



Top 10 internal audit focus areas for technology companies

Top 10 in 2017

Cybersecurity	2
Mergers, acquisitions, and divestitures	3
Use of data and analytics in internal audit	4
Base Erosion & Profit Shifting and global tax reform	6
Data governance	7
System implementation and upgrades: transitioning to the cloud	8
New accounting standards	10
Global compliance framework	11
Research and development efficiency	12
Business continuity management	14





The importance of internal audit for technology companies

Every day, technology companies grapple with challenges such as cyber threats, new industry and business disruption, and regulatory compliance. Our annual edition of the top 10 internal audit focus areas for technology companies outlines the crucial role internal audit (IA) plays in helping technology companies manage some of today's most important risks.

The 10 focus areas explore some of the leading business issues technology companies face as they strategize and make investments. An effective IA function will stay current with these issues so it can help monitor related risks and their potential effects. The top 10 list can help ensure that IA allocates its resources to those areas of highest impact to the organization.

To provide the greatest value, IA must question the status quo, help improve controls, and identify potential efficiencies and cost savings. This should result in a wide range of benefits, from improved internal control environments to enhanced risk management processes to a more confident audit committee.

KPMG LLP's (KPMG) selection of focus areas is based on a number of inputs, including:

- Discussions with chief audit executives at technology companies
- KPMG's IA share forums for technology companies
- Insights from KPMG professionals who work with technology companies
- KPMG survey data

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

Cybersecurity

Drivers:

- Adopting new cloud and “aaS” (as-a-service) delivery models, and the requirements to protect customer data
- Avoiding costly consequences of data breaches such as investigations, legal fines, coverage of customer losses, remediation efforts, loss of executive and mid-level management time and focus, loss of intellectual property and capital, and potential loss of customers and business
- Averting reputational damage to the organization, especially with regard to lost customer data
- Protecting key company assets, processes, data, and information

Cybersecurity is a key focus point for many technology companies, going beyond headline news to the top of many board agendas. Several factors have driven the increased attention paid to cybersecurity issues, including the rate of adoption and rapid shifts in technology, the ever-changing threat landscape, the continued movement to the cloud and cloud services, more stringent and diverse regulatory environments, social change, and changes in corporate culture. New capabilities and techniques 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, such as identity access management systems and data loss prevention techniques. 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 internal audit focus areas:

- Perform a top-down risk assessment around the company’s cybersecurity process using industry standards as a guide, and providing recommendations for process improvements
- Evaluate existing processes and controls, such as Data Loss Prevention (DLP) solutions or Identity Access Management (IAM) systems, to help ensure that threats posed by a constantly evolving environment are considered
- Review the alignment of the organization’s cybersecurity framework with regulatory expectations, new computing, hosting and storage capabilities (i.e., cloud), new “aaS” (as-a-service) business models and global expansion
- Assess the implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- Evaluate the organization’s security incident response and communications plans
- Assess third-party security providers such as cloud service providers to evaluate the extent to which they are addressing current and emerging risks completely and sufficiently

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 internal audit focus areas:

- Perform “post mortem” reviews on prior deals or divestitures to assess the effectiveness of procedures and playbooks
- Assess 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
- Gauge the coordination between deal teams, internal audit and finance to help ensure financial controls are being addressed during active integrations or divestitures
- Conduct a project risk assessment of the business integration or divestiture process, focusing on potential risks, integration success metrics, and information systems
- Monitor and test accounting policy alignment, financial reporting integration, and control compliance to avoid financial misstatements or significant internal control deficiencies



02

Drivers:

- Increasing volume of mergers & acquisitions (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 difficulties
- 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
- Ensuring policy and control alignment post-acquisition to enable effective and compliant reporting

Use of data and analytics in internal audit

Drivers:

- Leveraging internal and external big data sources to provide a holistic organizational view
- Facilitating continuous risk assessment
- Enabling early detection of potential fraud, errors, abuse, and regulatory non-compliance
- 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 D&A tools and infrastructure implemented by management

In the past few years, data and analytics (D&A) has helped revolutionize the way in which technology companies assess and monitor risk, especially in terms of efficiently expanding the scope of audits, and improving detail levels to which audits can be performed. D&A 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 internal 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 analytics that provide a more thorough and risk-based approach. With D&A, internal audit teams 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 D&A also accommodates the growing focus on timely identification of fraud, waste, abuse, and potential regulatory non-compliance.

Some of the emerging trends in D&A in internal audit for 2017 include:

- A continued evolution from rules-based analytics to more advanced, repeatable and sustainable analytics
- Increased adoption of D&A capabilities by the business functions for continuous monitoring activities
- The inclusion of quantitative data into risk assessment activities to better identify emerging risks or significant changes to known risks
- Increased use of visualization tools and dashboards to improve data discovery and results interpretation to drive deeper insights



- Interest in where and how automation may be implemented for internal audit activities, as well as the ability to assess risks, controls and governance around the automation used by the business functions (first line of defense), and risk management and compliance functions (second line of defense)
- Assessment of the risks around analytic models, including the quality and reliability of the underlying data and resulting management reports, and the governance around management-owned D&A programs and activities.

Example focus areas for internal audit:

- Assist 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
- Assess 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
- Develop D&A-enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level
- Perform automated auditing focused on root cause analysis and management's responses to risks, including business anomalies and triggering events
- Recommend consistent use of analytics, including descriptive, diagnostic, predictive, and prescriptive elements, along with the use of internal, external, structured and unstructured data
- Enhance the planning, scoping and performance of the internal audit plan by using D&A to identify the right audits to perform, increase the number of audits, decrease the amount of time to get through the internal audit plan, increase the frequency of audits in key risk areas, and increase the scope of specific audits.

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 multi-national companies
- 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 BEPS regulatory requirements across multiple countries

Throughout 2016 we witnessed countries around the world adopting the tax reforms recommended by the Organization of Economic Cooperation & Development (OECD) in its Base Erosion & Profit Shifting (BEPS) work. BEPS is the use of tax planning by multi-national companies to shift profits from jurisdictions that have high taxes to jurisdictions that provide no or low taxation, with little or no economic substance. In short, the BEPS legislation is having an impact on multi-national technology companies' global tax landscape.

BEPS reforms have been driven in significant part by political pressures arising from reports of corporate tax avoidance, public governmental investigations, growing public debt levels, and nationalist politics. These forces are expected to gain momentum in 2017 and fuel greater proliferation of BEPS legislation in countries around the world. BEPS reforms cover many aspects of corporate taxation, including transfer pricing rules that force the taxation of profits in jurisdictions where multi-national technology companies do business (not in tax havens), and broadening tax nexus rules to extend the tax reach of regulators.

Technology companies face challenges with BEPS legislation particularly due to their heavy investment in intangible assets, such as intellectual property (IP), and having developed practices over the years that place ownership of these assets in low tax jurisdictions. With one of the main goals of BEPS legislation being enhanced tax transparency, technology companies that hold economic IP rights in low tax jurisdictions (i.e., Bermuda, Caymans, etc.) are bringing the ownership of IP back to the jurisdictions where they operate or where their 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 BEPS measures are highly complex, presenting compliance challenges for multi-national technology companies.

Example internal audit focus areas:

- Assist management in re-evaluating the Target Operating Model and supporting business models (the weight of tax savings supporting historical business models is likely to shift dramatically in the future, requiring a realignment of core operating functions to achieve optimal business models)
- Advise management on the enhancement or development of a corporate tax code of conduct and supporting tax controls that account for the new regulatory environment
- Assess the company's readiness for compliance with the array of transparency measures to which multi-national companies will be subject, including identifying the stakeholders and data sources necessary to properly report income and taxes paid by country
- Assist management in evaluating the effectiveness of automated compliance programs for tax transparency reporting and enhanced transfer pricing documentation

Data governance

Technology companies, like organizations across all industries, are capturing, transforming, and analyzing internal and external, structured and unstructured, and transactional and historical data to change the way they run their businesses and create new businesses. Software-as-a-service (SaaS) companies in particular are collecting valuable data through their platforms to measure their performance, gain a better understanding of customer behavior, and gauge user adoption. Organizations unleashing the power of their data are seeing big payoffs. However, as the collection, storage and transmission of data proliferates, managing the data and ensuring good governance presents multiple challenges around how the data is defined, maintained, accessed, consumed, and secured.

Further, the expectations on technology companies from a regulatory perspective are also growing as organizations must comply with requirements to secure customer data, adhere to privacy standards in multiple geographies, protect customer personal identifiable information (PII), obtain customer consent to use their data, or disclose to customers how their data will be used and shared. Technology companies must ensure that their data governance programs consider not only internal requirements, but also the external factors at play from an industry perspective.

Example internal audit focus areas:

- Assist in the formation or review of data governance policies and processes to increase the availability, usability and integrity of company data
- Document the data model and points of control to identify security gaps around data collection, data storage, data usage and access
- Assist management in the creation or review of information management policies that entail designing, organizing, retrieving, and distributing information in the most efficient manner
- Evaluate the company's data classification framework and related security controls
- Review the effectiveness of the company's ability to respond to new policies and emerging legislative mandates and regulations

05

Drivers:

- Validating and maintaining the accuracy, integrity, and versioning of a company's data
- Ensuring proper data security policies are established and being followed
- Bringing together business and technical collaboration not just for policy execution, but for policy management and impact analysis
- Increasing usability and metadata comprehension by business owners
- Operationalizing metadata to make it actionable

System implementation and upgrades: transitioning to the cloud

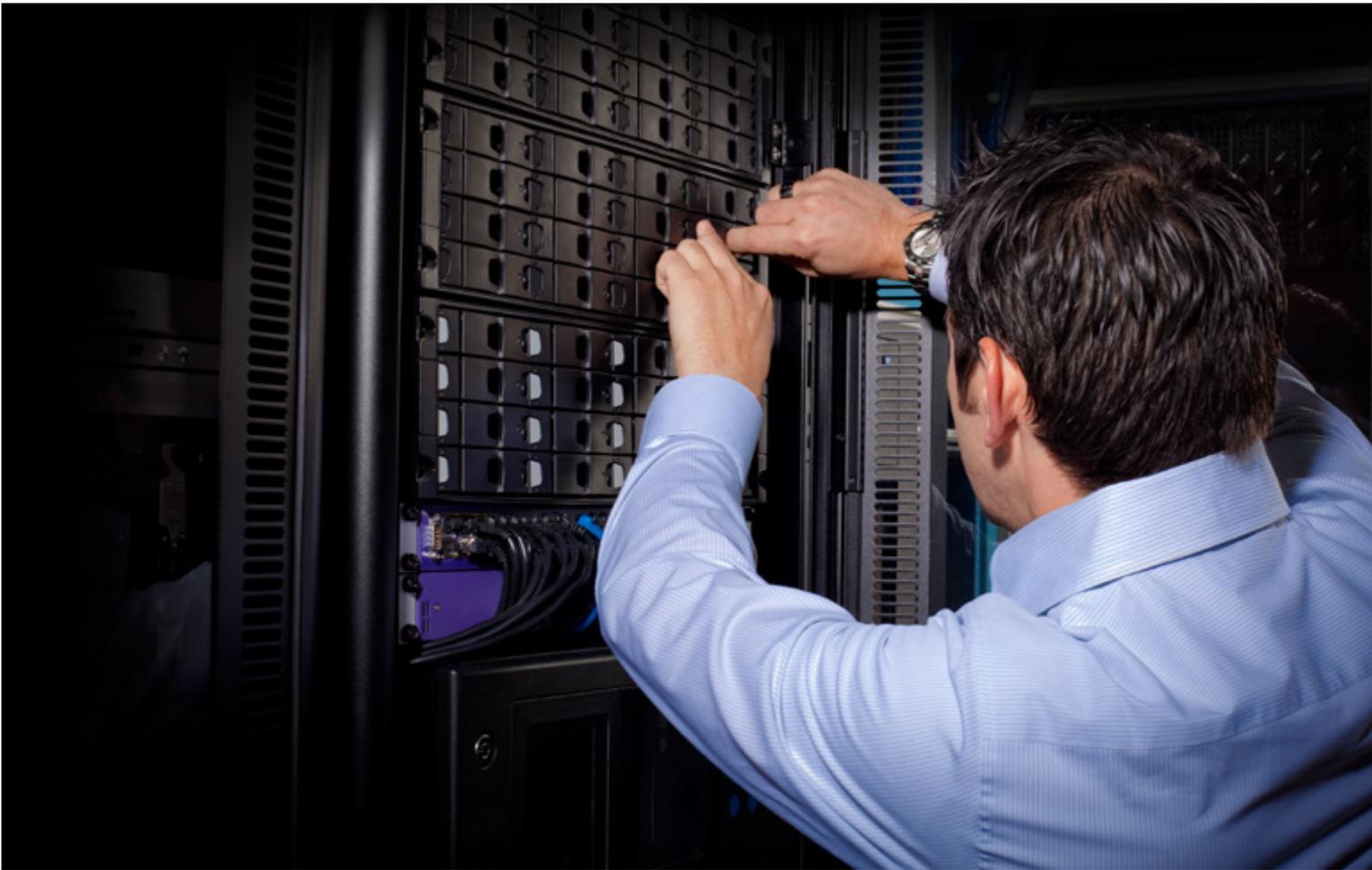
Drivers:

- Reducing the capital investment and on-going operating costs associated with on-premise applications and IT infrastructure in favor of cloud technologies
- Providing management with a timely view into the risks and issues associated with the implementation of the cloud solution, allowing management to course correct or put risk mitigation strategies in place prior to going live
- Increasing focus on data privacy, cybersecurity, and business resiliency
- Improving security and aligning internal control requirements with business processes and regulatory mandates

Technology companies continue to adopt cloud solutions at a rapid pace, from both a business applications and IT infrastructure perspective. Beyond traditional enterprise resource planning (ERP) and customer relationship management (CRM), companies are looking to SaaS solutions for sales commissions, budgeting and forecasting, payroll, expense reporting, and procurement, to name a few. Additionally, more and more technology companies are moving their IT infrastructure to cloud service providers as they seek benefits such as the rapid scalability of IT infrastructure, platform flexibility, and high availability/reliability. Companies must evaluate a number of factors when deciding to adopt cloud solutions, including the nature of the data (e.g., customer vs. corporate data) and related data security and privacy requirements, contractual considerations, vendor viability, total cost of ownership, and other impacts on the organization (i.e., tax considerations, reduced headcount, etc.).

Organizations often face multiple challenges when upgrading or moving their applications or IT infrastructure to the cloud. These include risks associated with the implementation or upgrade, such as budget and schedule overruns, completeness of requirements/design, and project resourcing, to more strategic challenges such as defining metrics and measuring the solution's benefits/value, organizational change management (i.e., transforming IT, etc.), and integration with existing technology.

Internal audit can play a key role in these critical initiatives by helping management understand the risk profile associated with the cloud solution and appropriate risk mitigation strategies, to evaluating and reporting on risk mitigation activities throughout the key phases of the initiative. Internal audit can be a key partner with the business in helping to ensure that the adoption of cloud-based technologies is a success.



Example internal audit focus areas:

- Review management’s business case for the cloud solution to determine that benefits have been clearly defined and are measurable, as well as review management’s subsequent plans and results for measuring and reporting on the benefits achieved
- Participate in the company’s vendor selection process to help ensure cloud vendors are able to meet the company’s security, control and legal/regulatory compliance requirements
- Evaluate the organization’s change management and business readiness plans around the implementation of the cloud solution
- Assess management’s approach to implementing controls to help ensure controls are optimized for efficiency and effectiveness and that management has increased the ratio of automated to manual controls where appropriate
- Review and provide recommendations on the organization’s or department’s new target operating model, particularly where new cloud solutions are replacing “on-premise” systems and technologies

New accounting standards

Drivers:

- Updating existing policies and procedures to be in line with new standards
- Modifying existing or implementing new systems/processes to comply with requirements under the new standards
- Revising the internal control environment to address the changing risks associated with the new standards
- Providing management with a timely view into the risks and issues in order to course correct or implement risk mitigation strategies prior to adopting the new standards
- Avoiding reputational risk of having control deficiencies or a material weakness in internal controls relating to the adoption of new accounting standards and ongoing business processes

Efforts by the Financial Accounting Standards Board (FASB) and International Accounting Standards Board (IASB) to update accounting requirements across several key topics are driving significant changes in both U.S. Generally Accepted Accounting Principles (U.S. GAAP) and International Financial Reporting Standards (IFRS). Technology companies must evaluate the impact of these new standards, which include accounting for revenue from contracts with customers, leases, financial instruments, etc., and develop an approach for implementing the new standards.

In particular, the new revenue standard, effective for companies with annual reporting periods beginning after December 15, 2017, may lead to significant changes in accounting for the software and software-as-a-service (SaaS) industry. The new standard introduces a core principle that requires technology companies to evaluate their transactions in a new way, which may require more judgment and estimation than today's accounting. New risk points may arise from changes to IT systems and reports that provide data inputs used to support these new estimates and judgments. To the extent that data is needed in order to comply with the new standard, technology companies will need to consider the internal controls necessary to ensure the completeness and accuracy of this information – especially if it was not previously collected, or was collected outside of the financial reporting system (e.g., projections made by the financial planning and analysis department for estimating variable consideration).

The volume and significance of the forthcoming changes will significantly impact the way technology companies conduct business and track, measure, and report various transactions and interests. The implementation of these is likely to affect operations throughout the organization, require significant time and resources, and result in changes to accounting policies, systems and processes. Company processes and controls around how the new standards are implemented as well as how the company manages the compliance requirements on a go-forward basis are critical to the company's success.

Example internal audit focus areas:

- Perform an impact assessment (gap analysis) around how the new standards will impact the company, and provide a road map for transition and assist in communicating new standards to stakeholders
- Analyze existing IT systems and accounting processes to determine what changes/upgrades may be needed
- Update understanding of the flow of information through the system
- Perform a top-down risk assessment around the company's processes and control environment
- Provide recommendations for the design and implementation of new internal controls or modification of existing controls to account for changing risk points
- Provide transparency to the Audit Committee into the depth of the company's plan for adoption and the reasonableness of the deadlines relative to the company's commitment of resources

Global compliance framework

While not considered heavily regulated when compared to other industries, technology companies innovate and disrupt several highly regulated industries, and are thus faced with the challenge of understanding and complying with a variety of regulatory requirements. For example, a cloud service provider supporting healthcare customers might need to consider HIPAA (Health Insurance Portability and Accountability Act of 1996) privacy rules, or a technology supplier to the Federal Government might have to consider FedRAMP compliance. Separately, a number of technology companies must comply with a myriad of country specific regulations around customer data privacy and competition/anti-trust laws.

In parallel, technology companies are transforming the compliance function to align and integrate compliance requirements throughout the global enterprise. Improved compliance effectiveness can foster a compliance culture that is attuned to multiple stakeholders, and embedded in the enterprise's global governance, planning and operations. For some technology companies, implementing a global compliance framework may just be a natural progression along their compliance journey. For other organizations, it may reflect a much more radical shift from their current approach. Regardless, companies need to achieve a global balance of governance, risk-management, regulatory compliance, and performance. Moving towards a holistic, global model improves cost efficiencies, will better protect the organization's brand reputation, and will better meet the demands of regulators, the board of directors, and key stakeholders.

As a third line of defense, internal audit has traditionally focused on conducting audits to assess regulatory compliance focused on specific regulations such as Anti-Bribery, Privacy, Anti-Trust, etc. Given the rapidly transforming compliance processes and implementation of global compliance frameworks, internal audit can play a key role in this transformation by evaluating the effectiveness of each of the elements of a compliance program.

Example internal audit focus areas:

- Assess the maturity of the company's overall compliance program, as well as key elements such as training, monitoring, investigations, etc.
- Review the compliance function's internal policies and procedures for managing existing regulations and identifying new regulations, and the compliance function's effectiveness in addressing key regulations
- Conduct audits of compliance activity for specific regulations
- Develop an integrated audit approach that addresses compliance risk as part of an overall audit of a business unit or function

08

Drivers:

- Organizations need to adapt people, processes and technology to support compliance activities in light of continually changing internal and external environments
- The pace and complexity of regulatory change, coupled with the increase in regulatory scrutiny and enforcement action by relevant authorities, continues to make compliance a top concern for the Board
- Boards are asking for centralized visibility into the organization's compliance with the rules and regulations applicable to the company
- Increasing focus on developing a consistent compliance culture and framework across the enterprise
- 78% of CFOs and Audit Committee Chairs consider providing compliance feedback as an attribute that makes internal audit valuable, while 68% consider regulatory expertise among the top 10 skills necessary for Chief Audit Executives*

*Forbes Research Insights on Internal Audit -2015

Research and development efficiency

Drivers:

- The rapid pace of innovation requires delivery of the right product at the right time to the market
- Finite R&D budgets demand that funds be allocated to products with the highest return on investment (ROI) to both positively impact today's bottom line and better position the company for future success
- Inefficient R&D spending can create a cycle of missed opportunities, market share loss, and lower funding for future R&D
- R&D spending must be efficient to mitigate the risk of being disrupted by a new competitor or new technology

Technology innovation that creates disruption and transformation is the new way of life. Businesses now realize that they must regularly adapt and evolve to better serve their customers. Operating in a fast-paced, disruptive environment necessitates that technology companies constantly retool their product portfolio while still delivering strong results and shareholder return. The goal is to meet the demands of the market by delivering the right product at the right time. Achieving this requires thoughtful capital allocation to both the current products that fund the business today and tomorrow's products that will drive future growth.

There is a large opportunity for technology companies to more efficiently allocate their research and development (R&D) funding within their portfolio to the products with the highest ROI. Without proper discipline, chasing multiple incremental opportunities that do not generate enough revenue can snowball into multiple generations of delayed key products. This can lead to market share loss or aggressive price discounting, which generates fewer margin dollars to fund future R&D investment. Technology companies can avoid this cycle by embracing disciplined portfolio management and implementing an integrated planning process.

The areas of greatest importance are: (1) alignment of R&D investment with market needs, (2) allocation of the proper resources, and (3) clear financial requirements for the programs to meet. The integrated planning process requires input from sales and marketing, R&D, operations, and finance. The process should capture market requirements within a specified time frame and should align with the R&D organization's ability to deliver. Once the portfolio management team has aligned internal R&D capabilities (and external M&A targets) with opportunities from the marketing organization, they can provide management with a list of potential programs the company should pursue. After financial requirements and analysis, management can rank the potential programs based on the company's strategic priorities and expected ROI.

Once program execution begins, management should make sure the programs with the highest priority are fully resourced and brought to market on time. Linkages between the marketing, R&D, and finance organizations are important to align the company's strategy with its go-to-market approach. The proper channels must be in place to ensure alignment at key junctures of program development and execution. This enables the organization to course correct if changing market requirements impact a program's business case. Identifying these changes early can make the difference between being on time to market for a program, or missing market windows and sustaining heavy losses on an investment.

Example internal audit focus areas:

- Review the consistency of the process by which management establishes the business case and ROI projection for current and future products
- Analyze the data that has been selected for inclusion in the disciplined resource allocation methodology
- Assess risk and difficulty of delivery of future products being considered
- Evaluate the effectiveness of the integrated planning process
- Assess the alignment of the strategic goals to risk management practices



Business continuity management

Drivers:

- Mitigating the risk of business interruption
- Moderating the risk to employee safety and the organization's profitability
- Mitigating the risk to the organization's brand and reputation
- Improving compliance with regulatory and legal requirements
- Improving availability and recoverability across the value chain

Business continuity management (BCM) – consisting of emergency response, crisis management, business continuity and IT disaster recovery activities – is an effective way to instill resiliency in an organization's people, processes, and technology infrastructure, and an effective tool to help ensure the continuity of business operations in the face of a natural or man-made disaster.

Technology companies should consider mitigation plans for situations such as disasters, data security attacks, macroeconomic crises, and other potential disruptions to provide resiliency for ongoing operations. As technology companies continue to migrate customer offerings to the cloud, place more reliance on SaaS vendors for corporate applications, and with supply chain integration being critical to success, technology companies must consider BCM to be critical to the entire value chain, and continue to evolve their BCM programs to extend beyond the organization.

Example internal audit focus areas:

- Assess the maturity of the BCM program, including a remediation plan to mitigate risks and a benchmark comparison against companies of similar size and industry peers
- Evaluate BCM program elements, such as governance and oversight, risk assessments, business impact analyses, continuity strategies and business resumption plans, IT disaster recovery plans (including SaaS and cloud-based systems), and crisis management to determine if plans are current and would be executable in a disaster situation
- Review the integration and alignment of business continuity, IT disaster recovery and cyber breach response procedures
- Review the appropriate elements of the company's BCM program to help ensure alignment with key customer requirements, particularly in the areas of availability and recoverability of customer-facing systems
- Assess supply chain resiliency by identifying critical suppliers and evaluating mitigation plans to address the specific risks, such as sole-sourced components or other single points of failure in the manufacturing and distribution processes
- Review the company's vendor management policies and procedures and evaluate compliance with the company's recovery requirements for key SaaS applications and cloud infrastructure vendors
- Analyze the effectiveness of business continuity exercises and IT disaster recovery tests





How KPMG can help

Our network of professionals has extensive experience working with global technology companies ranging from the FORTUNE 500 to pre-IPO (initial public offering) start-ups. In addition to providing Audit, Tax, and Advisory services, KPMG firms aim to go beyond today's challenges to anticipate the potential long- and short-term consequences of shifting business, technology and financial strategies. KPMG continues to build on our member firms' successes thanks to our clear vision, values, and more than 189,000 people in 152 countries. We have the knowledge and experience to navigate the global landscape.

Internal Audit, Risk and Compliance services

KPMG's advisory Internal Audit, Risk, and Compliance services are designed to help enhance the efficiency and effectiveness of internal audit functions, enterprise risk management programs, reviews of third party relationships, regulatory compliance, governance, and sustainability initiatives. Our professionals bring both deep technical and industry experience, allowing you to strengthen your key governance, risk management, and compliance efforts while at the same time enhancing your business performance. Our experienced professionals can help you navigate the complex demands of regulators, directors and audit committees, executive management, and other key stakeholders, and assist you in transforming disruptive marketplace and regulatory forces into strategic advantages.

About the authors

Tim Zanni

Tim Zanni is the Global and U.S. Technology Leader for KPMG. Tim plays a key client relationship role for the firm's largest global technology accounts. Tim has over 35 years of global experience and his responsibilities include representing the firm in the marketplace, developing marketplace strategies, leading the growth and success of the firm's global technology industry, and helping to ensure that our clients receive outstanding service. Prior to his global role, Tim served as the Silicon Valley managing partner for seven years and before that, in a leadership role in KPMG's New York office. Tim has also worked in KPMG's executive office in the Department of Professional Practice, which helps KPMG professionals and their clients address and resolve complex accounting, reporting, and SEC-related issues. Tim is the current host and former moderator of KPMG's Audit Committee Roundtable series and current moderator of KPMG's Audit Committee Chair Peer Exchange.

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 vital to technology firms.

Ron Lopes

Ron is the Advisory Leader for KPMG's Silicon Valley practice and has more than 25 years of 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.

Contributors

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

Chad Poplawski, Managing Director, Advisory

Robert Rosta, Associate Director, Technology Marketing

Contact us:

Timothy Zanni

Global and U.S. Chair,
Technology, Media and Telecommunications
408-367-4100
tjzanni@kpmg.com

Richard Hanley

Advisory Leader,
Technology, Media and Telecommunications
408-367-7600
rhanley@kpmg.com

Tom Lamoureux

Risk Consulting Leader,
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



©2017 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.

The KPMG name and logo are registered trademarks of KPMG International