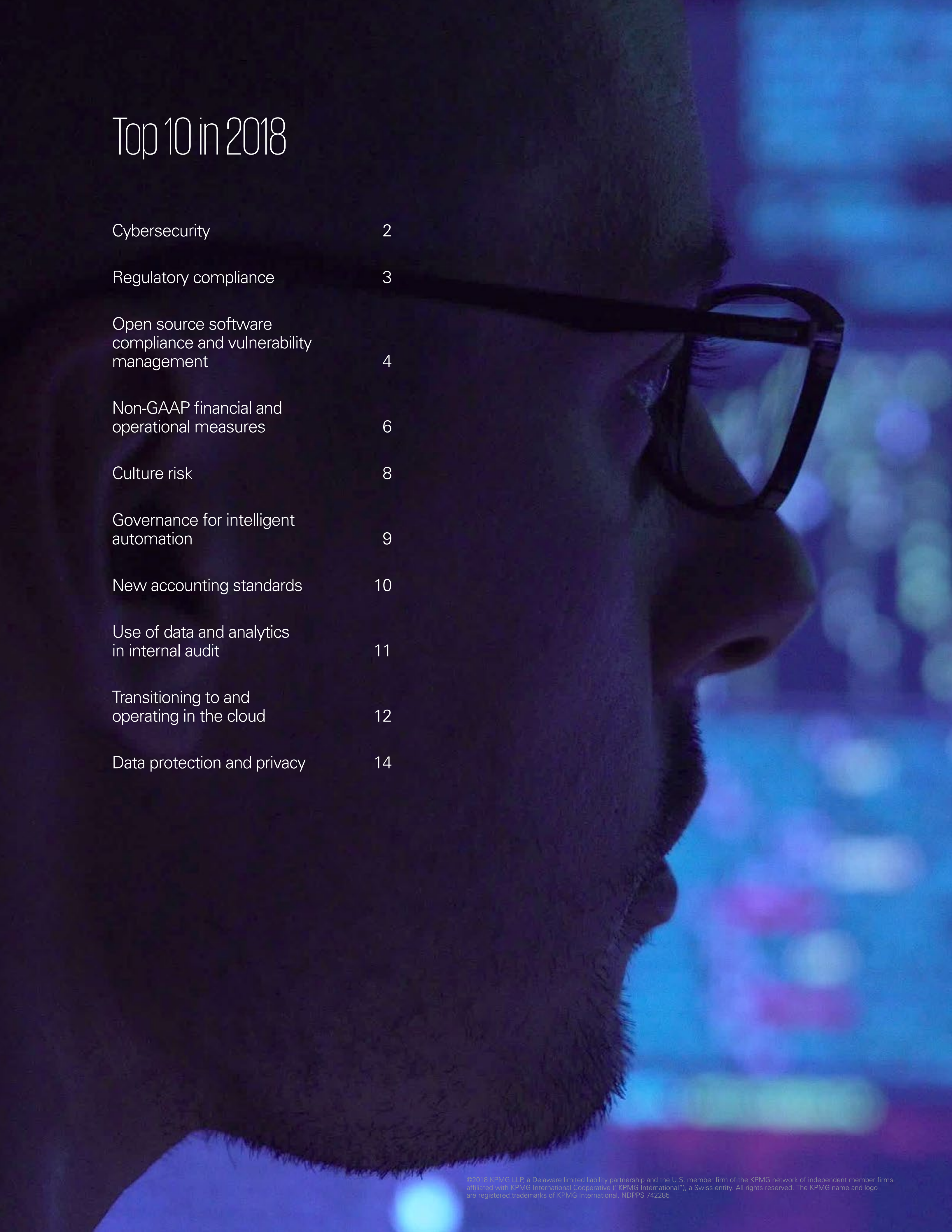
KPMG

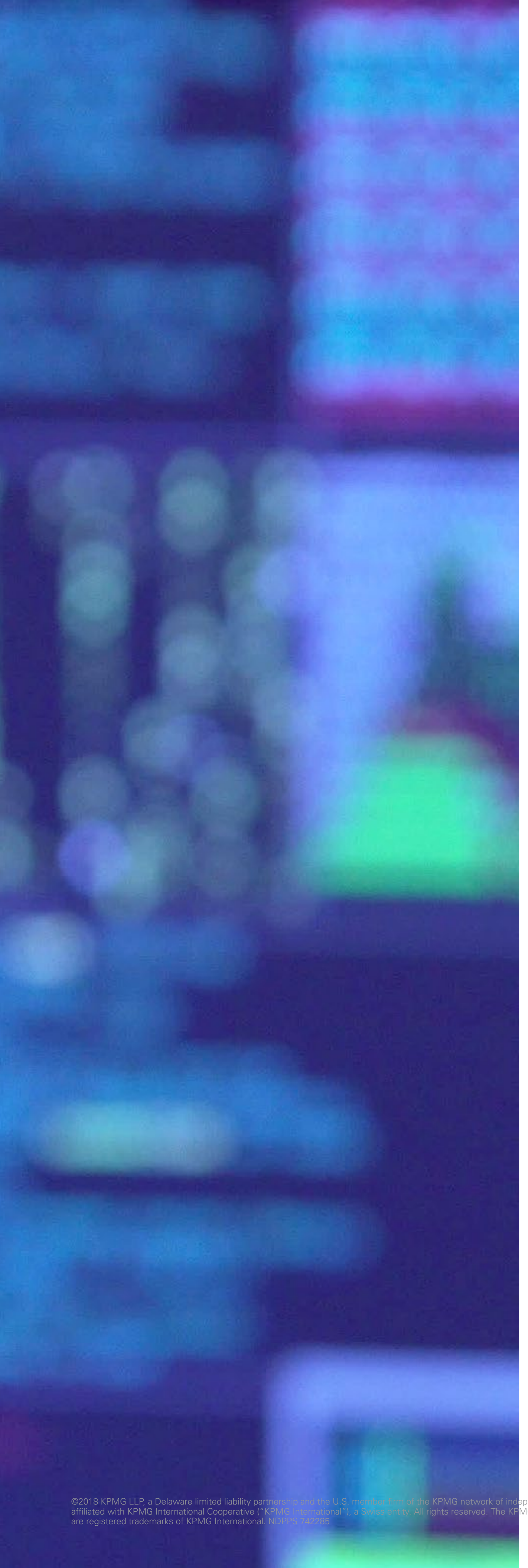
Strategies for the third line of defense

Top 10 internal audit focus areas for technology companies in 2018

kpmg.com



Top 10 in 2018



Internal audit strategies are critical as technologies evolve and business environments change

A number of megatrends continued to manifest themselves in 2017 and early 2018. Cyber breaches seem to be growing in scope and frequency. The importance of integrity and a strong corporate culture is more important now than ever, especially for technology companies. Artificial intelligence (AI) and data and analytics (D&A), in their many forms, are accelerating their impact on our workplaces and personal lives. New regulations surrounding accounting standards and data protection are here instead of "coming down the road."

For internal audit (IA) professionals at technology companies, these issues and a host of others have created a new risk matrix, placing greater priority than ever before on the efficient oversight of corporate governance, internal controls, and regulatory compliance.

As always, our annual top 10 focus areas represents our assessment of the key challenges facing technology companies right now. Of course, every technology company is unique. It is critical that IA as a function takes a company-specific view of the risks involved in the development and prioritization of its own focus areas.

As in past years, our focus areas are informed by the insights we have gathered from several sources, including:

- Conversations with audit leaders at a variety of established and emerging technology companies
- Our technology industry IA share forums
- Input from KPMG professionals whose work gives them specific perspective on the priorities of the technology sector
- Relevant KPMG survey findings

In the end, it is not important if our #6 is your #2 and our #1 is your #4. What is significant is that, collectively, this list inspires you to think critically and develop strategies for combating the internal and external threats that can keep your organization from innovating and growing.

01

Cybersecurity

Drivers:

– Adopting new policies and procedures to protect personal data and manage data transfer channels

– Avoiding costly consequences of data breaches such as investigations, legal fines, coverage of customer losses, remediation efforts, loss of executive and midlevel 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 personal 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 automated services, more stringent and diverse regulatory environments (especially around personal data protection), 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 personal data protection policies. Internal audit can execute technical and process-driven assessments to identify and evaluate cybersecurity risks and offer strategies and recommendations to help mitigate the identified risks.

Example focus areas for internal audit:

– Perform a top-down risk assessment around the company’s cybersecurity process using industry standards as a guide, and providing recommendations for process improvements

– Assess personal data transfer channels and lineage to confirm alignment with stakeholder documentation and understanding

– Evaluate existing processes and controls, such as data retention policies or identity access management 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 personal data breach and broader incident response planning

Regulatory compliance

Companies, regardless of industry, have numerous domestic and foreign regulatory requirements that they need to comply with. Technology companies in particular often converge with other industries and move into new geographies at a rapid pace. This can quickly make them subject to new regulations with which they are not familiar. An increase in applicable regulations increases the burden on technology companies' chief compliance officers and their staffs. This in turn increases the possibility that some compliance requirements will be missed.

Satisfying new regulations adds considerable cost to compliance budgets and complexity to internal structures and information needs. Meanwhile, mergers and acquisitions continue, which means companies need to combine their existing compliance function with that of the acquired entity and ensure a holistic approach to compliance.

Example focus areas for internal audit:

- Take inventory of regulatory bodies and requirements affecting the company
- Assess the company's approach to managing its global compliance responsibilities, including integration of the requirements of acquired companies
- Proactively support management in the development of compliance programs and controls
- Conduct/facilitate risk assessments and support or lead investigations
- Evaluate the company's response to any notable instances of noncompliance
- Ensure compliance training programs offered to employees and other stakeholders are appropriate for role and geography
- Perform activities as directed by the compliance team when visiting locations to minimize inefficient duplication of effort while still achieving objectives

02

Drivers:

- Increasing importance of effective corporate compliance programs
- Ensuring compliance with domestic and foreign regulations
- Increased global cooperation among regulators and enforcement agencies
- Mitigating the increasing costs of complying with an ever-growing number of regulations
- Developing a strategy to lessen the restraining effects of compliance-related activities on business operations
- Ensuring compliance operations are aligned following a merger or acquisition

03

Open source software compliance and vulnerability management

Drivers:

- Observing all copyright notices and satisfying license obligations for open source software used in conjunction with commercial products and internal software
- Avoiding restrictions on the use of open source code used commercially (such as, in some cases, being forced to share the source code publicly)
- Identifying and tracking potential vulnerabilities in deployed open source code (such as the Heartbleed virus)
- Providing management with a timely view on identified open source compliance and vulnerability risks to facilitate quick remediation

Today, developers are leveraging more than 50 percent of open source software (OSS) in their proprietary applications. This speeds up time-to-market and progresses technological innovation. However, in the current environment, security vulnerabilities, data breaches, and compliance lawsuits are real concerns. Organizations that do not manage OSS assets proactively are putting their security and license compliance obligations at risk.

This especially applies to an organization’s commercially developed products, where understanding licensing restrictions and the implications associated with the use of OSS components in externally distributed products is imperative. Companies that are not on top of their OSS assets may be forced to publicly release the source code of their commercial applications if license terms are breached. In addition, companies need to understand all aspects included in the software build and the potential vulnerabilities associated with the open source components used. For example, an older version of Struts can expose an organization to potential hacks.

Example focus areas for internal audit:

- Perform a top-down risk assessment of the organization’s open source compliance management processes using industry standards as a guide and provide recommendations for governance and process improvements
- Review technical due diligence procedures for identifying and interpreting potential open source compliance liabilities for acquisition targets
- Audit a sample of commercial products and/or internal software currently in use to identify potential OSS license compliance issues and security vulnerabilities
- Provide recommendations for the design and implementation of new internal controls or modification of controls to improve OSS compliance and security for both product design and build, as well as ongoing monitoring

```
if ($_COOKIE['lang'] =='rus') {
ководство проектами";

ojektu vadiba";
/li>
<a href="foto-galerija.php">
<? if ($_COOKIE['lang'] =='eng'){
 "Foto galery";}
if ($_COOKIE['lang'] =='rus') {
тогалерея";

oto galerija";
:/li>
<a href="sadarbibas-partneri.php">
 <? if ($_COOKIE['lang'] =='eng'){
o "Partners";}
eif ($_COOKIE['lang'] =='rus') {
артнеры";

adarbibas partneri";
</li>
><a href="kontakti.php"><? if ($_COOKIE['lang'] =='eng'){
o "Contacts";}
eif ($_COOKIE['lang'] =='rus') {
онтакти";

ontakti";
</li>
><a>&nbsp;</a></li>



les/slider.php");

argin">

r">
t1">
rc="pic/house.png" alt="house" />&nbsp;&nbsp;<? if ($_COOKIE['lang'] =='eng'){
ho "About the company";}
seif ($_COOKIE['lang'] =='rus') {
) предприятии";

Par uzņēmumu";
>
IE['lang'] =='eng'){
paruzneng;

COOKIE['lang'] =='rus') {
paruznrus;

paruznlv;
```

04 Non-GAAP financial and operational measures

Drivers:

- Incomplete or inaccurate information may damage company reputation in the eyes of the public
- Increased scrutiny by regulatory bodies (e.g., SEC) on the accuracy of non-GAAP measures, including concern that measures may be misleading, hard to interpret, and confusing

Technology companies include non-GAAP financial and operational measures in their earnings releases and other informational material to provide investors, analysts, venture capital firms (VCs), and bankers richer insights into performance and results. Consumers of non-GAAP financial and operational measures rely on this information to make key investment and other financial decisions. Incomplete or inaccurate information may damage company reputation in the eyes of the investor community or result in possible punitive action by regulatory authorities. The U.S. Securities and Exchange Commission (SEC) and other regulatory bodies are increasingly scrutinizing the reporting of non-GAAP financial measures. As a result, companies reporting non-GAAP financial measures may face the risk of having to:

- Eliminate certain non-GAAP financial measures in earnings releases and company disclosures
- Revise calculations and reporting of non-GAAP financial measures
- Face enforcement actions by the SEC or other federal regulatory authorities

Despite these potential risks, the use of non-GAAP financial measures to supplement communications under U.S. GAAP (Generally Accepted Accounting Principles) continues to increase. Likewise, private companies continue reporting similar measures to their investors who rely on this information to better understand the company's performance, strategy, and initiatives and in many cases, assess its valuation. Companies believe that these non-GAAP measures more accurately reflect their value to potential investors.

Internal audit can play a key role by helping management understand the risks associated with the nature and extent of reporting non-GAAP financial and operational measures, and assisting in the development of strategies to help mitigate the risk of inaccurate financial information.

Example focus areas for internal audit:

- Identify the non-GAAP financial measures being reported that are covered under SEC regulations, as well as operational measures being reported. Consider factors such as:
  - The use of the financial/operational measure reports
  - The importance of such measures to investors and other users
- Assess the processes, procedures, and controls that apply to non-GAAP financial and operational measures (non-GAAP measures fall under Disclosure Controls and Procedures and require officer certification). For example:
  - Formalize and document the process of calculating and reporting these non-GAAP financial and operational measures similar to the way you would treat internal controls over financial reporting (ICOFR) or SOX controls (e.g., process narratives or flowcharts). Consider establishing an internal policy to document and ensure how the non-GAAP financial and operational measures are transparent, consistent, and comparable.
  - Identify and document key risks, corresponding internal controls, and/or gaps to address the risk (e.g., risk and controls matrices)
  - Design controls over non-GAAP financial and operational measures so they address compliance with regulations, completeness and accuracy of source data, reconciliation to GAAP or comparable measurement, consistency between periods, review and monitoring by the appropriate level of management, and monitoring of related IT systems and applications
- Ascertain whether internal controls over the calculation and reporting of non-GAAP financial and operational measures are appropriate. This includes non-GAAP financial measures that are disclosed in earnings releases furnished on Form 8-K.
- Perform controls testing on a periodic basis (e.g., quarterly) to gain insight into the operating effectiveness of these controls related to the calculation and reporting of non-GAAP financial and operational measures

Despite the potential risks, the use of non-GAAP financial measures to supplement communications under U.S. GAAP continues to increase.

05

Culture risk

Drivers:

- Increased investor attention
- Growing regulatory scrutiny
- Heightened focus on reputational/brand risk as a concern among global CEOs[1]
- Global organizations placing high priority (74 percent) on trust, values and culture in order to sustain their long-term future[1]
- Majority of global CEOs (72 percent) correlating being a more empathetic organization with higher earnings[1]

[1] KPMG International, Disrupt and Grow, 2017 Global CEO Outlook

Culture risk has gained the attention of technology company leaders as a leading cause of highly visible incidents of misconduct that have impacted the public's trust. Even if a company has a well-defined strategy, if the company culture does not support its execution, success is less likely. Over 90 percent of CEOs and CFOs believe that improving culture would improve the value of their company. Only 15 percent believe their culture is where it needs to be.[2] Companies with weak cultures have been shown to experience misconduct rates up to ten times higher than those with strong ethical cultures.[3]

Culture can be observed, monitored, and changed over time to mitigate misconduct and encourage desired behaviors. A broad cultural dynamic that addresses the specific issues of governance, compliance, and risk management will invariably also focus on understanding how the organization makes decisions to meet the demands of its various stakeholders, and how these decisions, in turn, influence the culture—both current and desired. Stakeholders, resources, and skills should be aligned and available prior to internal audit starting any reviews.

Example focus areas for internal audit:

- Conduct an assessment to determine if the day-to-day cultural drivers are aligned to the organization's core values and mission statement
- Review the alignment between performance measures and core values to ensure desired behaviors are being incentivized and rewarded
- Provide assurance regarding the evolution and alignment of the organization's culture with compliance activities, as well as financial objectives and business and operating models
- Assess the quality of the cultural drivers that are preconditions for the operating effectiveness of controls
- Surface culture risk through data analytics and third-party audits
- Lead or participate in investigations into matters involving potential misconduct
- Drive continuous improvement through testing and evaluation of the organization's culture change program, include cultural aspects in reporting
- Perform systematic root cause analysis on audit findings and other non-compliance incidents with specific consideration of soft controls

[2] "Corporate Culture: Evidence from the Field"; Graham, Harvey, Popadak, and Rajgopal; Duke University 2015. Richard Chambers GAM Presentation, 2016.

[3] "Research Reveals That Integrity Drives Corporate Performance: Companies With Weak Ethical Cultures Experience 10x More Misconduct Than Those With Strong Ones"; PR Newswire; September 2010.

Governance for intelligent automation

06

Intelligent automation—such as robotic process automation, machine learning, and cognitive solutions—is changing the world of business right before our eyes. This new technology that both complements and augments human skills has the power to exponentially increase enterprises' speed, scale, quality, precision, and operational efficiency.

Smart machines now perform activities, and even make decisions, that were previously the domain of humans—and they do it faster, more accurately, and at far greater scale. The days when employees clock in to work just to repeat mundane, manual tasks over and over will soon be a distant memory.

Given its clear benefits and numerous use cases, it is no wonder intelligent automation has become a mission-critical initiative. But when embarking on such an important digital transformation project, companies must remain vigilant. Companies must be cognizant of the risks related to intelligent automation tools and applications and the accompanying governance responsibilities. A well-designed risk and governance function helps ensure that intelligent automation programs avoid business disruption and noncompliance and that the associated risks are effectively identified, evaluated, and mitigated—or accepted, where appropriate.

The biggest risk associated with intelligent automation is business disruption. Additional risks include skill gaps, inconsistent developer training, lack of change management processes, insufficient cybersecurity, and a lack of or ineffective controls. Multiple factors can create an unstable bot environment and increased bot failure rates. And when your bots stop working, so does your business.

A lack of well-defined automation program guidelines can prevent the organization from satisfying governance, risk, controls and compliance requirements. This could damage relationships with partners, auditors, and regulators, potentially resulting in significant fines. Noncompliance can lead to program instability and operational failures. Organizations that deploy intelligent automation programs may need to provide formal assurance that they are abiding by relevant regulatory and compliance guidelines. Identifying impacted internal and external compliance requirements should be one of the first considerations when implementing an intelligent automation program.

Example focus areas for internal audit:

- Integrate governance, risk management, and controls throughout the automation program life cycle
- Identify opportunities to embed automation-enabled control activities within the impacted business processes
- Capitalize on intelligent automation labor innovations to increase the efficiency and effectiveness of internal audit activities

Drivers:

- The digitization of labor is rendering traditional ways of operating a business obsolete
- Technology leaders are maintaining or ramping up investment in innovation, particularly digital labor
- Artificial intelligence, cognitive computing, and robotics are among the top technologies that will drive business transformation going forward

07

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 have driven significant changes in both U.S. GAAP and International Financial Reporting Standards (IFRS). As a result, companies have been evaluating the impact of these new standards, which include accounting for revenue from contracts with customers, leases, financial instruments, etc., and developing an approach for implementing the new standards. As the U.S. GAAP new revenue standard went into effect for public calendar year-end companies with annual reporting periods beginning after December 15, 2017, many are now switching focus towards the new leasing standard, which is effective for public companies with annual reporting periods beginning after December 15, 2018.

The new leasing standard now requires lessees to recognize all leases, including operating leases, with a term greater than 12 months on-balance sheet. This is a significant change as it will require companies to inventory and reasses their entire lease populations, which may prove onerous depending on the structure of the company (centralized vs. de-centralized) and whether formal leasing processes are currently in place and documented.

Due to the magnitude of the lease population for some companies, selection of a leasing tool may be necessary. This brings a whole host of new issues as they relate to controls around the collection and migration of data to support the completeness and accuracy of the information. Companies will need to ensure that systems, processes, and controls being implemented are sufficient to capture information needed for the new expanded disclosures.

Example focus areas for internal audit:

- Perform an impact assessment (gap analysis) around how the new standards impact the company, 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, including assessment of what new internal controls may be required
- Update understanding of the flow of information through the existing system and how the flow of information will occur using any new software solutions
- 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, considering both controls over transition and ongoing controls
- 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

Use of data and analytics in internal audit

08

The term "data analysis" is often used to refer to automation and the use of advanced technologies, as well as the analysis of data. The goal of data analysis is to improve decision making, which can occur through one or more of the following:

- Better understanding of the data and processes that create the data
- More timely access to data
- Access to more data
- Improved consistency in the data being used to make decisions

Companies often begin with analyzing business processes where either the company has access to a reasonable quantity of quality data and/or where the company has some analytical efforts occurring already. Starting small, such as with a proof of concept, enables companies to develop and refine their vision for how the resulting tools and insights will be used to achieve the organization's missions and objectives.

Internal audit teams might start by automating manual activities that already occur with regularity (e.g., monthly or quarterly). When ready, teams might then look to projects where existing analytics are migrated onto advanced technology platforms and expanded upon. Another place where teams can start is with developing discrete analytical tools (e.g., automated data collection, pre-defined data cleansing and /or preparation procedures, dashboard templates) for higher-risk processes that are reviewed annually. Over time, increased use of advanced data analytics should result in improved insights, as well as decision making, concerning risks and controls.

Some of the emerging trends in D&A in internal audit for 2018 include:

- Undertaking formal data analytics assessment projects, including strategy development and pilot initiatives
- Consolidating disparate analytic efforts into a single platform to realize the benefits of data blending
- Partnering with other internal organizations to maximize budget and resources to undertake data analytics projects (e.g., information technology, compliance)
- Hiring resources with technical skills in anticipation of establishing and maturing data analytics programs for the longer term

Example focus areas for internal audit:

- Examining current processes to identify activities and projects in which data analytics and/or automation could provide efficiencies
- Evaluating higher risk business processes to identify whether or not data analytics could facilitate transparency and oversight

Drivers:

- Improve internal audit knowledge and awareness of enterprise activities
- Facilitate data-driven risk assessment
- Increase effectiveness of internal audit activities
- Enable earlier detection of potential fraud, errors, abuse, and regulatory non-compliance
- Free resources by automating repetitive tasks
- Reduce human error associated with analysis
- Improve the quality of reporting
- Improve speed to insight in response to inquiries and investigations

09

Transitioning to and operating in the cloud

Drivers:

– Reducing the capital investment and ongoing 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 and operating in the cloud environment, allowing management to course correct or put risk mitigation strategies in place in a timely manner

– 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 business applications and IT infrastructure perspectives. 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, cloud based services offer faster access to tools and expertise that are not always readily available within an organization, thus allowing for rapid adoption of newer technologies and tools with minimal investment (both system/implementation and personnel). It further augments rapid development methodologies by providing on-demand and easily scalable resources, thereby cutting down time-to-market for new products and prototypes. More and more technology companies are operating their IT infrastructure in the cloud, both in public and private clouds, and are leveraging 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 versus 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 consuming cloud services, such as:

– Risk of security and/or control failures at the cloud service providers and potential loss of control over data or data leakage

– Properly tracking and monitoring the usage of cloud service by its employees and preventing abuse of such services

– Potential contractual breach with customers or violation of regulatory requirements (e.g., data sovereignty requirements, data privacy requirements, etc.)

– Risks associated with the implementation or transition, such as budget and schedule overruns, completeness of requirements/design, and project resourcing

– Risk of operational failure is proportional to the size of the operating environment, and increase in cloud consumption may introduce additional operational risks

– Properly designing controls and checks to ensure they do not result in compliance fatigue for the employees (e.g., automated controls versus manual controls)

– Properly defining metrics and measuring the services' 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 as well as evaluating and reporting on risk mitigation activities throughout the operation and consumption of the cloud services. Internal audit can be a key partner with the business in helping to ensure a smooth adoption and successful operation of cloud-based technologies.

Example focus areas for internal audit:

- 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
- Ensure threat modeling and risk assessments are performed and security requirements are developed and integrated within implementation plans and day-to-day operating procedures
- 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
- Periodically review the compliance posture of the cloud service providers (i.e., conduct on-site audit, review third-party audit reports, etc.) to determine whether the cloud service provider maintains an acceptable level of controls
- Review management's plan to monitor the usage of cloud services, including the plan for security monitoring and insider threats/abuse
- Review existing policies and procedures to determine suitability for cloud-based deployments and operations, and evaluate management's plan for business continuity and disaster recovery for the cloud operations (e.g., participate in business continuity disaster recovery exercise)
- Evaluate the organization's change management and business readiness plans around the implementation of the cloud solution
- Assess management's approach to designing and implementing controls to help ensure control efficiency and effectiveness, and an appropriate ratio of automated to manual controls
- 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

More and more technology companies are operating their IT infrastructure in the cloud, both in public and private clouds, and are leveraging benefits such as the rapid scalability of IT infrastructure, platform flexibility, and high availability/reliability.

10

Data protection and privacy

Drivers:

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

As technology companies navigate continued globalization, technology innovation, and business model evolution, information security and privacy protection are clear priorities. Data breaches are in the headlines almost daily. With the increased use of cloud and social platforms, companies need to ensure data is safe. If privacy and security are not constantly re-addressed, organizations can be exposed to a host of risks ranging from the breach of personal information/identity theft, fraud, access management issues, system availability, and company reputation damage.

From a regulatory perspective, the European Commission finalized the introduction of the General Data Protection Regulation (GDPR) in December 2015. Its official adoption was in May 2016, and enforcement starts in May 2018. The GDPR is the biggest and most impactful change on privacy and data protection in recent history and introduces a range of new requirements for organizations in relation to data protection.

The GDPR is a fundamental game changer, and its impact is comparable to the impact of Sarbanes-Oxley on internal controls over financial reporting, especially for technology companies. It introduces a broader geographic reach, meaning that provisions of certain European Union (EU) regulations will be applicable to organizations outside the EU. The potential impact of the GDPR on an organization's bottom line can include fines as high as four percent of global turnover and increased reputational risks. As a result of GDPR, organizations need to demonstrate continuous data protection compliance. This can include:

- Extended privacy rights to the data subjects
- Increased transparency and accountability requirements from organizations
- Obligations to report personal data breaches within 72 hours
- Implementation of data privacy by design, embedding privacy in relevant processes and systems
- Appointment of data protection officers positioned independently within the organization

Example focus areas for internal audit:

- Assess the potential impact of GDPR on the organization’s information governance strategy and budget
- Integrate GDPR requirements into the organization’s annual audit program to assist in improving GDPR compliance
- Evaluate the compliance of business partners or third-party providers and understand the compliance initiatives they are undertaking
- Review security monitoring and detection programs, as well as controls, with a focus on Security Incident Event Monitoring (SIEM)
- Examine the data breach notification process for regulatory and legal compliance
- Help ensure that employees have only the necessary levels of access to systems and data
- Assist with creating and delivering security and privacy training (e.g., password protection, information risks, and appropriate handling of confidential customer/employee information, etc.)
- Perform security audits around cloud and social platforms

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 member 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 200,000 people in 154 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 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 serves as KPMG's Risk Consulting Leader for the Technology, Media, and Telecommunications practice. In this role, he guides the delivery of KPMG advisory services to some of the world's leading technology companies to help them create leading 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.

Chad Poplawski

Chad is an Advisory Managing Director in KPMG's Silicon Valley practice with more than 20 years of experience in the technology sector. He has delivered business consulting, system implementation, internal audit, and Sarbanes-Oxley (SOX) services and solutions to a range of clients, from pre-IPO and recently public companies to well-established multinational entities. Chad has extensive experience assisting clients with internal audit, enterprise risk assessments, process reviews, internal control assessments, IT project reviews, and SOX 404 programs, from documentation to testing to remediation. Chad is currently focusing on emerging companies, both pre-IPO and newly public, and has helped several clients in this space address their unique set of needs around internal controls readiness, SOX compliance, cloud/SaaS solutions, and IT risk assessment.

Contributors

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

Ron Lopes, Partner, Advisory

Parth Jhaveri, Director, Advisory

Robert Rosta, Associate Director, Technology Marketing

Contact us:

Timothy Zanni
Global and U.S. Technology Sector Leader,
Chair of Global and U.S. Technology, Media, and
Telecommunications Line of Business
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

Chad Poplawski
Managing Director, Advisory
408-367-7639
cpoplawski@kpmg.com

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

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