Navigating a transforming life sciences landscape

Top trends and risks for 2018
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. 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:

1. Pricing
2. General Data Protection Regulation (GDPR)
3. Anti-bribery and corruption (ABC)
4. Social media and digital marketing
5. Opioids
6. Patient support programs
7. Third parties
8. Cyber-security threats
9. Serialization
10. Accounting Standards
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). 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 co-pay 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. 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 also continue to change (e.g., Medicaid Final Rule, 340B developments), authoritative guidance is often unclear and sometimes conflicting, transactional data sets are expanding, and expectations for calculation precision are high.
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, and failure to report adverse events, off-label promotion, and inadequate safeguards over patient data and privacy.
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 (R&D) 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 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
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**: Cybersecurity 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 (ABC) 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 2016.³

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, 5 of 27 Foreign Corrupt Practices Act (FCPA) enforcement actions targeted life sciences companies,⁴ and all but 1 of the 5 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 ABC 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 ABC benchmarking,⁵ “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 (M&A):** Adequacy of predeal due diligence, postdeal integration, and transition to business-as-usual activities (Respondents to the 2017 KPMG/Forbes Insights Cyber-Security Survey 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
Cybersecurity threats: An undeniable reality

Despite the level of focus and investment related to managing cyber risk over the past decade, the number, scale, and sophistication of cyber breaches continue 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, the focus on intellectual property and R&D data will likely 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.

Mergers & acquisitions: M&A can significantly elevate cyber risk through the introduction of new IT systems and disparate internal control protocols. However, in our recent cybersecurity study, nearly 40 percent of companies said no action was required postmerger, signaling potential weaknesses in postdeal integration procedures for managing cyber risk.

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.
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, 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.

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.
Serialization

Ensuring a smooth supply chain

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 most recent compliance due date was November 27, 2017 (FDA has indicated an intent to defer enforcement until November 27, 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.
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. On August 10, 2017, President Trump declared the country’s opioid crisis a “national emergency.”

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.
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 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.

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.
References:
1 “Pharmaceutical spending trends and future challenges,” Health at a Glance 2015, OECD.
6 2017 KPMG/Forbes Insights Cyber-Security Survey
7 2017 KPMG/Forbes Insights Cyber-Security Survey
8 2017 KPMG/Forbes Insights Cyber-Security Survey
9 2017 KPMG/Forbes Insights Cyber-Security Survey
11 American Society of Addiction Medicine report.

Contact Us
Kelli Brooks
Principal, Risk Consulting
T: 213-533-3389
E: kjbrooks@kpmg.com

Matthew G. McFillin
Partner, Risk Consulting
T: 267-256-2647
E: mmcfillin@kpmg.com

Acknowledgements include content and editorial contributors:
Tracey Keele, R. Zimmerer, David Remick, Angela Rodin, Rupen Bavishi, Regina Cavaliere, David Colombo

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

kpmg.com/socialmedia