

Expanding horizons for risk management in pharma

With risks mounting, drugmakers can take a page from other highly regulated, capital-intensive businesses.

Ajay Dhankhar, Saptarshi Ganguly, Arvind Govindarajan, and Michael Thun



Risk management has become a top-of-mind issue for C-suites and boards around the world—nowhere more than in pharmaceutical companies. In a politically and economically turbulent environment, the risks pharma companies face, especially in clinical-trial design and execution, drug approval, product quality, and global commercial practices,

are increasing in both frequency and magnitude (see sidebar, “Growing risks in pharmaceuticals”). One obvious sign of the challenging risk environment (among several factors at work) is the sharp decline in the valuation of specialty companies (35 percent decrease), generic-drug manufacturers (25 percent decrease), and biotech companies

Growing risks in pharmaceuticals

Our experience suggests that pharma companies are likely to face heightened risks over the next few years in the following areas:

- **Pricing, reimbursement, and market access.**

Traditional models of pricing are losing their relevance in the context of expanding exclusion lists, indication-specific pricing, complex and often outcomes-based rebate structures, drugs that can cure rather than just control disease, and intensified public scrutiny. Many companies have run afoul of pricing concerns, particularly in the heated environment of US healthcare politics. By way of response, the pharmacy benefit managers CVS and Express Scripts have increased the number of drugs on their exclusion lists from 132 to 344 from 2014 to 2018, a jump of more than 160 percent, and signaled that they will exclude products with very large price increases.

- **Clinical-trial design and drug approval.** Late-stage failures and sustained high attrition rates—now averaging around 86 percent from Phase I to new drug application—can sink a company’s growth prospects and stock price. Between 2007 and 2016, the probability of moving from Phase I to launch was lower than in the previous ten-year period for eight out of the top ten pharma companies globally. Even when drugs succeed in trials, they can still fail in the market, as several new drugs have done recently.

- **Challenges abroad, including legal, compliance, and commercial issues.**

As pharma companies grapple with a vast set of regulatory frameworks and requirements in different countries, they run an increasing risk of failing to comply with the guidance. In recent years, several companies have run afoul of complex regulations outside their home country. Companies have also sometimes misunderstood or struggled to adjust to the way business is done in these countries.

- **Operations, supply chain, and drug quality.**

As supply chains globalize, outsourcing increases, and pharma companies manufacture more complex molecules, cost pressures and the quest for economies of scale are driving concentration. This increases pharma companies’ dependence on their suppliers and exposes them to significant supply-chain risks. In June 2017, Merck, in common with dozens of other multinational corporations, was hit by a severe cyberattack that disrupted its global operations, forced a temporary shutdown in its manufacturing, and caused extensive losses.¹

¹ See Michael Erman and Jim Finkle, “Merck says cyber attack halted production, will hurt profits,” Reuters, July 28, 2017, reuters.com.

(30 percent decrease) over the past two years. Many pharma companies admit they feel poorly prepared to navigate these choppy waters because their risk analysis and management is not as robust, data driven, action oriented, or far-reaching as they would wish.

We believe that the advanced risk-management practices developed in other heavily regulated sectors, such as banking and energy, can yield valuable insights and provide helpful models that pharma companies could usefully emulate.

Learning from other industries

The pharmaceutical industry is unique in several ways, such as the particular clinical challenges it faces in R&D processes, and the elaborate requirements for market access.

However, our experience indicates that these unique characteristics, while important for risk management, are not the whole story. Several other sectors have much in common with the pharma sector, and the advanced risk-management practices they adopt can be readily adapted to a pharma context, just as leading risk-management practices in the pharma industry are transferable to other industries.

Like energy companies, pharma companies have high capital expenditure and long payoff periods for assets. Like banks, pharma companies operate in a highly regulated environment in which compliance risks are very high (for instance, for improper or poor filings) and other risks (such as sales-conduct risks) are present across many markets globally. Pharma companies also face risks that cut across sectors, such as cyberthreats, data breaches, supply-chain risks, quality risks, geopolitical exposures, and risks from third and fourth parties.

With these commonalities in mind, we have identified five risk-management ideas frequently seen in other sectors that can bring benefits to the pharma industry. These ideas will not only help

pharma companies protect themselves against risk but also enable them to optimize their risk taking—whether to differentiate themselves from competitors or to deepen their thinking about risk/return trade-offs in management decisions.

1. Develop a robust quantitative view of which risks matter most

Effective risk management begins with a robust process to identify, quantify, and inventory risks, both familiar and new. In this respect, pharma companies can emulate the leading banks that have established clear processes for identifying emerging financial and nonfinancial risks. One best-practice bank set up a process consisting of the following four steps:

1. Create an inventory of risks, and map them against a standardized risk taxonomy.

2. Estimate the likelihood and severity of each risk, and consider potential correlations among them.

3. Aggregate the risks, and rank them in order of priority.

4. Manage the risks by linking them to regular business processes, such as strategic and financial planning, enterprise risk management, and controls.

After a few cycles, this approach becomes second nature to institutions and boards. It is important that the risk inventory is neither so detailed that it becomes a box-ticking exercise nor so high-level that it cannot be acted on.

One leading biopharmaceutical company has already adapted its strategic planning to incorporate a taxonomy of risks and a process to calculate their impact. It began by holding a series of workshops for subject-matter experts from across the organization to identify and classify risks. Next it assessed each risk qualitatively and quantitatively by measures

such as probability, impact, and current mitigation efforts to sort the list in order of priority. It also developed a simulation-based model to estimate the cumulative impact of risks on its balance sheet, income statement, and cashflows decades into the future.

A global pharma company took an integrated approach to its strategic-planning process by introducing risk as a key input. The company used a risk taxonomy to rapidly identify roughly eight top risks (such as pipeline, safety, and launch risks, data breaches, and so on). It quantified each in terms of its potential impact on enterprise value (EV). Sensitivity analysis illuminated the cumulative impact on EV if two or more of the risks materialized at the same time. The analysis also showed that the biggest risk to the company stemmed from a relatively thin and concentrated pipeline.

2. Organize around three lines of defense to strengthen oversight and minimize duplication

Organizing roles, responsibilities, oversight, and governance along three lines of defense, known as the 3LOD model, is a proven method for risk management across sectors. The first line comprises the frontline teams that engage in activities that might create risk. The second line—usually the risk function—provides independent oversight and challenge and directly reports to the CEO. It sets policies and standards, ensures that the company’s risk profile does not exceed its risk appetite, and oversees the effectiveness of controls. The third line is usually the corporate audit function, which might be supported by external auditors. When implemented well, the 3LOD structure clarifies roles and accountabilities as well as minimizes duplication through first-line processes with built-in controls, second-line testing and aggregation of risk, and independent assessment of risks and risk management undertaken by the first and second lines.

One large pharma company decided to apply the 3LOD principle to improve the efficiency and

effectiveness of its R&D-quality processes. It began by clarifying roles across each line of defense: clinical research and clinical operations monitoring teams in the first line, medical-quality teams in the second line, and corporate audit in the third line. While doing so, the company took care to eliminate overlaps in activities across the lines. For instance, instead of having all three lines of defense conduct full-scale quality testing of clinical-trial sites, the company switched to selective checks by the second and third lines to provide effective challenge to the first line.

Defining the lines of defense also helped the company identify missing activities and fill gaps. For instance, an undue focus on risk at individual clinical-trial sites meant that cross-cutting processes, such as vendor risk management, were not getting the attention they deserved—a gap the company filled by redefining the remit of the second and third lines to include an end-to-end risk-management view.

3. Establish your risk appetite and prioritize where to focus

Developing a strong risk-appetite framework enables a company to make better informed risk decisions as well as appropriately allocate resources for monitoring and mitigation. It creates a fact base to underpin strategic decision making on topics such as capital allocation, M&A, investment, and divestment. The framework also provides a transparent view of the company’s target risk profile. Well implemented, such a framework helps leaders align on key decisions and optimize their risk/return perspective.

Companies should base their risk-appetite framework on their risk taxonomy and business imperatives, ensuring that they take account of patient/customer, operational, financial, and employee dimensions. The framework usually contains qualitative statements about the company’s risk-management goals as well as quantitative metrics that can be used to define risk appetite and monitor adherence. The enterprise and the

businesses that will use the framework on a day-to-day basis should jointly develop it so that ownership is shared from the outset.

Financial-services institutions have been leaders in defining risk appetite. One large public-finance corporation developed a series of statements about cyberrisk—such as “very low to no appetite for theft of customers’ personally identifiable information (PII)” —to focus resources on its most critical assets. It linked these statements to metrics such as the number of third parties with access to PII and the number of vulnerabilities identified from hacking simulations. Then it defined thresholds for each metric and set up reporting mechanisms to allow senior-level managers to understand how the corporation’s cyberrisk profile compared with its risk appetite and where investment was needed to fill gaps.

4. Take advantage of big data and advanced analytics

The use of advanced analytics and machine learning to improve risk management is rapidly gaining traction across industries. In the energy and materials sectors, for instance, companies have long used advanced analytics and simulation modeling in planning large projects, such as the opening of a new mine. Such an approach is highly applicable to the analysis of risks in the healthcare sector.

One global pharma company adopted an advanced analytic approach to help it prioritize clinical trial sites for quality audits. The model assesses level attributes to identify which sites are higher risk and the specific types of risk that are most likely to occur at each site. The company is tightly integrating its analytics with its core risk-management processes, including risk-remediation and monitoring activities of its clinical operations and quality teams. The new approach identifies issues that would have gone undetected under its old manual process while also freeing 30 percent of its quality resources.

A leading biopharma company has gone a step further by using simulation analytics to determine the interplay among strategic decisions, risks to the business, and overall outcomes. It analyzes risks across the life cycle of individual programs as well as those affecting the whole company. Next it considers a range of strategic choices: adding to or removing products from the portfolio, licensing development and commercialization to a partner, hiring decisions, and so on. The company then determines which set of choices creates the best conditions for success while enabling it to stay within its risk appetite.

Another area in which advanced analytics can capture significant value is in predictive maintenance. One railway operator we worked with applied advanced analytics to major component failures to reduce its total failure cost for rolling stock by 20 percent. In the pharma sector, in which production is dependent on multiple high-performance components, moving from standard maintenance practices to optimized analytics-driven approaches could yield similar cost reductions; more importantly, the approach could reduce downtime for valuable assets.

In the financial-services sector, institutions are exploiting rich data sources to develop new insights into risk in areas as diverse as underwriting, marketing, operations, and compliance.¹ One bank analyzed complaint data using a machine-learning engine to identify recurrent issues and monitor conduct risk. Taking a publicly available database published by the Consumer Financial Protection Bureau, it used automated natural-language processing to analyze the content of free-text complaints and extracted 15 topics, including potential fraud in account opening. It also developed insights into how new topics emerge, spike, and trend over time. Thanks to this effort, the bank can identify possible compliance risks before they become significant issues.

5. Form strong crisis-management preparedness

However robust an organization's risk-management capabilities, they can never rule out the possibility of a crisis event. Indeed, research has shown that such events have at least doubled—and in some cases more than quadrupled—over the past ten years across industries.² As the threat level increases, so does the need to not only improve core risk capabilities but also maintain a strong level of crisis preparedness.

Being prepared for a crisis includes both obvious elements, such as ensuring that senior leaders can quickly respond, and less-obvious aspects, such as integrating crisis scenarios into budgeting and planning. Too often, crisis-management training and preparation revolves around crisis communications, which is only one part of a much broader challenge. Instead, executives need to plan how the whole company would function during a crisis.

That preparedness planning needs to include considering how the organization and leadership will respond, how to stabilize stakeholders, and which operational and technical activities will be critical. It should include deciding how investigation and governance will be conducted; how marketing, brand, and communications teams can help with crisis management; and what financial and liquidity provisions are in place. Finally, it should include thinking through how legal, third-party, and other issues will be handled and how ready the whole organization is to cope with any crisis that might emerge.³

Best-practice institutions thoughtfully plan their crisis-management approaches and regularly update them by identifying risk scenarios, developing playbooks to manage each one, and using war-gaming techniques to practice their responses. One European bank went as far as devoting an entire day to perform a live test of a key crisis-recovery plan as part of its preparedness efforts.



In a fast-changing pharma-sector landscape with rising regulatory complexity, new delivery methods, and data-driven innovation, most companies urgently need to upgrade their risk-management capabilities. Now is the time to adopt best practices from other sectors. A surgical focus on the areas highlighted here will best equip companies to thrive in today's unpredictable environment. ■

¹ Sanjay Kalavar and Mihir Mysore, "Are you prepared for a corporate crisis?," *McKinsey Quarterly*, April 2017, McKinsey.com.

² Ibid.

³ For more information on a list of 25 questions that executives should ask to determine whether their organization is prepared for the worst, see Kalavar and Mysore, "Are you prepared for a corporate crisis?."

Ajay Dhankhar is a senior partner in McKinsey's New Jersey office, **Saptarshi Ganguly** and **Arvind Govindarajan** are partners in the Boston office, and **Michael Thun** is a senior expert in the Munich office.

Copyright © 2018 McKinsey & Company.
All rights reserved.