KPMG

# Internal audit: unlocking value for technology companies

## Top 10 internal audit considerations for technology companies in 2016

kpmg.com

**Our annual edition of the top 10 internal audit considerations for technology companies outlines the critical role internal audit holds in helping technology companies manage some of today's most important risk areas more effectively and unlock underlying value for the company in the process.**

The 10 focus areas explore some of the leading risks technology companies face as they strategize and make investments.

KPMG LLP's (KPMG) selection of consideration 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, including a recent study, "Seeking value through internal audit," in which KPMG and *Forbes* surveyed more than 400 chief financial officers and audit committee chairs to identify the insights internal audit functions are providing as well as opportunities where internal audit organizations can improve.

Note: Every technology company is unique and it is important that internal audit rely on a company-specific analysis of its risks in developing its internal audit focus areas.

## Top 10 in 2016

01

# Cybersecurity

**Drivers:**

- – Avoiding costly consequences of data breaches such as investigations, legal fines, coverage of customer losses, remediation efforts, loss of executive and mid-level time and focus, and potential loss of customers and business
- – Averting reputational damage to the organization, especially with regard to lost customer data
- – Preventing loss of intellectual property and capital and other privileged company information

Cybersecurity is a key focus point for many technology companies, shifting beyond headline news to the top of many board agendas. Several factors have driven the increased attention paid to cybersecurity issues, including rapid shifts in technology and the threat landscape, more stringent and diverse regulatory environments, social change, and changes in corporate culture.

The capabilities and techniques used by hackers evolve continuously, especially in targeting specific information or individuals. New methods are constantly being developed by increasingly sophisticated and well-funded hackers — including organized crime, nation states, hacktivists and insiders — who can target companies not only directly, but also through social engineering, phishing scams, and connections with key suppliers and technology partners.

The consequences of lapses in security can be disastrous as an organization's bottom line and reputation are impacted. It is critical for technology companies to remain vigilant and up to date on emerging threats and protection criteria.

Internal audit can execute technical and process-driven assessments to identify and evaluate cybersecurity risks, and offers strategies and recommendations to help mitigate the identified risks.

**Example focus areas for internal audit:**

- – Performing a top-down risk assessment around the company's cybersecurity process using industry standards as a guide, and providing recommendations for process improvements
- – Reviewing existing processes and controls to help ensure they consider the threats posed in the constantly evolving environment
- – Reviewing the alignment of the organization's cybersecurity framework with regulatory expectations
- – Assessing implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- – Evaluating the organization's security incident response and communications plans
- – Assessing third-party security providers to evaluate the extent to which they are addressing current and emerging risks completely and sufficiently

KPMG

# Use of data analytics and continuous monitoring in internal audit

In the past few years, data analytics have helped to revolutionize the way in which companies assess and monitor, especially in terms of efficiently expanding the scope of audits and improving detail levels to which audits can be performed. Data analytics and continuous monitoring can help internal audit departments simplify and improve their audit process, resulting in a higher quality audit and tangible value to the business. Consider the traditional audit approach, which is based on a cyclical process that involves manually identifying control objectives, assessing and testing controls, performing tests, and sampling only a small population to measure control effectiveness or operational performance.

Contrast this with today's methods, which use repeatable and sustainable data analytics that provide a more thorough and risk-based approach. With data analytics, companies have the ability to review every transaction—not just samples— which enables more efficient analysis on a greater scale. This can also reduce the need for costly on-site audits. Leveraging data analytics also accommodates the growing risk-based focus on fraud detection and regulatory compliance.

**Example focus areas for internal audit:**

– Assisting in creating automated extract, transform, and load (ETL) processes, along with repeatable and sustainable analytics and dashboards enabling monitoring against specified risk criteria by internal audit or business management

– Assessing the alignment of the strategic goals and objectives of technology companies to risk management practices while providing a mechanism to monitor and prioritize strategic objectives and risks on a continuous basis

– Developing data analytics enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level

– Performing automated auditing focused on root cause analysis and management's responses to risks, including business anomalies and trigger events

– Recommending consistent use of analytics, including descriptive, diagnostic, predictive, and prescriptive elements

02

**Drivers:**

– Leveraging internal and external big data sources to provide a holistic organizational view

– Facilitating real-time, continuous risk management

– Enabling early detection of potential fraud, errors, and abuse

– Taking a "deeper dive" into key risk areas through analysis of key data

– Increasing overall efficiency of audits being performed (frequency, scope, etc.)

– Reducing auditing and monitoring costs

– Leveraging data analytics tools and infrastructure implemented by management

03

# System implementation and upgrades: transitioning to cloud

**Drivers:**

- Identifying needs for cloud solutions to facilitate transition and leveraging recent advances in off-premise technology for operational efficiencies
- Providing a timely view into the risks and issues that allows management to correct course or implement risk mitigation strategies prior to going live
- Enabling continuous monitoring of cloud risks and data following implementation, leveraging security analytics and data mining capabilities, where possible, over large volumes of available internal data
- Increasing focus on data privacy, cybersecurity, and business resiliency in the context of cloud
- Implementing an effective process for identifying and managing regulatory, legal and compliance requirements in a global market, both pre- and post-implementation of a cloud platform

As cloud services can be delivered via different ways (e.g., SaaS, PaaS, and IaaS) and operational models (such as public, private, and hybrid), companies face risks and challenges when moving their IT infrastructure to the cloud. These include risk of cloud systems implementations not being able to deliver the intended value/benefits, budget and schedule overruns, overlooking processes or work groups, and managing individuals who are resistant to change. The solution architecture should account for the nature of risks in the cloud environment as well as the implementation itself, and determine how the provider implements controls. A prime opportunity to reduce or remediate risks lies with the proactive involvement of IT teams during the solutions architecture phase. Any proposed cloud approach should be evaluated for regulatory compliance before it is implemented. Cloud planning cycles should also be monitored continuously throughout the cloud solution's life cycle (from initial design through vendor selection, implementation, usage, and decommissioning/data reclamation).

Beyond IT implications, critical business operations such as tax, regulatory compliance, vendor management, and a host of other areas are also affected. As companies manage through the impact of continued globalization and economic recovery, an increased sense of urgency has emerged surrounding information security and privacy. As technology companies increase their use of cloud platforms, these companies need to ensure data is protected.

**Example focus areas for internal audit:**

- Reviewing the process by which management establishes a business case for cloud and performing due diligence for services provided, such as assessing internal controls of the vendor and the cadence for roles and responsibilities of the vendor and company
- Evaluating the organization's approach to change management and business readiness around the implementation
- Assessing policies, practices, and controls for data protection, segregation, location and ownership to determine if these are aligned with identified risks, the operating business model and the implemented cloud solution
- Appraising programs around incident management and communication, specifically around data breach and unauthorized access
- Analyzing provisions and responsibilities for system availability, disaster recovery, and business continuity, both within the company and outsourced to the vendor
- Examining vendor compliance with legal and regulatory requirements including having insight into known deficiencies, user control responsibilities, and the company's controls over its cloud usage to meet compliance requirements
- Assisting management in developing robust security and privacy programs, including training
- Overseeing security audits around cloud services

# 04 Third-party outsourcing relationships

**Drivers:**

- Reducing revenue loss
- Preventing cost escalation
- Complying with regulatory requirements
- Mitigating risk

Organizations leverage third parties to provide a variety of services such as product sales and distribution, data storage, marketing funds program administration, customer service, and call centers. Outsourcing frees up organizational resources to focus on core competencies and can help reduce costs.

While third parties facilitate business, they can expose an organization to financial, regulatory and reputational risk. These risks can be extensive, including revenue loss, import/export exposures, data privacy breaches, cybersecurity issues, and bribery and corruption risk. Organizations have the ability to outsource a variety of tasks, however, they remain accountable for these outsourced activities.

An effective third-party management program, such as one that incorporates third-party risk assessment, due diligence, and ongoing monitoring, can help companies manage their exposure to these risks.

**Example focus areas for internal audit:**

- Evaluating the methodology the organization uses to identify third parties, including segmentation and classification, and the risks associated with them
- Providing insight and feedback on the organization’s third-party management program, including vetting, due diligence and monitoring
- Executing risk-based third-party reviews that include procedures tailored to address the specific risks a third-party presents
- Investigating anomalies identified as a result of the organization’s third-party vetting process

# Product security

05

In today’s cloud-based marketplace, products are the lifeline and face for technology companies. Product security, accordingly, has been brought to the forefront in the cybersecurity field as a key focus for companies. Each product has its own regulatory requirements, privacy policies, and vulnerabilities that add an extra layer of complexity for corporate security teams. Unfortunately, the concept of product security playing second fiddle to corporate security has led to a proliferation of issues including financial loss, lengthy litigations, and damaged reputations.

When implemented properly, product security can lead to a secure development lifecycle, continual monitoring, and effective forensics logging which can minimize day zero vulnerabilities, lower maintenance costs, and potentially eliminate incoming threats. It is critical that technology companies understand the importance of product security and utilize it to complement and optimize their cybersecurity policies.

**Example focus areas for internal audit:**

- Evaluating encryption processes for at-rest and in-motion content and leveraging industry standards as a guide to provide recommendations
- Analyzing role-based product access policies to help ensure compliance with regulations regarding confidentiality and need-to-know basis
- Performing a top-down risk assessment on vulnerable OS, database, and application level ports to help ensure data integrity is retained
- Evaluating the regulatory compliance of each product
- Assessing existing product continual monitoring and effective logging processes and providing recommendations for process improvements

**Drivers:**

- Reducing market, reputation and regulatory risks associated with product vulnerabilities
- Mitigating product security flaws that can expose customer or organizational data
- Supporting product designers in reaching an appropriate balance between customer convenience and security
- Helping the organization respond appropriately to discovered or reported vulnerabilities

06

# BEPS (Base Erosion & Profit Shifting) and global tax reform

**Drivers:**

- Reducing the risk of global tax expense and effective tax rate volatility due to rapid and significant change in international tax norms and targeted reforms designed to eliminate common tax structures used by many multinational enterprises (MNEs)
- Averting reputational damage to the organization due to new regulatory requirements for enhanced tax transparency and country-by-country reporting
- Decreasing tax compliance risk related to the proliferation of anti-BEPS regulatory requirements across multiple countries

With the release of the Organization of Economic Cooperation & Development's (OECD) recommendations to combat Base Erosion & Profit Shifting (BEPS) on October 5, 2015, the foundation for global tax reform is complete. Throughout 2016, and beyond, tax administrations around the globe are expected to adopt the many BEPS recommendations into domestic law. Indeed, some countries have already moved forward as early adopters. The October 2015 recommendations represent a major milestone in the G-20's effort to combat aggressive tax planning by MNEs.

BEPS reforms have been driven in significant part by political pressures arising from mainstream media reports of corporate tax avoidance, public governmental investigations, and growing public debt levels. These forces will fuel widespread global adoption of the October 2015 BEPS recommendations. BEPS reforms cover many aspects of corporate taxation with emphasis on enhanced tax transparency, transfer pricing rules forcing taxation of profits in jurisdictions where MNEs do business (not in tax havens), and broadening tax nexus rules to extend the tax reach of regulators in the countries where MNEs' customers reside.

BEPS reforms will be supported by extensive documentation requirements, including, in some countries, penalties for compliance failures. The new reporting requirements are extensive in many cases and several of the anti-BEPS measures are highly complex, presenting compliance challenges for MNEs.

**Example focus areas for internal audit:**

- Assisting the company and its tax function in preparing a BEPS readiness assessment and developing an action plan to address identified risks arising directly from BEPS reforms as well as the implementation of BEPS remediation strategies
- Advising on the enhancement or development of a corporate tax code of conduct and supporting tax controls that account for the new regulatory environment
- Assessing the company's readiness for compliance with the array of transparency measures to which MNEs will be subject, including identifying the stakeholders and data sources necessary to properly report income and taxes paid by country
- Aiding the company in evaluating the effectiveness of automated compliance programs for tax transparency reporting and enhanced transfer pricing documentation

# Mergers, acquisitions and divestitures

A need to manage execution risk more effectively is leading many technology companies to design additional rigor into their merger, acquisition, and divestiture programs to help ensure a fact-based and well-controlled diligence, valuation, planning, and execution process. The recent trend in divestitures in the technology industry has led to major levels of effort managing very complex and time-consuming projects.

**Example focus areas for internal audit:**

- Performing "post mortem" reviews on prior deals or divestitures to assess the effectiveness of procedures and playbooks
- Assessing the adherence to accounting and internal control due diligence checklists that address key deal areas (i.e., quality of earnings and assets, cash flows, unrecorded liabilities) and identify internal control gaps for both the acquired company and on a combined basis
- Understanding communication processes between finance, internal audit, and deal teams to assess control implications of executing business process change during active integrations or divestitures
- Conducting a project risk assessment review of the business integration or divestiture process, focusing on potential risks, integration success metrics, and information systems

07

**Drivers:**

- Increasing volume of M&A and divestiture activity in the technology sector
- Focusing on strategic risks of M&A and divestiture activity, including impacts on other parts of the business in the form of stranded costs and post close operational entanglements
- Improving integration (or carve-out) processes across all key functions
- Ensuring the acquired or spun-off entity is SOX 404-compliant, typically within 12-24 months of the transaction's completion

08

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

**Drivers:**

– Continuing enforcement by domestic and foreign regulators on corruption

– Reemphasizing recent policy initiatives by the U.S. Department of Justice (DOJ) on holding individuals accountable in corporate wrongdoing

– Rekindling focus on the effectiveness of compliance programs

– Increasing resources at both the DOJ and FBI allocated to FCPA enforcement

On September 9, 2015, the DOJ published the Yates Memo which announced the DOJ's focus on holding individuals accountable for corporate misconduct and outlines six points of focus for DOJ attorneys:

– Corporations must provide to the DOJ all relevant facts about the individuals involved in the corporate misconduct to be eligible for any cooperation credit

– Corporate investigations should focus on individuals from the inception of the investigation

– Criminal and civil attorneys handling corporate investigations should be in routine communication with one another

– Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals

– Corporate cases should not be resolved without a clear plan to resolve related individual cases and declinations as to individuals in such cases must be memorialized

– Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay

The DOJ has recently added resources that are responsible for providing guidance to DOJ prosecutors concerning the existence and effectiveness of any compliance program that a company had in place at the time of the conduct giving rise to the prospect of criminal charges, as well as evaluating corporate compliance and remediation measures.

### Example focus areas for internal audit:

– Supporting management in designing a global anti-bribery compliance strategy based on internal audit's "in-field" knowledge and experience

– Updating its internal audit programs to ensure they contain suitable anti-bribery and corruption procedures

– Facilitating management's bribery and corruption risk assessment activities to help ensure emerging risks specific to the company's industry and lines of business are identified and prioritized effectively

– Collaborating with the business and other compliance teams on awareness and education campaigns, especially on a global scale

– Partnering with the business to enhance existing anti-bribery and corruption programs, including third-party risk management, due diligence, and advanced data analytics

– Assisting the company to help ensure it meets the requirements/guidance provided by the DOJ related to the elements of an effective compliance, anti-bribery and corruption program

# Data governance

There is an explosion of data being captured and stored in big data platforms. Leading organizations across all industries are leveraging the power of big data technologies to capture, merge, and analyze internal and external, structured and unstructured, and transactional and historical data to change the way they run their businesses and in some cases create new businesses. Organizations unleashing the power of their data are seeing big payoffs. However, the risks to these organizations are also growing as data lakes are built. Regulations require companies to secure their data, protect customer PII (Personal Identifiable Information), obtain customer consent to use their data, or disclose to customers how their data will be used and shared. Internal audit plays a key role in ensuring big data does not cause big problems.

**Example focus areas for internal audit:**

– Assisting in the formation or review of data governance policies and processes to increase the accuracy and integrity of a company's metadata

– Documenting the data model and points of control to identify security gaps. What data is collected? Where is it stored? How is it used? Who has access to the storage systems?

– Helping in the creation or review of information management policies that entail designing, organizing, retrieving, and distributing information in the most efficient manner

– Reviewing the effectiveness of the company's ability to respond to new policies and emerging legislative mandates and regulations with appropriate data

09

**Drivers:**

– Validating and maintaining the accuracy, integrity, and versioning of a company's big data

– Ensuring proper data security policies are established and being followed

– Increasing usability and metadata comprehension by business owners

– Operationalizing metadata to make it actionable

10

# Intellectual property protection

**Drivers:**

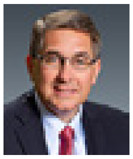
- Helping to ensure company-specific privileged information is kept secure and reducing risks of data leaks
- Recognizing when intellectual property (IP) strategy is not aligned with business or product strategy and adjusting accordingly
- Ensuring IP management processes are aligned with compliance requirements
- Lowering costs related to errors and litigation
- Confirming your top researchers, engineers and scientists are submitting ideas to be protected
- Determining if you should buy or create your IP
- Identifying and scoring the best ideas, so you know which to protect
- Realizing which IP should be abandoned or sold
- Deciding if you should commercialize your IP

With intellectual property at the heart of technology companies' core competencies and business relationships, identifying and protecting IP assets is a critical challenge for companies seeking to maximize the value of their intellectual property. In dealing with IP identification, management should have a process in place to ensure the best ideas are being brought forward and identified for protection. In the current age of outsourcing, cloud services, and remote access options (such as VPN), new challenges can arise around protecting data that is sent to third parties, from both a technology perspective (e.g., encryption) and business perspective (e.g., consistent policies regarding sharing of information). Company processes and controls around how this transfer of data is managed and secured is critical to help prevent potential exposures. Additionally, compliance training becomes a central point in making sure employees are aware of policies in place and what information is considered privileged.

**Example focus areas for internal audit:**

- Performing an audit of IT access and security around the technology company's IP to determine if any potential areas of risk are present, especially around company changes such as new systems, mergers/acquisitions, etc.
- Assisting with the implementation of controls to help improve the integrity and security of critical business data
- Aiding with the drafting of consistent compliance standards and, once approved, communicating these to relevant individuals through a training and awareness program
- Conducting a process, gap and risk assessment of the internal IP process as it relates to the IP lifecycle
- Guiding third-party risk assessment and compliance specifically related to IP agreements with third parties

# About the authors

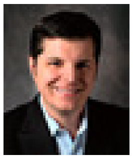


## Tom Lamoureux

Tom Lamoureux serves as KPMG's Risk Consulting leader for Technology, Media and Telecommunications. In this role, he guides the delivery of KPMG advisory services to some of the world's leading technology companies to help them create world-class risk and business management processes. These services include internal audit, Sarbanes-Oxley 404 projects, information technology and other risk management services.

Tom has developed and implemented state-of-the-art risk assessment and audit planning methodologies, high-value-added internal auditing services for domestic and international objectives, and self-assessment strategies and solutions for internal audits. In addition he spearheads the development of new risk management services in response to evolving client needs.

In his industry leadership capacity, Tom has directed original research, white papers and roundtable forums on emerging topics of vital interest to technology firms.



## Ron Lopes

Ron is a partner in KPMG's Advisory practice and has more than 25 years of experience in the Silicon Valley. Ron has significant experience guiding the delivery of services to many leading multinational technology companies to help them create high-value-added risk and business management processes.

Ron has worked on a multitude of projects for clients, including internal audits, financial and operational control reviews, risk assessments, third-party compliance audits, process reviews, financial statement audits, process improvement engagements, and Sarbanes-Oxley 404 compliance efforts. Ron has developed and implemented high-impact risk assessment and audit planning methodologies as well as self-assessment strategies for internal audits.

Ron has significant experience in revenue recognition, financial reporting, and benchmarking leading practices. A significant portion of his career has involved assisting clients with the coordination and execution of large international projects.

## Contributors

We acknowledge the contribution of the following individuals who assisted in the development of this publication:

**Neha Bhatia** Director, Advisory

**TingTing Cui** Manager, Advisory

**Robert Rosta** Associate Director, Technology Marketing

## How KPMG Can Help

An experienced team. A global network. KPMG's Internal Audit, Risk, and Compliance 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.

KPMG's Advisory professionals combine technical, market and business skills that allow them to deliver objective advice and guidance that helps the firm's clients grow their businesses, improve their performance, and manage risk more effectively.

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. With a worldwide presence, KPMG continues to build on our member firms' successes thanks to our clear vision, maintained values, and our people in 155 countries. We have the knowledge and experience to navigate the global landscape.

## Contact us:

**Gary Matuszak**
Global and U.S. Chair, Technology,
Media & Telecommunications
408-367-4757
gmatuszak@kpmg.com

**Richard Hanley**
U.S. National Advisory Leader,
Technology, Media & Telecommunications
408-367-7600
rhanley@kpmg.com

**Tom Lamoureux**
Risk Consulting Leader for Technology,
Media and Telecommunications
206-913-4146
tlamoureux@kpmg.com

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

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

**kpmg.com/socialmedia**