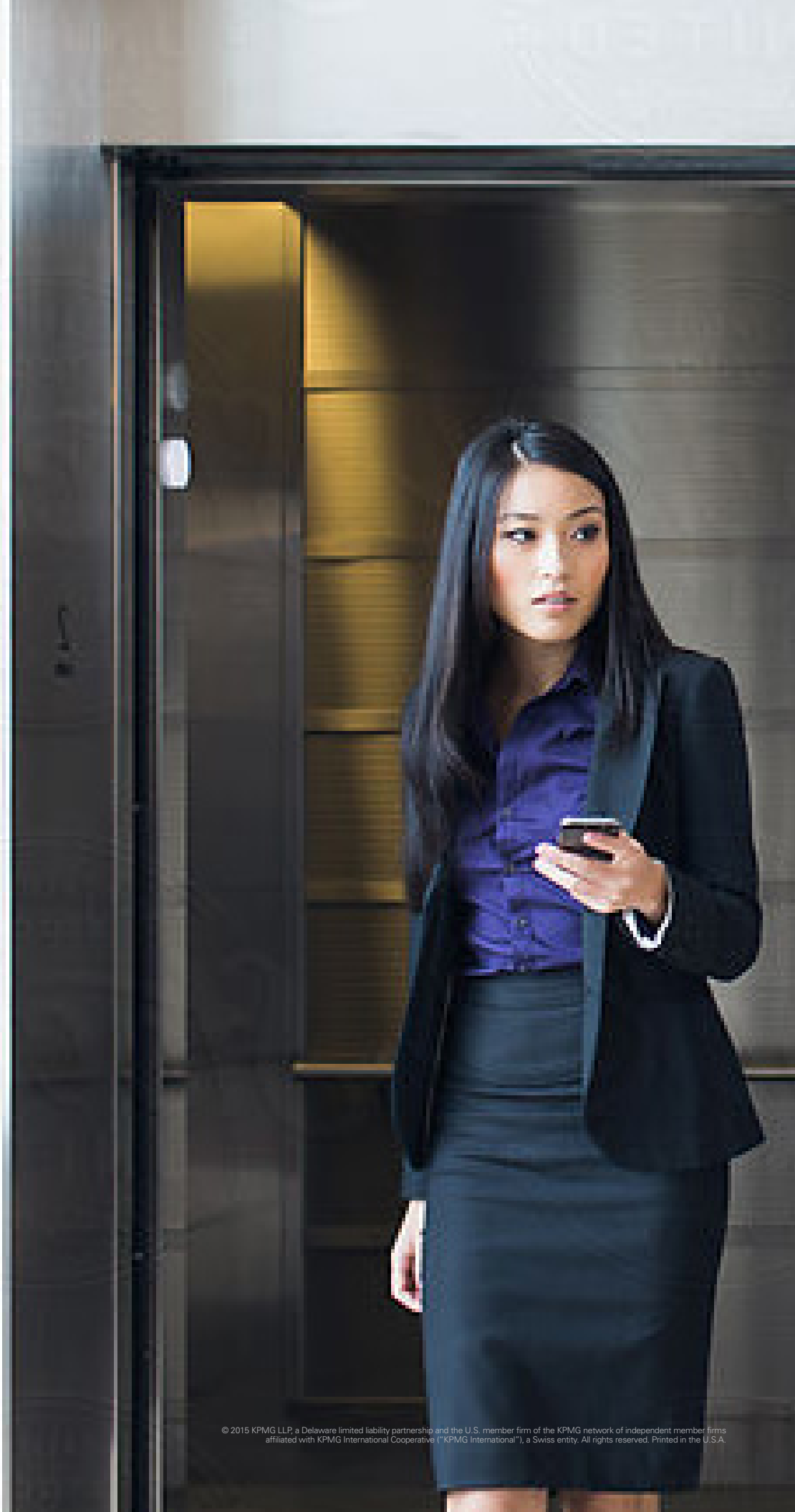
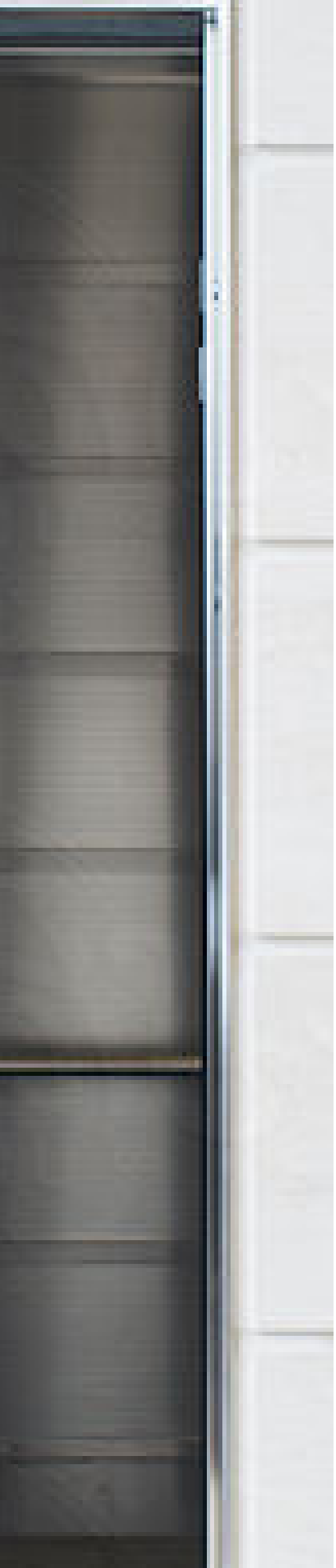
KPMG Internal Audit: Top 10 considerations in 2015 for technology companies

kpmg.com

KPMG
cutting through complexity





Our annual compilation of Internal Audit considerations for technology companies, "Top 10 in 2015," focuses on the critical role Internal Audit can play in helping companies manage some of their leading risks more effectively in today's challenging environment.

In this year's publication, you will notice the continuing importance of disruptive technologies in determining the focus areas of Internal Audit—both in terms of presenting opportunities and new sources of risk.

Top 10 in 2015:

1. Cybersecurity
2. Intellectual property protection
3. Evolving business models
4. International operations
5. Vendor management
6. Government contracting
7. System implementations and upgrades: Transitioning to the cloud
8. Mergers, acquisitions, and divestitures
9. Revenue from contracts with customers
10. Use of data analytics and continuous monitoring in Internal Audit

The often overlapping relationships among these areas demonstrate how tightly connected our organizations have become in today's global markets. For example, relationships with key business partners often include the exchange of intellectual property, highlighting the importance of monitoring our partners' security frameworks and procedures, as well as performance and contractual compliance.

Similarly, evolving business models are frequently enabled, and supported, by emerging technologies, such as cloud initiatives that can enhance business performance while reducing costs and risk.

These connections highlight the value Internal Audit can provide in helping organizations address these risks holistically, as well as individually.

KPMG LLP's (KPMG) 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's professionals who work with technology companies
- KPMG survey data.

The top 10 focus areas on the following pages explore the leading risks technology companies face as they evaluate their strategies and make investments. All of these areas highlight the leading exposures companies are working to address as they enter 2015.

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 plan.

1 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.

As the term implies, in today's world of constant connectivity, cybersecurity is a key focus point for many technology companies. Cybersecurity frequently appears on the top of many board agendas, and data security breaches now appear to be headline news almost on a weekly basis. Several factors have driven the increased attention paid to cybersecurity issues, including changes in the threat landscape, rapid changes in technology, changing regulatory environments, social change, and corporate change. Additionally, the capabilities and techniques used by hackers are continuously growing and evolving, especially with regards to targeting specific information or individuals. New methods are constantly being developed by increasingly sophisticated and well-funded hackers who can target companies not only through networks directly but also through 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 that technology companies remain vigilant and up to date regarding all the recent protection criteria.

How Internal Audit Can Help:

- Perform a top-down risk assessment around the Company's cybersecurity process using industry standards as a guide, and provide recommendations for process improvements
- Review existing processes to help ensure they consider the threats posed in the constantly evolving environment
- Assess implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- Assess third party security providers used by technology companies to evaluate the extent to which they are addressing the most current risks completely and sufficiently.

2 Intellectual property protection

Drivers:

- Helping to ensure company-specific privileged information is kept secure and reducing risks of data leaks
- Recognizing when 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.

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 protection, management should consider a wide-ranging approach to understand and classify enterprise data, and map appropriate controls to help protect the confidentiality and integrity of this data both within and outside the organization's boundaries. 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.

How Internal Audit Can Help:

- Perform 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
- Assisting with the drafting of consistent compliance standards and, once approved, communicating these to relevant individuals through a training and awareness program.

3 Evolving business models

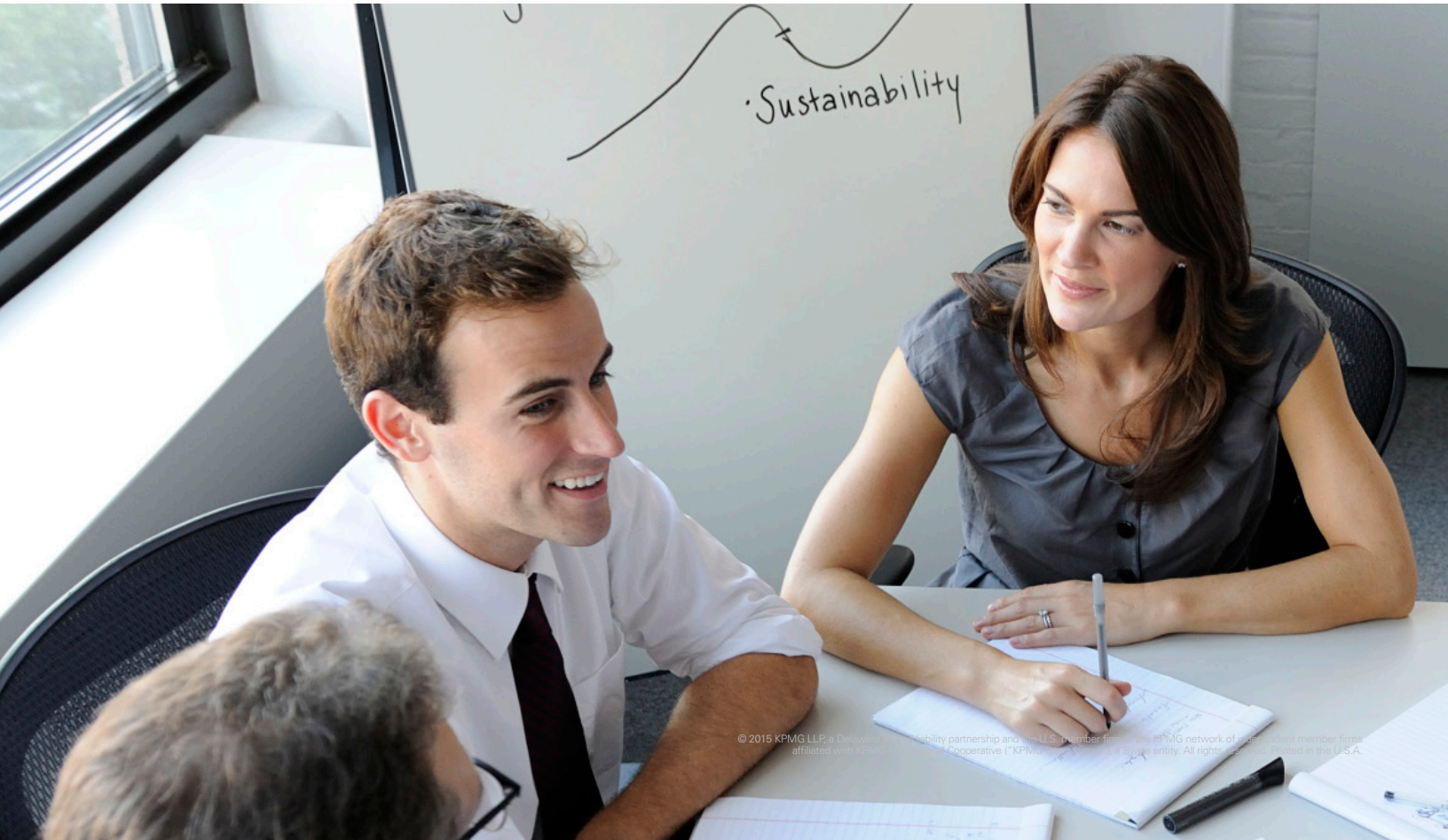
Drivers:

- Adjusting operating and financial models to reflect current and emerging business opportunities
- Shifting methods for delivery of products in rapidly evolving technological environment
- Helping to ensure companies have appropriate processes, infrastructure, controls, etc., in place to address new risks presented with changes to business models.

Given the ever-increasing competitive atmosphere, combined with the speed at which new technologies are being developed, evolving business models (such as shifting from delivery of physical "box" products to digital subscriptions and cloud-based deliveries) are a standard part of today's environment for technology companies. Changes occur rapidly and can often bring about new challenges and needs, which are overlooked in the urgency to quickly get new products to the market. Internal Audit's role is to ask questions such as "Do we have the right controls in place?" and "Can our infrastructure support this new model?" New risks often come with the territory, so it is crucial that companies are aware of the new risks and ensuring that their processes in place are adequately addressing them.

How Internal Audit Can Help:

- Review transition plans against industry standards and leading practices and provide recommendations around potential risks and operational issues
- Assist in identification and documentation of key risks and controls unique to the new operating model
- Assess how regulatory and compliance requirements apply to the evolved business model and developing internal audit's ongoing monitoring process around these newly applicable requirements
- Assist with training and education to relevant individuals around the changes.



4 International operations

Drivers:

- Enhancing oversight and visibility into international operations, especially with regards to regional geopolitical issues
- Achieving greater confidence in the propriety of local business practices and compliance with corporate policies and regulations (e.g., FCPA)
- Increasing consistency of business policies and processes across regions
- Reducing risk of noncompliance with export laws and regulations
- Enhancing controls and global export sanction compliance processes.

Global operations present some unique challenges and risks for technology companies. Many technology companies are exploring global opportunities for revenue generation and operational efficiencies. International operations, however, lead companies to have concerns around a multitude of issues ranging from product quality to complying with complex local regulatory requirements. Geopolitical issues (such as sanctions, embargos, cross-border trade regulations) add yet another dimension of complication to dealing with foreign countries, requiring companies to have detailed knowledge around world events and evolving expectations. Additional risks include inconsistency in business practices, inadequate corporate oversight, and complicated and changing legal and regulatory requirements.

How Internal Audit Can Help:

- Review overall key process areas and control environment, including compliance with U.S. and local requirements (such as import and export regulations). Assisting with creating and/or updating existing corporate documentation in these areas
- Reviewing business practices, potential code of ethics, and anti-bribery and corruption issues among foreign entities or business partners
- Assisting companies in documenting policies and procedures for export controls and sanctions compliance
- Communication of the company's risks and controls to international employees, to support consistency of corporate policies and procedures in each entity.

5 Vendor management

Drivers:

- Continued pressure on margins and profitability
- Monitoring vendors' contract compliance and intellectual property protection strategies
- 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 fail to meet their contractual obligations. This does not necessarily imply the business partners have acted deliberately, but these miscues are often driven by the complexity of the environment. Third parties often work under highly complex contracts, where the requirements are not clearly identified or key responsibilities may be overlooked. In addition, contracts may not reflect changed circumstances. No matter the reasons, the need to manage risks related to vendor relationships is critical for technology companies to maintain control over their costs.

How Internal Audit Can Help:

- Reviewing the process by which vendors are identified, due diligence selection and on-boarding processes and controls for selected vendors
- Conducting vendor audits that focus on compliance with contract terms and effectiveness of vendor internal controls, including reviewing the processes and controls over data that is self-reported by these third parties
- Assisting in developing, implementing, and calibrating a continuous monitoring system over vendors related to their self-reported data.

6 Government contracting

Drivers:

- Enhancing compliance and monitoring processes for doing business with governments
- Improving contract governance
- Avoiding financial exposure and other risks due to noncompliance
- Providing education and knowledge sharing to employees involved in government work to help ensure that specific requirements are adhered to.

Government contracting can make up a substantial portion of business for technology companies, which also adds additional levels of complexity (e.g., compliance and reporting). Doing business with governments can be very different from dealing with private companies. For example, government agreements often have best pricing clauses or requirements that data be kept within the United States and only handled by U.S. citizens. It is important that companies have an understanding of the specific legal and regulatory requirements in dealing with government institutions and also have the appropriate processes and controls in place for monitoring compliance. A key area of focus is core government contract requirements, including financial accounting and reporting (FAR), cost accounting standards (CAS), and other specific contractual requirements that are critical to many federal, state, and local government contracts. Management should be taking a hard look to identify, evaluate, and prioritize the risks that are inherent in the government contracting compliance environment.

How Internal Audit Can Help:

- Performing a "gap analysis" against applicable government contractual requirements to determine potential exposures
- Assisting management in assessing and/or enhancing the effectiveness of internal controls and processes unique to managing government contracts
- Assist management in establishing a framework for ongoing monitoring compliance with government requirements.
- Reviewing potential government contract work to assess impact on the company's business and ability to deal with regulatory requirements.

7 System implementation and upgrades: transitioning to cloud

Drivers:

- Identifying needs for cloud solutions in order to facilitate transition, and leveraging recent advances in off-premise technology for operational efficiencies
- A timely view into the risks and issues that allows management to correct course or implement risk mitigation strategies prior to going live
- Continuous monitoring of cloud risks and data following implementation
- Implementing an effective process for managing regulatory and legal requirements postimplementation of a cloud platform.

As cloud services can be delivered in 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 implementation not being able to deliver the intended value/benefits, budget and schedule overruns, overlooking related process/people, 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. The greatest 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.

How Internal Audit Can Help:

- Review the process by which management establishes a business case for cloud and performing due diligence for services provided, such as assessing internal controls of vendor and cadence for roles and responsibilities for vendor and company.
- Review the approach to organization change management and business readiness around the implementation
- Review programs around data breach/unauthorized access as required by legal and regulatory compliance.
- Assist management in developing security and privacy programs and training
- Security audits around cloud services.

8 Mergers, acquisitions, and divestitures

Drivers:

- Assessing strategic risks of M&A and divestitures activity, including impacts on other parts of business
- Implementing a more rigorous and better-controlled M&A program to identify and manage these risks, as well as obtaining validation of transaction risk and expectations prior to communicating them to shareholders
- Enhancing execution planning, delivery, and performance tracking
- Improving integration (or carve-out) processes across all key functions.

A need to manage execution risk more effectively is also 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.

How Internal Audit Can Help:

- Perform "post mortem" reviews on prior deals or divestitures to assess 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
- Understand communication processes between finance, internal audit, and deal teams to assess control implications of executing business process change during active integrations or divestitures
- Perform a project risk assessment review of the business integration or divestiture process, focusing on potential risks, integration success metrics, and information systems.

9 Revenue from contracts with customers

Drivers:

- Structuring and tailoring existing systems to account for revenue under the new standards
- Educating employees to provide a fundamental understanding of the new requirements
- Revising internal control environment to cover the changing risks associated with the new standards
- Updating existing policies and procedures for recognizing revenue to be in line with new standards.

In May 2014, IASB and FASB published new standards of revenue recognition, which will replace the existing standards. The new standards provide a framework that moves away from the industry and transaction-specific requirements under U.S. GAAP. New qualitative and quantitative disclosure requirements aim to enable financial statement users to understand the nature, amount, timing, and uncertainty of revenue and cash flows arising from contracts with customers. While the 2017 date by which companies must comply may seem far off, many technology companies are already assessing potential impacts, as they may require significant revision of existing systems, policies, procedures, and internal controls. For some entities, there may be little impact, however, arriving at this conclusion will require an understanding of the new model and its application to particular transactions.

How Internal Audit Can Help:

- Perform an impact assessment (gap analysis) around how the new standards will impact the company, provide road map for transition and assist in communicating new standards to stakeholders
- Assist management in identifying tax implications of new standards
- Analyze existing IT systems and accounting processes to determine what changes/upgrades may be needed
- Assist with the design and implementation of new internal controls or modification of existing controls to account for changing risk points

10 Use of data analytics and continuous monitoring in Internal Audit

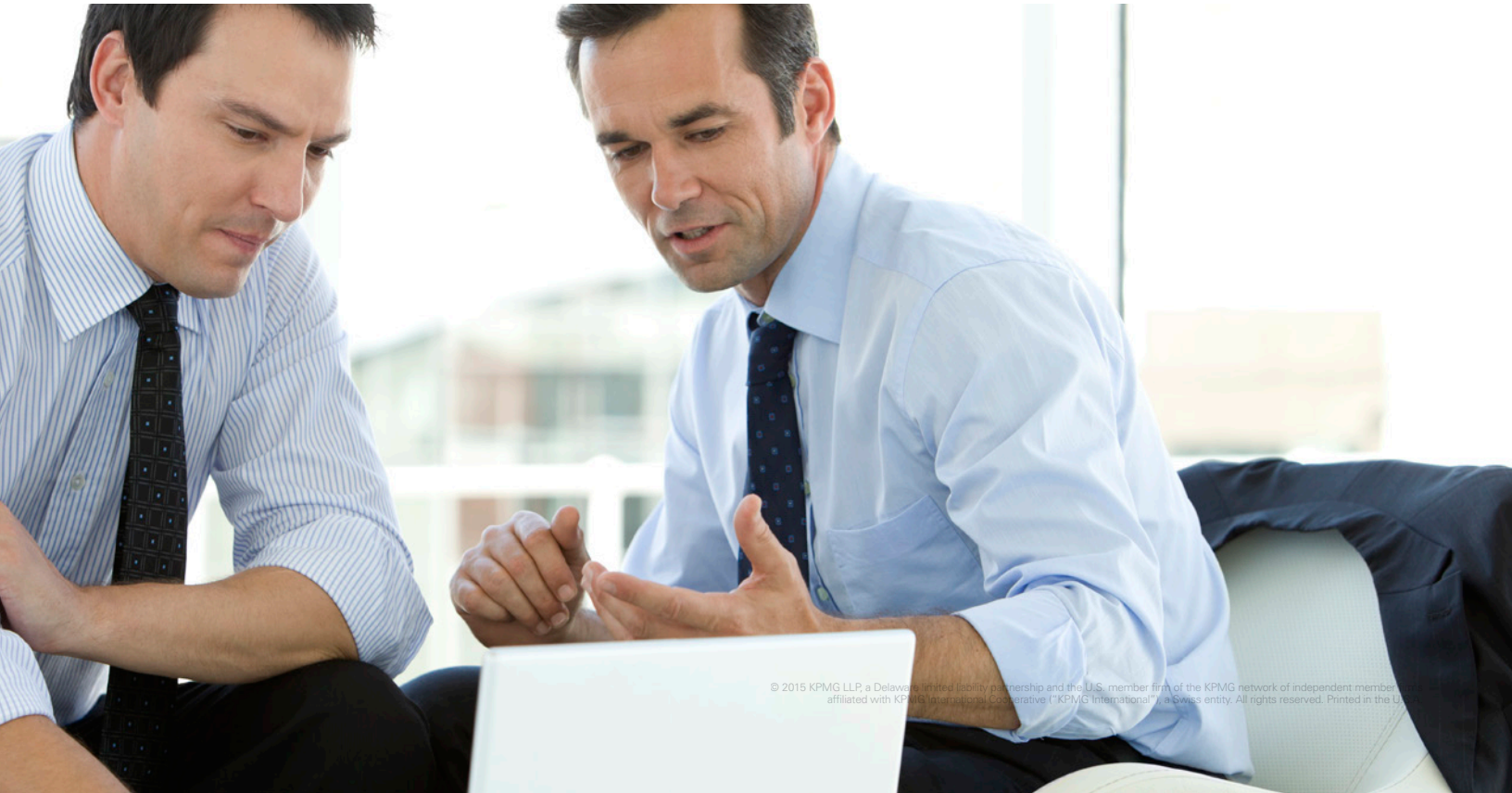
Drivers:

- Enabling real-time, continuous risk management
- Increasing overall efficiency of audits being performed (frequency, scope, etc.)
- Taking a "deeper drive" into key risk areas through analysis of key data
- Reducing costs involved in auditing and monitoring
- Enabling early detection of potential fraud, errors, and abuse

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. In addition, leveraging data analytics also accommodates the growing risk-based focus on fraud detection and regulatory compliance.

How Internal Audit Can Help:

- Assist in creating automated extract, transform, and load (ETL) processes, along with system-generated analytics and dashboards monitored by the business against specified risk criteria
- Assessing the alignment of the strategic goals and objectives of technology companies to risk management practices and monitoring and prioritization of the strategic objectives and risks on a continuous basis
- Data analytics enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level
- 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.



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 extensive experience delivering strategic information technology consulting services and assisting clients in building effective distributed systems management solutions. He 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 software and technology firms. Some examples include Software License Compliance, Software Asset Management and Identity Access Management.

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 (SOX) Section 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, and objectives.

Contributors

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

Neha Bhatia
Director, Advisory, IA & SOAS Strategic Sourcing

Dan Mochizuki
Manager, Advisory, IA & SOAS Strategic Sourcing

About 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.

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