribery and Corruption (ABC) compliance

Drivers:

• Improving risk assessment of noncompliance with applicable ABC laws

• Mitigating reputational, financial, and business harm associated with potential noncompliance through effective compliance programs

• Optimizing use of third-party due diligence, communications, and compliance audits.

Thirty-five years after its enactment, the FCPA continues to cause concern for corporate boards of directors. The threat of costly investigations, multimillion-dollar settlements, imprisonment, and litigation guarantees the FCPA will continue to command significant attention from companies doing business internationally. Companies need to continue FCPA compliance efforts given continued globalization, the changing landscape of anti-bribery and corruption laws abroad, and steady regulatory activity.

A robust and effective anti-bribery and corruption program can help shield a company from the most severe consequences of an FCPA violation. The U.S. Securities and Exchange Commission, as well as the Department of Justice, have historically considered several factors in determining an appropriate response to FCPA violations, including cooperation, self-reporting of potential violations, and the quality of the organization’s ethics and compliance program.

For multinational companies, the U.S. FCPA is but one of a growing number of anti-bribery and corruption laws and regulations to be mindful of. A growing number of countries have enacted, or are in varying stages of enacting, their own anti-corruption legislation. While the international community appears to be coalescing in support of outlawing bribery, the global enforcement landscape is becoming more complex.

Internal audit can help organizations, officers, and employees understand, assess, and mitigate bribery and corruption risk by assisting with the following:

• Facilitation of global bribery and corruption risk assessment

• Assisting in the development of data analytics to monitor bribery and corruption risk, including third-party risks

• Proactive investigation into exceptions flagged by continuous monitoring or look-back data analytics

• Reactive investigation into matters involving potential noncompliance

• Testing of anti-bribery and corruption controls, and incorporating bribery and corruption procedures into routine internal and third-party audits

• Assessment and evaluation of anti-bribery and corruption program

• Developing and delivering bribery and corruption policy training.
Intellectual property protection

Drivers:
- Achieving protection of IP assets from loss or overuse
- Ensuring IP management processes are in line with internal and external compliance requirements.

Every day, businesses lose countless dollars without even realizing it. In many cases, revenue can vanish because vendors, distributors, and licensees unintentionally fail to meet contractual obligations. Today, intellectual property (IP) is at the core of many business relationships. As business increasingly takes place through a network of separate entities—joint ventures, alliances, and less-structured arrangements—IP makes it possible to share intangible assets in an effective ecosystem that spans the globe. Many organizations license their valuable intellectual property—trade secrets, designs, patents, and trademarks—or share them with other third parties (e.g., vendors for use in contract manufacturing or channel partners for co-marketing efforts).

IP-related risk can stem from highly complex contracts that do not identify key requirements or responsibilities clearly, or from changed circumstances, mistakes, or deliberate misstatements, but managing IP means more than enforcement. IP can be sold or licensed for revenue, to support tax-efficient structures or as collateral for borrowing. Whatever the situation, the need to manage risks related to third-party IP relationships is critical to delivering significant bottom-line benefits.

Internal audit can support these efforts by monitoring the compliance of third-party IP contracts (both internally and externally) to help protect the bottom line and nonfinancial impacts (e.g., unlicensed transfer of IP to restricted countries).
Talent management, retention, and succession planning

Drivers:

- Increasing awareness and adherence to policies and procedures around recruiting, on-boarding and off-boarding
- Improving employee morale and productivity through adoption of leading practices around recruitment, retention, learning, and development programs
- Reducing risk of losing top talent or being unprepared for the loss of top talent
- Enhancing alignment between employee and company goals.

Technology companies face the challenge of meeting ever-changing workforce expectations and ensuring the right talent is hired, retained, motivated, and developed to help the company achieve its business objectives and strategies. Companies also need to evaluate risk mitigation plans for top talent departures.

Internal audit can assist management with these challenges by assessing the following:

- The on-boarding process for employees, contractors and temps, focusing on areas such as security and background checks, employee agreements, buddy assignments, and education of health and safety, emergency management, code of conduct, and other key policies and procedures (e.g., security, computer use, approvals and delegations, leave, travel, expense claims)
- Training and development programs, including processes for ensuring programs are adequately targeted to meet management’s and staff’s learning and development needs, and tied to wider business objectives, as well as processes for identifying and developing managers, leaders, and high performers across the organization
- Recruitment and retention processes, including need identification and requisition, position descriptions and requirements, selection and interview, use of recruitment suppliers, recruitment incentives, offers and acceptance, delegated authority, and employee retention programs
- Performance and career management framework and processes, including identification of high-impact employees, goal development, linkage of individual goals to company objectives, and processes for monitoring, evaluating and reporting performance
- Succession planning process for key executive positions and high-impact employees, including critical role vulnerability analysis, and internal vs. external recruitment to fill critical roles
- Compensation strategy and structure, and benefits and reward programs, including market positioning and competitor benchmarking, signing bonus and referral payouts, relocation allowance payouts, and rewards
- Off-boarding and exiting processes, including resignations and acceptance, exit interviews (reason analysis), department clearance, and full and final settlement.
Corporate social responsibility

Drivers:

- Mitigating ever-changing and emerging risks, including an evolving and increasingly complex regulatory environment
- Reducing costs and driving business value through improved quality and service
- Generating new revenue streams
- Stimulating innovation in new products and services, business processes and efficient facilities
- Increasing workplace productivity, employee attraction and retention.

Businesses today are operating in an ever-more interconnected and globalized world. Greenhouse gas emissions, energy prices, toxic ingredients in products, and access to water and raw materials are increasingly seen as material risk factors that warrant scrutiny by shareholders, customers, and regulators. The demand for increased transparency and disclosure of nonfinancial information means companies are under growing pressure to produce reliable and accurate information, not only for their own operations but also for their supply chains.

Increased focus by nongovernmental organizations and the rise of sustainability ratings and stock indices such as the Dow Jones Sustainability Index are elevating the scrutiny of nonfinancial data and reporting to the board and the C-suite. Internal audit has a key role in mitigating the risks and enhancing the opportunities that a sustainability focus brings to an organization beyond the next quarter’s results.

In addition to environmental considerations, the social dimension of sustainability affects an organization’s impact on the communities and societies in which it operates. The social dimension warrants consideration of labor practices (health and safety, training and education, quality of the work environment), human rights and societal and community aspects. Many of these considerations are not easily quantifiable.

Section 1502 of the Dodd-Frank Act, Conflict minerals, and the 2012 California Supply Chain Transparency Act are recent examples of legislation requiring companies to make certain disclosures concerning the supply chain to state and federal agencies such as the Securities and Exchange Commission (SEC). These disclosures relate to the source of conflict minerals and a company’s measures to address conditions of forced labor, slavery, human trafficking, and child labor within their supply chains.

Internal audit can assist management with these challenges by assessing the following:

- The company’s sustainability strategy, its alignment with the company’s corporate strategy, and related risks
- Gaps and opportunities with respect to operational procedures and controls for environmental and social compliance with laws and regulations including the supply chain
- Environmental and social risks, and alignment with Enterprise Risk Management (ERM).

(continued on the next page)
• Processes and controls for carbon, water, and waste data and metrics to determine areas for improvement, gaps and opportunities from a people, process and technology perspective, and readiness for attestation
• Institutionalize processes that help companies prepare, monitor, and report on compliance issues such as conflict minerals
• Design and procurement of an environmental management information system (EMIS).

About KPMG

KPMG: An experienced team, a global network

KPMG’s Internal Audit technology professionals combine industry knowledge with technical experience to provide insights that help technology leaders take advantage of existing and emerging technology opportunities and proactively manage business challenges.

Our professionals have extensive experience working with global technology companies ranging from Fortune 500 companies to pre-IPO start-ups. We go beyond today’s challenges to anticipate the potential long- and short-term consequences of shifting business, technology and financial strategies.
Contact us
For more information about this study, or about KPMG’s Technology practice and capabilities, please contact the following

**Tom Lamoureux**
Principal, Risk Consulting Industry Leader—Technology, Media & Telecom
T: 206-913-4146
E: tlamoureux@kpmg.com

**Ron Lopes**
Partner, Advisory
T: 408-367-7615
E: rjlopes@kpmg.com

kpmg.com