



**KPMG Internal Audit:**

# Top 10 in 2018

**Considerations for impactful  
internal audit departments**

[kpmg.com](http://kpmg.com)



234	113	215	876	234	113	215	876
34	216	745	345	34	216	745	345
657	410	465	890	312	906	321	145



234	113	215	876	234	113	215	876
34	216	745	345	34	216	745	345
657	410	465	890	312	906	321	145
1233	432	987	523	412	234	753	1236
987	523	412	234	978	432	709	2315
234	113	745	890	34	113	215	876
34	216	465	523	234	216	745	345
657	410	987	876	34	906	321	145
1233	432	412	234	978	234	753	1236
987	523	215	345	312	234	709	2315
234	113	745	890	412	432	215	876
34	216	465	523	234	113	745	345
657	410	987	876	34	906	321	145
1233	432	412	234	978	234	753	1236
987	523	215	345	312	234	709	2315
234	113	745	890	412	432	215	876
34	216	465	523	234	113	745	345
657	410	987	876	34	906	321	145
1233	432	412	234	978	234	753	1236
987	523	215	345	312	234	709	2315



Competing in a rapidly changing world, companies must grapple with emerging challenges seemingly every day: new regulatory requirements, changing accounting standards, third-party relationship risk, and more. All of these challenges bring both risks and opportunities. Identifying the fine line between the two factors is critical. Because only 10 percent of CFOs and audit committee chairs responding to the recent KPMG/Forbes “Seeking Value through Internal Audit” study feel their internal audit (IA) function adequately identifies and responds to emerging risk, the area is ripe for IA leadership. In fact, IA can play an important role in helping organizations manage the risk environment while making progress on strategic priorities.

An impactful IA function will stay current with wide-ranging business issues as they emerge so it can help monitor related risks and their potential effects on the organization. To provide the greatest value, IA must find opportunities to challenge the status quo to reduce risk, improve controls, and identify potential efficiencies and cost benefits across the organization.

To help IA functions achieve these goals, we present KPMG Internal Audit: Top 10 in 2018, which outlines areas where IA should focus so it can effectively add value across the organization and maximize its influence on the company.

## Top 10 in 2018

<b>1. Accounting standards</b>	<b>Page 2</b>
<b>2. Culture risk</b>	<b>Page 3</b>
<b>3. Digital labor governance</b>	<b>Page 4</b>
<b>4. General Data Protection Regulation</b>	<b>Page 5</b>
<b>5. Non-GAAP financial measures</b>	<b>Page 6</b>
<b>6. Integrated assurance</b>	<b>Page 8</b>
<b>7. Third-party relationships</b>	<b>Page 9</b>
<b>8. Cyber breach/crisis preparedness and response</b>	<b>Page 10</b>
<b>9. Anti-bribery/anti-corruption</b>	<b>Page 11</b>
<b>10. Talent acquisition and retention</b>	<b>Page 12</b>





# 1

## Accounting standards

### Drivers:

- Ensuring company readiness for changing accounting standards
- Coordinating with external auditors to understand their expectations and how they view the current state of implementation
- Assurance on post-implementation controls within changed processes
- Simultaneously navigating tax reform legislation and the resulting demands on Finance organizations

Starting in 2018, a wave of new accounting standards begins with the introduction of the new revenue standard. Accounting Standards Codification (ASC) 606: Revenue from Contracts with Customers arguably represents one of the most significant changes to accounting standards in recent history and may require substantial time and investment to make fundamental changes to the areas of people (e.g., resourcing levels, capabilities), processes, and technology. The new revenue recognition standard is intended to simplify and harmonize more than 150 pieces of current U.S. GAAP revenue literature, developed over multiple decades, into a single, principles-based standard. A specific challenge for many companies is the variety of customer contractual arrangements present in the operating environment.

The new lease accounting standard takes effect on January 1, 2019 for calendar year-end public companies. The new rules require lessees to recognize leases on their balance sheets instead of as operating leases. The new standard will require grossing up the balance sheet with a right-to-use asset and lease liability that reflects the remaining lease obligation. Companies will need a system to track all leases, along with the necessary amortization each period.

The new standards are highly technical and represent a tremendous shift in expectations. Further, with the convergence of IFRS, the new standards are less specific and require a significant level of interpretation and judgment by management. Add to this the impact of recent tax reform legislation, and Finance organizations will be at capacity for the foreseeable future.

This features as a top risk for 2018 because the new requirements are complex, companies are tracking behind in their readiness, and the Securities and Exchange Commission (SEC) will be closely scrutinizing the implementation and related disclosures under Staff Accounting Bulletin (SAB) 74: Disclosures and Controls for New Accounting Standards.

### How internal audit can help:

- Conduct pre- and post-implementation assessments to understand the organization's response to the new requirements; how changes in people, process, and technology have been managed; and related updates to the control environment
- Evaluate the effectiveness of processes in place that determine the business units/processes affected by new revenue recognition and lease accounting rule changes, as well as assess the effectiveness of change management, training, and education
- Evaluate controls associated with adoption of the new standards, including the completeness and appropriateness of disclosure controls under SAB 74, and new footnote disclosure items
- Assess the impact of the new standards on processes such as contract management (for leases and revenue) and sales commissions
- Evaluate the reliability of key reports now utilized as part of the revenue/lease recognition process

# 2

## Culture risk

Culture risk has gained the attention of company leaders as the cause of many 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. Culture can be observed, monitored, and changed over time to mitigate misconduct and encourage strategic behaviors. A broader cultural program, while addressing the specific issues of governance, compliance, and risk management, will also focus on understanding how the organization makes decisions to meet the demands of its various stakeholders, and how these decisions influence culture, both current and desired.

### How internal audit can help:

- Conduct an assessment of the organization's cultural drivers in relation to the organizational norm
- Evaluate the alignment of performance measures to strategy to help ensure desired behaviors are being incentivized and rewarded
- Provide assurance regarding the evolution and alignment of the organization's culture with its compliance activities, its financial objectives, and its business and operating models
- 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



### Drivers:

- Heightening regulatory scrutiny and increasing cultural expectations
- Increasingly global organizations with much more varied cultural norms and practices
- Social media outlets and the ability for incidents of misconduct to be widely broadcast
- Stricter governance, oversight, and accountability expectations



## 3 Digital labor governance

### Drivers:

- Identifying priority areas for technological transformation
- Developing a multifaceted strategy and road map for the workforce of the future
- Establishing a governance strategy and program to help companies realize and maintain the expected value and benefits from digital labor initiatives

The convergence of robotic process automation, machine learning, cognitive computing, artificial intelligence, and advanced analytics is driving extremely rapid business model transformation. By 2025, automation of work enabled by digital technologies is expected to supplement or replace the work of the preponderance of knowledge workers. As the processing power, cost, and performance of technologies that enable digital labor continue to advance at a dizzying pace, companies need to fully understand the coming changes—including tax, governance, and contractual implications to outsourcing arrangements—and take the steps necessary to avoid business disruptions.

As more and more robots and other cognitive technologies work side-by-side with a human labor force, leaders are increasingly challenged to integrate and make the most of both kinds of labor. It is important to understand and prepare for the potential impacts that digital labor will have on the shape and size of organizations. A structured approach to digital labor governance is critical to help ensure the benefits are realized and the risks are mitigated. Companies will need controls over technologies deployed, including development and implementation, as well as audit logging, testing, and general system controls.

### How internal audit can help:

- Evaluate the company's governance process for building, managing, and monitoring digital labor
- Discuss with management the company's future expectations regarding transformation of the workforce and plans to address the coming changes
- Risk assess management's plans and processes in light of other risks in the organization and help ensure transparent communication to the audit committee
- Perform an assessment of the Human Resources department's capabilities in light of evolving labor models, including a need for new thinking around behavioral economics, systems, analytics, and consultancy skills

# 4

## General Data Protection Regulation (GDPR)



The digital revolution is significantly transforming how organizations do business. At the same time, emerging technologies and big data introduce challenges and risks when it comes to safeguarding data and adopting appropriate data privacy governance models. In response to these risks, a game changing regulation has been introduced in the European Union (EU)—the General Data Protection Regulation (GDPR). GDPR is relevant to most companies due to the multinational nature of operations today. Specifically, GDPR will have an impact if a company has operations in the EU, offers free or paid goods or services to EU residents, or monitors the behavior of EU residents.

If this regulation has not yet captured your organization’s attention, it should. Fines for noncompliance are up to 4 percent of global annual sales from the prior year, or €20 million, whichever is greater. All indications are that data privacy authorities are serious about enforcement.

New requirements will mandate examination and risk assessment of operational practices across a wide variety of functions, including research and development, human resources, sales and marketing, and regulatory compliance. GDPR will be in effect on May 25, 2018, and despite aggressive efforts, many companies will not be in full compliance by the deadline.

### How internal audit can help:

- **Get connected to the organization’s GDPR response in order to provide input into program governance and implementation activities**
- **Support organizational risk assessment to help ensure both program and organizational resources are dedicated to the highest risk and highest impact areas**
- **Help spot exposures and/or gaps in the organization’s response early in the process through in-stream program assessment and audits**



### Drivers:

- **Ensuring compliance with a dramatically increasing number of global regulations**
- **Mitigating the increasing costs of complying with this ever-growing number of regulations**
- **Understanding the full breadth of impact from global regulations and related impact on business operations and processes**



## 5 Non-GAAP financial measures

### Drivers:

- Increasing use of non-GAAP measures in reporting financial performance
- Management latitude in deciding which measures to use
- Unaudited data sources for the financial measures, which often lead to stock price movement
- Increased focus by the SEC on governance surrounding non-GAAP financial measures

A non-GAAP financial measure is a numerical measure of a company's historical or future financial performance, financial position, or cash flows that is not determined under U.S. Generally Accepted Accounting Principles (GAAP). Non-GAAP financial measures are often presented in conjunction with GAAP measures in earnings releases and other communications to provide investors with additional information and insight into a company's historical and future financial performance. One common example is adjusted earnings, which may be used to remove nonrecurring items from GAAP earnings to provide a better year-over-year comparison of financial performance.

While GAAP measures are audited and provide a reliable and standardized method for understanding a company's historical and future financial performance, management generally decides which non-GAAP financial measures are used and how they are calculated. There is no audit requirement or standard method for calculating non-GAAP financial measures. As a result, similarly titled non-GAAP financial measures may not be consistently calculated across the company's industry. Additionally, companies within the same industry may present entirely different non-GAAP financial measures, which may lead to a lack of comparability. For these reasons, controls in place that guide calculation and reporting of non-GAAP financial measures are critical.

### How internal audit can help:

- Understand non-GAAP financial measures regularly reported by the company
- Assess and challenge processes followed to calculate non-GAAP financial measures
- Test controls within these processes to help ensure consistency in calculations and management's thorough understanding of the data sources for externally reported non-GAAP financial measures
- Compare non-GAAP financial measures year-over-year to assess consistency







## 6

## Integrated assurance

### Drivers:

- Rapidly changing risk environment coupled with increasing need for insights to make decisions
- Collaborating among assurance providers to develop a common view of risk
- Streamlining risk assessment and assurance activities across the enterprise to gain efficiencies and maximize coverage
- Allocating limited resources towards highest risk areas for the enterprise

With a constantly evolving risk landscape, the board and senior management expect all assurance functions to work together to provide an integrated view of the organization's risk profile. Many companies fail to develop systematic processes for anticipating new and emerging risks, and as a result, critical risks are identified too late to be effectively and efficiently managed. Further, traditional approaches to providing assurance over risk responses are often siloed and uncoordinated. Companies that effectively anticipate and address changes in the risk environment, develop coordinated plans across multiple assurance functions, and maximize enterprise coverage are likely to be well positioned to provide insights and perspective to senior management and the board, for the benefit of more effective decision making and risk management.

### How internal audit can help:

- Lead or support coordination of the risk assessment, planning, work execution and reporting across multiple assurance functions to help minimize the footprint on the business
- Evaluate business implications of emerging trends and their associated risks
- Encourage increased utilization of data and analytics to optimize insights into the emerging risk environment
- Develop and execute holistic assurance plans considering enterprise risks, leveraging the various governance, compliance, and audit functions across the organization

# 7

## Third-party relationships



To boost productivity and adapt to changing business models, companies are increasingly relying on third parties to carry out vital business functions. As valuable as these relationships are, it is important for organizations to fully understand and appreciate the commercial, regulatory, and reputational risks that can arise. Using third parties opens up companies to numerous potential compliance failures that can lead to fines, lawsuits, operational bans, and reputational damage. Often, third parties can have access to the company's networks, increasing the possibility of data breaches, or companies can be unaware that third parties are employing subcontractors that may be wanting in their business and compliance efforts. Finally, third parties can operate in areas of political uncertainty, exposing contracting companies to further risks. Given all these factors, companies need to ensure they are getting anticipated benefits from these external relationships while having in place appropriate controls to reduce liabilities.

### How internal audit can help:

- Evaluate the organization's third-party risk management governance and controls framework and understand how third parties are identified, risk-assessed, and managed end-to-end
- Evaluate contract management processes used by management to track third-party relationships
- Perform audits consistent with right-to-audit clauses
- Assess third-party compliance with company's information security standards
- Develop, implement, and calibrate a continuous monitoring system of self-reported data from third-party business partners



### Drivers:

- Risks associated with an increasing number of third-party relationships, oversight of those relationships, and the risks related to those activities
- Enhancing revenue and cost reduction
- Improving contract and vendor governance
- Creating more effective contractual self-reporting processes
- Preventing or timely detecting risk management failures at third-party business partners



## 8

# Cyber breach/crisis preparedness and response

### Drivers:

- Mitigating the risk of business disruption
- Averting reputational damage to the organization
- Mitigating the risk to employee safety and the organization's profitability
- Protecting data and intellectual property of the organization

Many companies believe their disaster recovery and business continuity procedures are solid and capable of producing desired results, until they are tested in real crisis situations. No company can prepare individually for every possible crisis; however, an overall framework for responding to a crisis can provide much needed guidance and direction in the face of adversity. In today's world of constant connectivity, cybersecurity is a key focal point for many companies. But potential crises stretch well beyond cybersecurity, to disease outbreaks, natural disasters, workplace violence, and employee harassment. Due to the seemingly endless stream of potential crises, fatigue is setting in for many organizations. However, this is a dangerous time for a company to let its guard down as the consequences of unmitigated and unmanaged crises can be disastrous as an organization's bottom line and reputation are impacted.

### How internal audit can help:

- Conduct an in-depth audit of cyber-risk assessment practices and resource allocation to assess connectivity to the company's strategic priorities and understanding of value at risk
- Assess maturity of the organization's disaster recovery and business continuity program, including crisis preparedness frameworks and planned responses
- Evaluate the integration and alignment of business continuity, disaster recovery, cyber breach, and crisis response procedures
- Analyze the effectiveness of business continuity exercises and IT disaster recovery tests



# 9

## Anti-bribery/anti-corruption



The benefits of an effective anti-bribery/anti-corruption (ABAC) compliance program are clear. It is critical to demonstrate that the organization's program actively identifies potential issues and initiates remediation measures in a timely manner. The program should include support from senior leadership, clear policies, training, monitoring, and oversight. Policies that spell out prohibited activity, the commitment of executive management, audit clauses in agreements with third parties, and vigilance by compliance personnel can deter bribery and corruption, thereby reducing the risk of costly and disruptive regulatory enforcement activity. Should the unthinkable occur, a well-designed and executed anti-bribery and corruption compliance program may mean the difference between a prosecution and a nonprosecution agreement and may even reduce the amount of monetary fines and penalties levied.

### How internal audit can help:

- Undertake an objective assessment of the ABAC governance framework
- Evaluate the design and operating effectiveness of the organization's applicable preventative and detective controls
- Conduct culture audits to evaluate not only the hard controls, but also the soft controls that influence and provide insight into informal norms and behaviors
- Assess the strength of end-to-end third-party management, including due diligence and monitoring practices
- Evaluate due diligence and post-deal integration practices for managing ABAC risk, including review of acquired third-party relationships

### Drivers:

- Providing insight to stakeholders regarding the effectiveness of existing anti-bribery and corruption compliance activities
- Identifying emerging regulatory and compliance risk, such as that introduced by organic expansion into new markets, third parties, and acquired businesses
- Preserving the company's ability to control when it discloses a potential violation to the regulators, if at all



# 10

## Talent acquisition and retention

### Drivers:

- Increasing participation by IA in company strategic initiatives
- Increasing demands of external auditors on IA resources related to regulatory requirements
- Expanding role of IA to include review of enterprise risk management approaches; governance, risk, and control activities; operational improvement initiatives; and other areas beyond a historical compliance-based scope
- Resource disruptions caused by digital labor advancements and low-cost offshoring
- Shortage of strategic-thinking business professionals to execute IA's mission

Increasingly, IA is being called upon to expand its presence in more areas of the organization and become a strategic partner in the business. If IA is to successfully execute on its growing mission, it will need access to talented professionals and specific subject matter professionals knowledgeable of where the company's risk profile is changing. This need is made even more acute given today's scarcity of high-quality talent. An organization has several options for how to fulfill its needs, including full-time hires, outsourcing, and cosourcing. The challenge is ensuring the right talent is hired, retained, motivated, and developed to help the company achieve its business objectives and strategies. Companies also need to evaluate risk mitigation plans for top talent departures.

### How internal audit can help:

- Evaluate IA resource needs based on realistic views of executing the IA plan
- Assess new resource needs as IA becomes more involved in strategic initiatives of the business
- Conduct internal competency assessment for current resources to understand gaps in needed skill sets
- Determine areas in which specific subject matter professionals are needed as IA expands roles beyond compliance
- Build relationships with external service providers to leverage these subject matter professionals and resources when needed
- Provide IA professionals with training and development programs tied to regulatory developments, as well as wider business objectives beyond compliance
- Collaborate to help ensure company hiring practices are actively considering IA needs and stay closely involved in the hiring process for full-time auditors



Top 10 Area:	Link to additional information:
<b>Accounting standards</b>	<a href="https://home.kpmg.com/us/en/home/insights/2017/11/2017-issue4-article4.html">https://home.kpmg.com/us/en/home/insights/2017/11/2017-issue4-article4.html</a>
<b>Culture risk</b>	<a href="https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/five-steps-to-tackling-culture.pdf">https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/five-steps-to-tackling-culture.pdf</a>
<b>Digital labor governance</b>	<a href="https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/10/intelligent-automation-and-internal-audit.pdf">https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/10/intelligent-automation-and-internal-audit.pdf</a>
<b>General Data Protection Regulation</b>	<a href="https://advisory.kpmg.us/content/dam/kpmg-advisory/cyber/pdfs/2017/ready-for-gdpr.pdf">https://advisory.kpmg.us/content/dam/kpmg-advisory/cyber/pdfs/2017/ready-for-gdpr.pdf</a>
<b>Non-GAAP financial measures</b>	<a href="http://www.kpmg-institutes.com/content/dam/kpmg/financialreportingnetwork/pdf/2016/defining-issues-16-20-sec-non-gaap-finan-measures.pdf">http://www.kpmg-institutes.com/content/dam/kpmg/financialreportingnetwork/pdf/2016/defining-issues-16-20-sec-non-gaap-finan-measures.pdf</a>
<b>Integrated assurance</b>	<a href="https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/RiskConsulting/integrated-risk-assurance-services.pdf">https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/RiskConsulting/integrated-risk-assurance-services.pdf</a>
<b>Third-party relationships</b>	<a href="https://advisory.kpmg.us/risk-consulting/third-party-risk.html">https://advisory.kpmg.us/risk-consulting/third-party-risk.html</a>
<b>Cyber breach/crisis preparedness and response</b>	<a href="https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/cyber-fatigue-web.pdf">https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/cyber-fatigue-web.pdf</a>
<b>Anti-bribery/anti-corruption</b>	<a href="https://advisory.kpmg.us/risk-consulting/forensics/anti-bribery-corruption.html">https://advisory.kpmg.us/risk-consulting/forensics/anti-bribery-corruption.html</a>
<b>Talent acquisition and retention</b>	<a href="https://advisory.kpmg.us/managementconsulting/capabilities/talent-management.html">https://advisory.kpmg.us/managementconsulting/capabilities/talent-management.html</a>

## Contact us

### Deon Minnaar

**Service Network Leader, Internal Audit and Enterprise Risk**

**T:** 212-872-5634

**E:** [deonminnaar@kpmg.com](mailto:deonminnaar@kpmg.com)

### Patty Basti

**Partner, Internal Audit and Enterprise Risk**

**T:** 513-763-2499

**E:** [pbasti@kpmg.com](mailto:pbasti@kpmg.com)

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

### [kpmg.com/socialmedia](https://www.kpmg.com/socialmedia)



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.

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 727662