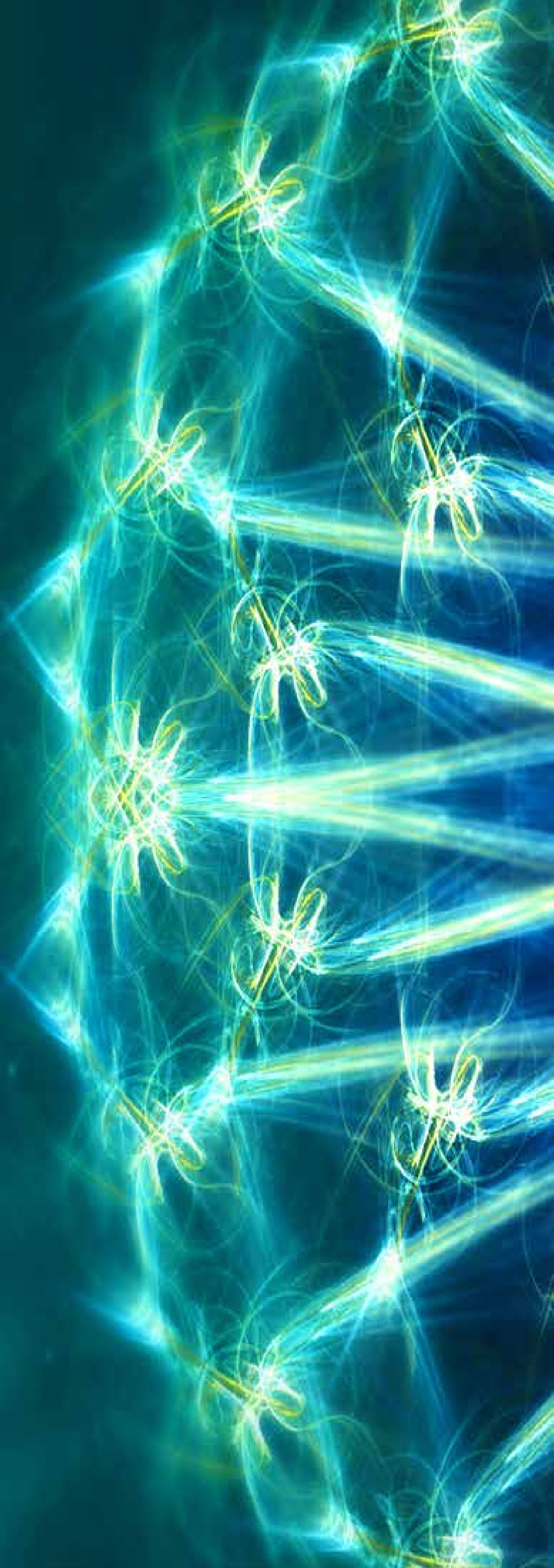
KPMG

Internal Audit:

Navigating a transforming life sciences landscape

Top trends and risks for 2018

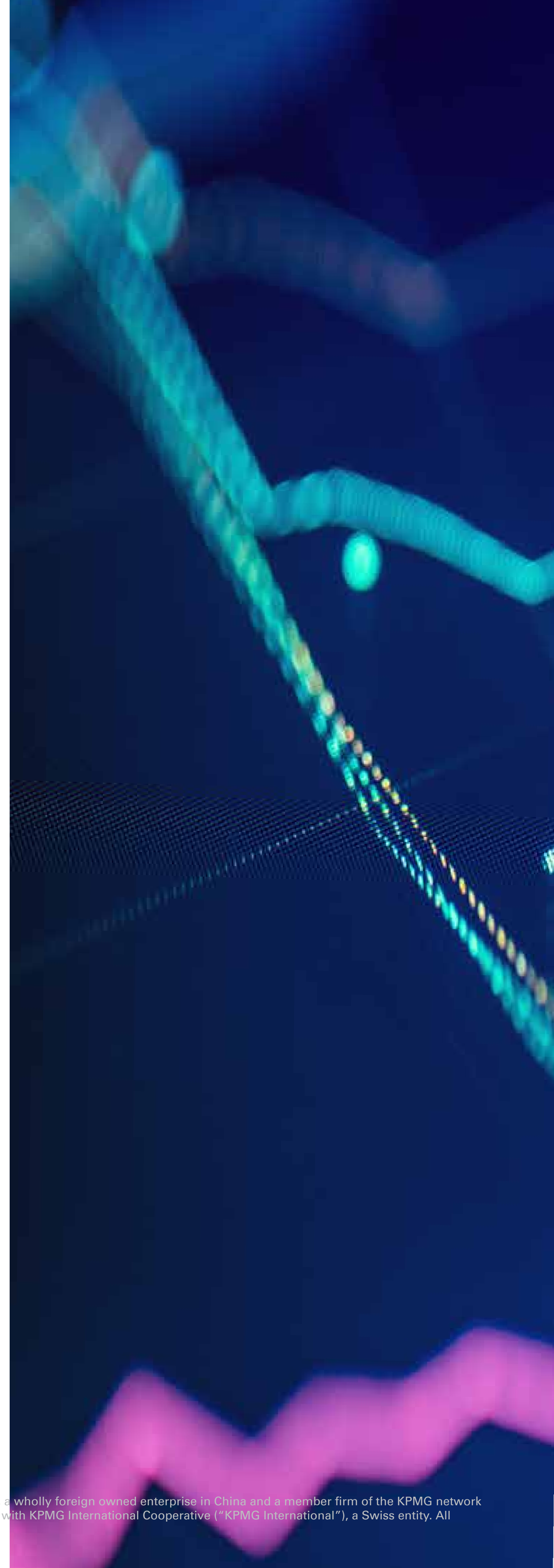


kpmg.com

The life sciences industry is transforming. Organizations face changing regulatory requirements, potential constraints on their use of patient data, evolving relationships with payers, fierce competition on a global playing field, and the need to respond to pricing pressure with proof of a product's value. These challenges are forcing organizations to re-examine their business portfolios, go-to-market strategies and customer engagement models to accelerate growth and enhance shareholder value.

All of these changes bring both risks and opportunities. Identifying the fine line between the two factors is critical. Although 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,[1] 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.

This white paper is designed to guide you in navigating today's risk environment. In many cases, risks and related control frameworks are interrelated. Our hope is that these insights will be catalysts for new thinking as you conduct your annual risk assessments and reflect on how you are covering these risks over time through your audit universe. We have also highlighted broader trends that may have a bearing on the evolution of your function and setting your strategic priorities.



Top 10 risk areas life sciences organizations should consider are:

Further, there are three key trends impacting IA that warrant attention:

– Digitization

– Culture

– Cost of compliance

In the following pages, we provide insights into these risks and trends and the elevated role that IA can play in supporting the business with their risk mitigation efforts.

01

Pricing: A multifaceted challenge

Governments are under tremendous pressure to curtail healthcare spending. And pharmaceuticals represent approximately 20 percent of the total spend, according to the Organization for Economic Co-operation and Development (OECD).[2] The increase in high-cost specialty medicines and aging populations has spurred a debate about prescription drug spend sustainability and the need for a shift to value-based-pricing models. In the United States, patients are increasingly bearing the cost burden of prescription medicines, and manufacturers have responded with copay assistance coupons and patient assistance programs, raising new and different compliance risks.

Political and regulatory scrutiny of drug pricing practices remains intensive in the United States, with pricing risks in markets like the EU and China on the rise. One-third of all open competition law cases in the United Kingdom relate to pharmaceutical pricing.[3] Price gouging, specialty pharmaceutical pricing, coupons, and assistance programs are all topics of regulatory attention and ongoing probes.

United States government pricing programs continue to be an area of elevated risk and regulatory attention. Not only are these programs highly technical and inherently complex, but expectations continue to change, authoritative guidance is often unclear and sometimes conflicting, transactional datasets are expanding, and expectations for calculation precision are high.

How IA can help:

- Continue to evaluate the pricing regulatory environment in the United States and globally and evaluate the impact on the audit plan.
- Conduct regular audits of government pricing programs including governance, regulatory change management, calculation accuracy, payment accuracy, and master data integrity.
- Evaluate governance over price increases, documentation of rationale, consideration of payer contract adherence, and potential reputational impacts.

Patient support programs: Already under scrutiny

Patient support programs (PSPs), often managed through HUB services and specialty pharmacies, are designed to improve patient outcomes and experiences. PSPs have expanded their focus from adherence to other services including benefits verification, insurance counseling, appeals support, appointment scheduling and reminders, financial assistance (free or discounted drugs), disease education and resources, patient counseling, patient surveys, rewards programs, and refill reminders.

While these services can have a positive impact on patient access and outcomes, they also open up channels for potential abuse and noncompliance through greater access to patients, their data, and related decision-making processes. Given these risks, organizations must tread carefully or risk violating anti-kickback statutes and government pricing regulations.

Already, these programs are under heightened regulatory scrutiny. A number of manufacturers are entering into settlements related to alleged kickback violations involving overutilization or inappropriate product utilization, government pricing violations via off-invoice discounts, minimization of product risks, failure to report adverse events, off-label promotion, and inadequate safeguards over patient data and privacy.

02

How IA can help:

- Understand the nature and range of patient support programs and the internal and external parties managing the programs, including related governance structures.
- Conduct audits of patient support programs, including the rigor of program governance (development, evaluation and oversight) and internal controls when managing discrete programs. Note that a high level of coordination and planning is required to perform end-to-end program reviews that include third-party engagement.

03

General Data Protection Regulation (GDPR): Not just in the EU

How IA can help:

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

The digital revolution is significantly transforming how life sciences organizations do business and improving the patient experience and health outcomes. At the same time, emerging technologies and Big Data introduce challenges and risks when it comes to safeguarding patient data and adopting appropriate data privacy governance models. In response to these risks, a game-changing regulation has been introduced in the EU – the General Data Protection Regulation (GDPR). GDPR is relevant to most life sciences companies, due to the multinational nature of operations. 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 four percent of global annual turnover from the prior year, or 20 million euros, whichever is greater. All indications are that data privacy authorities are serious about enforcement.

Life sciences organizations will face unique challenges when navigating and implementing GDPR: the question of whether or not they can collect and study personal data from emerging technologies such as the cloud, cognitive and the Internet of Things; the potential to be handcuffed in their ability to use advanced data and analytics to create new products targeting underserved patient populations; the need to transform clinical trial processes and policies, etc.

New requirements will mandate examination and risk assessment of operational practices across a wide variety of functions, including research and development, human resources, medical affairs, 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.

GDPR recap

The General Data Protection Regulation (GDPR) introduces a number of complex requirements including, but not limited to:

- Requirement to obtain explicit consent
- Requirement to report data breaches within 72 hours to impacted data subjects
- Expanded data subject rights, which include access, rectification (e.g., correction of inaccurate data), and erasure, or right to be forgotten
- Extension of the oversight burden and risk exposure from data controllers to third-party processors

04

Third parties: Know your partners

How IA 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.

– Conduct targeted theme audits by third party and/or risk type (e.g., CROs, data protection) and consider both internal controls and direct evaluation of third-party controls.

– Support the organization's evolution toward a holistic third-party risk management framework to ensure appropriate end-to-end risk life-cycle management and transparency of risk levels.

In many ways, organizations are reliant on third parties: from suppliers to service providers to customers and business partners. 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.

Life sciences companies often have thousands of third-party dependencies spanning drug discovery and development, manufacturing and supply, sales and marketing, and operational and administrative support. The sheer volume, often spanning multiple functions, makes it difficult to *know your third parties*, let alone assemble a holistic view of how third-party risk is managed across the enterprise. Failure to adequately assess risk and monitor third-party compliance can expose organizations to reputational damage, operational disruption, financial loss, regulatory fines, and potential criminal liability.

Potential risks associated with third parties include:

– **Healthcare practitioners and organizations:** Kickbacks and off-label promotions

– **Payers:** Inappropriate incentives, revenue leakage, contract noncompliance, unfavorable formulary placement

– **Distributors:** Issues with the designated channel of distribution at the agreed-upon price, as well as product diversion

– **Alliance partners:** Unfair cost-sharing for product development and marketing, inappropriately dispensed royalties and licensing payments, revenue leakage, adverse events, contract noncompliance

– **Vendors:** Cyber-security and data protection vulnerabilities, contract noncompliance

– **Ad agencies:** Financial, operational, reputational, and data transparency risks

– **Contract research organizations:** GxP noncompliance, data integrity and protection issues, adverse events, kickbacks

– **Contract manufacturing organizations:** Adulterated product quality, serialization issues, disruptions in supply continuity

Anti-bribery & corruption: A need for vigilance

There continues to be a proliferation of anti-bribery and corruption (ABAC) legislation and enforcement globally, with increasingly effective international regulatory cooperation. TRACE International's 2016 Global Enforcement Report highlights that enforcement actions doubled from 2015 to 2016.[4]

This is a major risk area for life sciences due to the regulated nature of the industry and reliance on government officials throughout the product development, sales and marketing, product manufacturing, and distribution life cycles. The high level of interaction with healthcare practitioners (e.g., doctors, nurses, pharmacists), many of whom are considered government officials, makes the industry more vulnerable.

In 2016, five of 27 Foreign Corrupt Practices Act (FCPA) enforcement actions targeted life sciences companies,[5] and all but one of the five included violations in China. In fact, we continue to see a disproportionate number of ABAC concerns arising in China; Southeast Asia; the Commonwealth of Independent States (Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Ukraine); Eastern Europe; and Latin America (Mexico, Brazil, and Argentina).

It is critical to demonstrate that the organization has a strong anti-bribery compliance program that 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.

Potential ABAC risks include:

- **Healthcare practitioners, organizations, and consultants:** Nature of services and appropriateness of fair market value calculations
- **Third parties:** Due diligence, contracting and ongoing monitoring of third parties. (According to a recent study on ABAC benchmarking,[6] "Forty percent of respondents say third-party violations are the top risk to their organization's anti-bribery and corruption programs." Further, more than half said they had identified legal, ethical, or compliance issues with a third party after due diligence had been conducted.)
- **Mergers and acquisitions:** Adequacy of pre-deal due diligence, post-deal integration and transition to business-as-usual activities. (Respondents to the 2017 KPMG/Forbes Insights Cyber-Security Survey[7] indicated they do not conduct the same level of data collection for third parties associated with their transaction targets as they do for themselves.)
- **Tenders:** Appropriate public/private tender documentation and oversight, including indirect tendering through third parties
- **Sales and discounting programs:** Practices and procedures governing discounts and allowances, both on and off invoice, including related business justification
- **Sponsorships:** Procedures and documented assessments related to requests, requestors and recipients, rationales, and disposition of funds
- **Grants and donations:** Documented assessments related to requests and recipients, intended purpose, and disposition of funds
- **Customs clearance:** Due diligence of customs brokers/clearance entities and fees that are in line with regulations and acceptable market practices

05

How IA can help:

- Conduct culture audits to evaluate not only the hard controls (e.g., policies, procedures, training), but also the soft controls that influence and provide insight into informal norms and behaviors.
- Undertake an independent review of the ABAC governance framework.
- 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.

06

Cyber-security threats: An undeniable reality

How IA can help:

- Conduct an in-depth audit of cyber-risk assessment practices and resource allocation, ensuring that there is connectivity to the company's strategic priorities and understanding of value at risk.
- Provide an independent voice on areas of priority investment.
- Undertake in-depth assessments of high priority areas, including M&A, medical device security, information sharing and GDPR, and response and recovery.
- Review the cyber culture to evaluate how individuals across the organization understand and respond to cyber threats.

Despite the level of focus and investment related to managing cyber risk over the past decade, the number, scale and sophistication of cyber breaches continues to grow. There is genuine cause for frustration, and cyber fatigue is setting in for many organizations. Nevertheless, life sciences organizations must realize that this is a dangerous time to let their guard down as the consequences can be catastrophic (e.g., loss of intellectual property, adulteration of data supporting clinical trials).

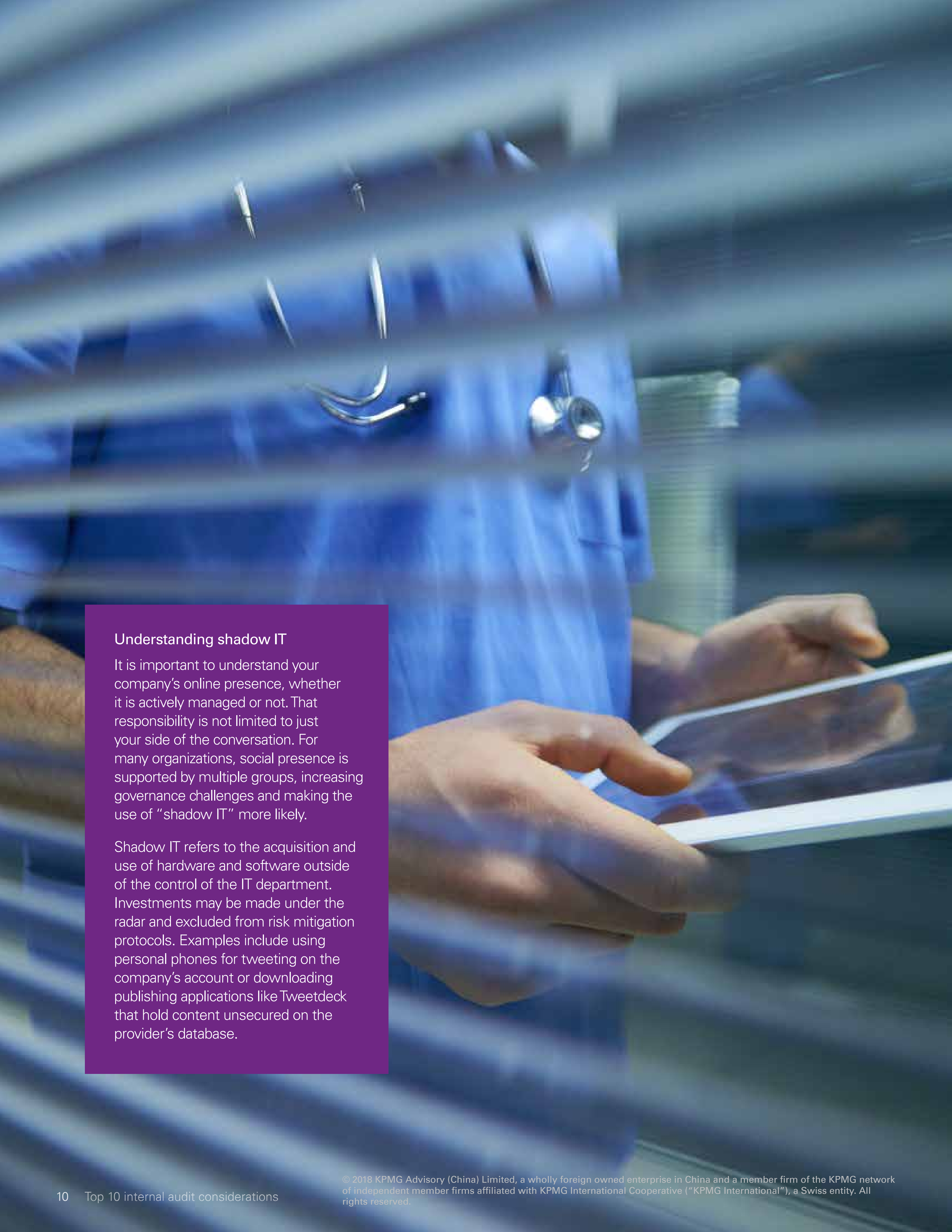
With nation states now representing the most likely source of a cyber-attack,[8] the focus on intellectual property and R&D data will only intensify, raising the stakes for an industry like life sciences that relies on collaboration and data exchange to fuel innovation. In tackling cyber risk, life sciences organizations face myriad challenges:

- **Sharing and analyzing data:** Organizations are sharing sensitive information with a wider variety of partners and vendors, across borders, with competitors, via the Cloud, and sometimes in real time. Despite knowledge of high-profile data breaches, there are signs of complacency: Fifty-seven percent of life sciences companies surveyed by KPMG feel more secure about their data than they did in the past.[9]
- **Mergers & acquisitions (M&A):** M&A can significantly elevate cyber risk through the introduction of new IT systems and disparate internal control protocols. However, in our recent cyber-security study, nearly 40 percent of companies said no action was required post-merger, signaling potential weaknesses in post-deal integration procedures for managing cyber risk.[10]
- **Medical device security:** Wireless, sensor-based medical devices are one of the most significant innovations in patient care. However, device tampering has the potential to cause great harm to patients, and devices can serve as gateways into a hospital's network, allowing access to sensitive patient information.
- **Response & recovery:** Since it's not a matter of "if" but "when" an attack will occur, organizations must have strong systems of response and recovery to minimize business disruption and associated costs. Life sciences companies are starting to invest more in these activities and reallocating resources from detection.
- **People:** Many breaches stem from human error or malicious intent, raising the importance of training and cultural considerations.

Digitization, a blessing and a curse

In this digital age, every part of the life sciences organization is innovating and often adopting consumer-grade technologies. Labs may be using smart home devices (e.g., cameras, switches, thermostats). Virtually everyone from the C-suite to facilities has adopted countless mobile solutions, many of which are off the shelf and not subject to the same governance and security vetting as enterprise applications. Individual business units are now introducing a number of digital labor or robotic process automation tools, from simple desktop automation to powerful cloud-based cognitive engines, to help their teams become more efficient and bring forward new insights. And while many of these technologies seem harmless, they open organizations up to a host of new risks if not governed effectively.

Every new Internet of Things device or smart sensor introduced into the ecosystem creates a new vector that a potential hacker may exploit as an entry point into the larger environment if not properly segmented and secured. Each new mobile app that an individual department or team may be using could potentially be malicious and collect sensitive information from other applications on the device. The new digital labor solution may save hundreds of person-hours, but an unmonitored error in coding may create hundreds or thousands more and, even worse, may directly impact patient care. IA is in a unique position not only to identify risk areas but also to put forward frameworks for good governance and control to help manage the risk/reward balance of digital technology.



Understanding shadow IT

It is important to understand your company's online presence, whether it is actively managed or not. That responsibility is not limited to just your side of the conversation. For many organizations, social presence is supported by multiple groups, increasing governance challenges and making the use of "shadow IT" more likely.

Shadow IT refers to the acquisition and use of hardware and software outside of the control of the IT department. Investments may be made under the radar and excluded from risk mitigation protocols. Examples include using personal phones for tweeting on the company's account or downloading publishing applications like Tweetdeck that hold content unsecured on the provider's database.

Social media/Digital marketing:
A need for transparency

07

The internet has fundamentally changed how life sciences companies share information and interact with consumers. While new platforms represent significant opportunities for consumer access, insight and information exchange, they also present governance challenges and amplify a company's exposure to a range of risks. Content is accessible to an audience beyond customers, including employees (past and present), shareholders, competitors, detractors, and regulators on a global scale. Companies need to actively consider and manage potential risk impacts on areas such as adverse event monitoring and reporting, data privacy, off-label promotion, intellectual property, and reputation.

In 2014, the FDA released guidance to manufacturers regarding the use of social media,[11] including requirements impacting how FDA submissions of post-marketing promotional materials are posted and shared through interactive media platforms. This guidance reinforces expectations that medical product information, regardless of the communication channel and character limits, will be presented in a truthful and unambiguous manner. It also must ensure that highlighted risks and benefits are aligned with the product's label and approved usage. Further, the guidance provides instructions for correcting inaccurate information posted to the internet (e.g., blogs, social media). In response, concerns have been raised that manufacturers will be held responsible for the comments of others and that applying old rules to new platforms like Twitter is overly restrictive.

All of these challenges must be considered in the context of the operational processes supporting online communications. The honeymoon period of leaving these processes to evolve informally has passed. Organizations will be better served with more formal, yet agile, control processes that bring executive transparency to digital engagement programs and allow for collaboration between stakeholders such as legal, finance, compliance, and IT.

How IA can help:

- Conduct independent reviews of social media governance and controls across the organization.
- Compare customer engagement processes, policies and tools with leading industry practices.
- Analyze the organization's use of data and analytics and monitoring of internet commentary to identify risk signals, including reputational risk.
- Incorporate internet commentary listening into the audit process.
- Assess the organization's digital strategy for handling threats and opportunities, apply KPIs to specific audience transformation processes, and measure whether projects meet critical success factors that were part of the original business case for investment.

08

Serialization: Ensuring a smooth supply chain

How IA can help:

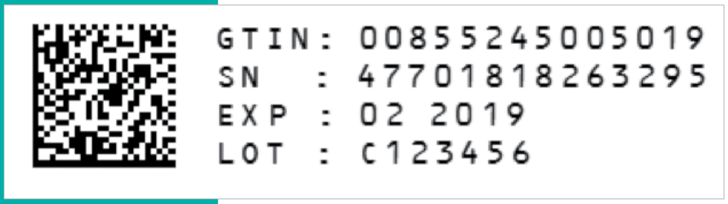
- Understand the organization’s response to global serialization regulations, including related governance, cross-functional coordination, and third-party coordination/evaluation to support responsiveness and compliance.
- Evaluate and support the organization’s readiness through pre-implementation and/or post-implementation reviews in response to new regulations.

With the constantly changing regulatory environment, life sciences organizations are grappling with global serialization regulations for supply chains. These regulations are a response to the growing concerns around product integrity throughout the supply chain, the risk of counterfeiting, and the need to curtail reimbursement fraud.

This introduces complex challenges for life sciences organizations: country-specific readiness, master data management, artwork change management, internal packaging site and contract manufacturer readiness, and sustainability of compliance once achieved. Failure to take appropriate measures and comply with requirements such as the Drug Supply Chain Security Act (DSCSA) can lead to disruption in the supply chain, financial loss and reputational damage.

Serialization milestones

Serialization, which is broadly defined as establishing and marking each saleable unit of product with a globally unique identifier, is an active regulatory topic in more than 40 countries, including the United States and the EU. In the United States, the Drug Quality and Security Act (DQSA) was signed into law on November 27, 2013. Under Title II of DQSA, known as DSCSA, a set of requirements and phased compliance dates were established for prescription drug manufacturers and other participants in the distribution chain. The next compliance due date is November 27, 2017 (FDA has indicated an intent to defer enforcement until November 28, 2018) when product serialization and enhanced verification processes go into effect. In the EU, a comparable requirement becomes effective February 9, 2019. These are significant compliance milestones for manufacturers.



GTIN: 00855245005019
SN : 47701818263295
EXP : 02 2019
LOT : C123456

Serialized DataMatrix Code

Opioids: A growing epidemic

In 2015, more than 33,000 people died in connection with what is considered the worst drug crisis in American history, the opioid epidemic. Drug overdoses have since become the leading cause of death of Americans under 50, with two-thirds of those deaths from opioids.[12]

Manufacturers, wholesalers and distributors are under increasing scrutiny and face potential legal action for irresponsible sales and marketing practices and failing to help address market oversupply. If your organization plays a significant role in the manufacture and/or supply of opioid analgesics, IA can play an important role in understanding and evaluating the company's related risk management strategies and response.

Connecting culture

The connection between culture and risk management has gained increased attention in recent years. Multiple high-profile culture failures and public relations gaffs, together with efforts from the Institute of Internal Audit, have strengthened the argument for culture and the need to adapt traditional monitoring and auditing practices.

IA is often uniquely positioned to be the eyes and ears of the organization, understand what is happening, observe leadership behaviors as they operate across the enterprise, and deliver insight into culture. IA can add culture considerations to existing audits (e.g., root causes, feedback on observed behaviors), perform stand-alone culture audits, and expand the audit universe to areas that significantly influence and signal culture (e.g., hotline reporting, incentive programs, business planning).

As culture has a pervasive impact on strategic, operational and compliance risk, we believe that auditing culture will become the new norm and expectation of IA. By ignoring culture, you are likely providing an incomplete view of risk.

09

How IA can help:

- Understand the company's risk management strategies and response related to opioids, and evaluate connectivity to broader enterprise risk management and corporate responsibility programs.
- Assess how holistically risks have been identified and assessed, clarity of ownership, and the rigor of related risk mitigation and reporting activities, including board-level dialogue and review.
- Evaluate controlled substance management practices, including *know your customer* monitoring procedures to identify and report on unusual and/or suspicious orders.
- Ensure that there are strong controls and safeguards over marketing and selling practices, including evaluation of reward and enforce activities to incent employees and hold them accountable for inappropriate practices.
- Review the corporate responsibility program and related reporting.

10

Accounting Standards: A seismic shift

How IA can help:

– Work closely with external auditors to understand their expectations and how they view the current state of implementation.

– Conduct pre- and post-implementation reviews to understand the organization's response to the new standards; how changes in people, process and technology have been managed; and related updates to the control environment.

– Evaluate the completeness of business unit inventory affected by new revenue recognition and lease accounting rule changes.

– Meet with appropriate personnel from business subdivisions to discuss the key aspects of the lease population with a focus on those that are expected to change upon adoption of ASC 842.

– Analyze sample customer contracts to identify accounting gaps.

– Evaluate one-time controls associated with adoption of the new standards, including the completeness and appropriateness of disclosure controls under SAB 74.

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 the most significant change 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 lease accounting standard takes effect just over a year later on January 1, 2019, for calendar year-end public companies.

The new standards are highly technical and represent a tremendous shift in expectations. Further, the absence of clear guidance requires a significant level of interpretation and judgment by management. This features as a top risk for 2018 because the new standards are complex, companies are tracking behind in their readiness, and the SEC will be closely scrutinizing the implementation and related disclosures under Staff Accounting Bulletin (SAB) 74: Disclosures and Controls for New Accounting Standards.

The new revenue recognition standard is intended to simplify and harmonize 150+ pieces of current U.S. GAAP revenue literature, developed over multiple decades, into a single, principles-based standard. Specific challenges include the variety of customer contractual arrangements, particularly the licenses and collaborations that are so prominent for life sciences companies.

The new lease accounting 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 cost of compliance

Life sciences companies have made huge investments in compliance activities over the last decade, often in response to something that has gone wrong. This has contributed to a proliferation of policies, monitoring and certifications, in many cases cobbled together over time. There have been significant investments in technology, and yet companies still have fragmented tracking and reporting. Further, organizations have multiple functions contributing to compliance, and there are often gaps, overlaps and inefficiencies in how these teams operate.

As organizations have come under pressure to reduce costs and reinvest in growth, efficiencies and the cost of compliance are starting to receive attention. IA can contribute to and influence not only effective compliance, but also a framework that is sustainable, maximizes the return on investment and garners stakeholder buy-in. A starting point is mapping the range of compliance and assurance functions and activities and identifying operational synergies and opportunities to better *connect the dots*.

How KPMG can help

KPMG's perspective is that internal audit should provide tangible value to the business by focusing on the risks that matter and providing practical recommendations that assist in achieving business objectives—in addition to validating compliance and providing risk coverage. KPMG's approach reflects direct input from CFOs and audit committee chairs, who report a gap between what internal audit functions are delivering to date and their expectation that IA become a strategic arm of the business. Based on recent surveys conducted by KPMG and Forbes, executive stakeholders:

— Envision a more strategic role for internal auditors

— Expect their internal auditors to have knowledge and expertise that aligns with the sophistication of their audit targets, enabling review of the technical areas of the company's operations and assistance with legal and regulatory compliance processes and requirements; and

— View technology as a tool not only to make audits more efficient and effective, but also to provide deeper insights that deliver tangible, strategic value.

KPMG helps IA take a strategic approach, elevating the function in terms of the insights, results and demonstrable value it can provide the organization. Bringing industry knowledge and experience to IA is critical to our value proposition and to helping you provide strategic value and insight relevant to the unique environment and context of life sciences.

KPMG can support your IA team with a range of services including but not limited to:

— Outsourcing and co-sourcing IA and SOX

— IA transformation and optimization (IA team build, strategic assessments, quality assessment reviews, new leader start-up/visioning, benchmarking)

— Internal controls transformation

— Data & analytics-enabled IA

— Technical audit delivery and support (augmenting the client's team with technical specialists from Tax, Cybersecurity, Data Protection, Supply Chain, Compliance, Risk)

— Enterprise risk management/dynamic risk assessment

— Governance assessments (risk and governance framework audits, compliance function audits, quality assurance function audits, integrated assurance)

— Strategic auditing (culture audits, emerging risk audit, e.g., digital disruption, strategy audits, in-stream audits)

— Revenue leakage and cost recovery (e.g., contract compliance, process efficiency)

— Remediation planning, delivery and support

References:

1 KPMG/Forbes Seeking Value Through Internal Audit Study

2 OECD (2015). Pharmaceutical spending trends and future challenges," Health at a Glance 2015.

3 Continued Focus on Pricing in the Pharma Sector; CMS Law Now; May 26, 2017; http://www.cms-lawnow.com/ealerts/2017/05/continued-focus-on-pricing-in-the-pharma-sector

4 Global Enforcement Report 2017 – March 2017. www.TRACEInternational.org

5 United States Securities and Exchange Commission, SEC Enforcement Actions: FCPA Cases; https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml

6 Anti-Bribery and Corruption Benchmarking Report – 2017; Kroll and Ethisphere

7 2017 KPMG/Forbes Insights Cyber-Security Survey

8 2017 KPMG/Forbes Insights Cyber-Security Survey

9 2017 KPMG/Forbes Insights Cyber-Security Survey

10 2017 KPMG/Forbes Insights Cyber-Security Survey

11 2014 FDA Draft Guidance for Industry: Internet / Social Media Platforms

12 American Society of Addiction Medicine report

Contact us

Tracey Keele
Partner, National Life
Sciences Internal Audit Lead
tkeele@kpmg.com
+1 267 256 3400

Li Fern Woo
Head of Life Sciences
KPMG China
lifern.woo@kpmg.com
+86 21 2212 2603

kpmg.com/socialmedia

This document was originally published by KPMG International.

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.