Pharmaceuticals and Life Sciences

Leveraging IT risk management to boost competitive advantage

Achieving integrated information technology, governance, risk, and compliance

Table of contents

The heart of the matter

Leveraging an IT Governance, Risk and Compliance foundation to create a competitive business advantage

The pharmaceutical and life sciences industries face unprecedented compliance challenges, and the close regulatory scrutiny of the industry is likely to only increase. Globalization, information protection requirements, business partnerships, heightened transparency expectations, external reporting obligations, and other drivers are forcing companies to reexamine their enterprise approach to information technology (IT) governance, risk, and compliance (GRC).

At the same time, the industry faces new pressures as the pipeline of blockbuster drugs dwindles, patents expire, and research and development (R&D) productivity decreases. Continued growth in convergence and outsourcing add to an already tangled mix.

These challenges make clear that companies in this historically profitable industry increase their reliance on technology to facilitate the necessary transformation. Technology also enables companies to deliver on promises of transparency, risk management, and enhanced compliance.

To ensure the innovation necessary for continued industry success, it is critical that companies implement a robust and agile risk-based technology compliance foundation. Businesses in the industry must shift away from a costly and inefficient compliance approach that reacts to regulations or inspections and audit findings with expensive, singular or redundant solutions. And as the risk and compliance profile of the industry changes with the introduction of increased technology, companies must focus on establishing embedded and sustainable risk management and compliance processes that continually anticipate and proactively manage risk on an ongoing basis.

At a time when pharmaceutical and life sciences companies must focus on cutting costs, organizations struggle to determine how to best spend scarce dollars on needed IT services and projects. A proactive and risk-based technology governance, risk and compliance approach will allow companies to better manage the cost of compliance, to streamline compliance and business processes through increased automation, and to fuel innovation objectives.

Companies that take action first not only will have a greater chance of survival — but also they can potentially gain a competitive advantage.

An in-depth discussion

Industry challenges place technology at the forefront of change, innovation, and sustainable IT Governance, Risk and Compliance solutions

Current challenges and trends point to tremendous changes on the horizon for the pharmaceutical and life sciences industry. Companies need to begin rethinking how they will operate into a more complicated future if they want to remain competitive.

As this transformation takes shape, pharmaceutical and life sciences companies must balance increasing regulatory pressures and cost management with the world's changing needs for medications. And they must do so by determining and working within an acceptable and controlled level of risk.

A 2008 PricewaterhouseCoopers (PwC) IT governance, risk, and compliance survey of 17 pharmaceutical and life sciences companies reveals a consistent challenge across the industry: A siloed approach to IT organization, process, and technology has resulted in reactive and costly technology GRC efforts that are based on functional or regulatory requirements. Instead, organizations need a proactive, efficient, and cost-effective risk-based approach that provides a foundation for innovation rooted in a sound understanding of the business needs.

This challenge demands a more coordinated approach toward risk and technology compliance. To effectively manage risk to an acceptable level, companies should consider adopting a framework that facilitates consistent decision making related to risk management, required policies, internal controls, and sustainable compliance.

As part of PwC's 2008 IT GRC survey, companies were queried in the following areas: IT risk management, IT governance, policies and standards, procedures, controls, monitoring, and data management. In our experience, these categories represent the elements of a successful IT governance, risk, and compliance program. The discussion that follows is based on company survey responses and subsequent interviews with a selection of participating organizations.

PwC surveyed 17 pharmaceutical and life sciences companies and supplemented that data by interviewing individuals across functional areas, including chief information officers, IT compliance organization leaders, general counsel, privacy, risk management, and internal audit.

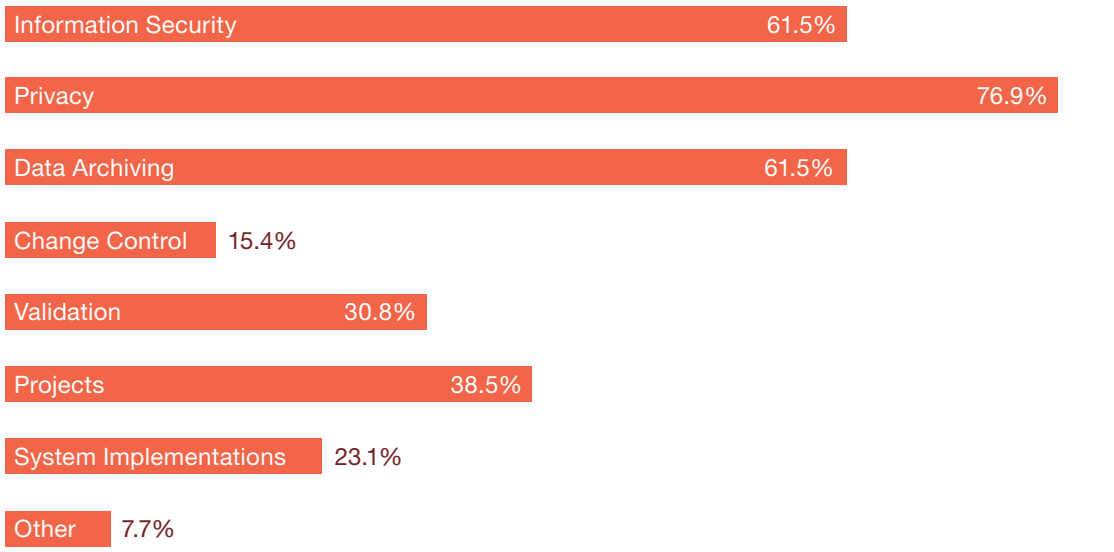
IT risk management should reach beyond compliance

Our survey revealed that organizations have broad and varying definitions and interpretations of risk.

All survey respondents indicated they have a sustainable IT risk management process in place to identify risk; however, only 60 percent have consistently defined risk across the organization and applied that definition to decision making. In addition, their risk efforts focus on compliance with laws and regulations, and they place much less emphasis on operational risk areas.

Based on our discussions with respondents, we learned that companies define risk differently across the organization. Respondents said quality assurance, internal audit, external audit groups, finance, legal, and IT units seldom have a consistent view of risk and use various tools and templates to introduce risk management into IT processes. Despite the different views and definitions of risk, our survey indicated the industry agrees that security, privacy, and data retention rank as priority risk areas. More than 60 percent of respondents said information security and data retention/archiving are key risk areas, while 76.9 percent indicated that privacy is a priority risk area. See Figure 1.

Figure 1: Percentage of surveyed companies that view the following as top compliance challenges



Source: PwC survey of IT governance, risk, and compliance among 17 pharmaceutical and life sciences companies, 2008

Respondents also stated that few organizations have formal processes in place to embed risk management into decision-making processes, and fewer have defined who will be accountable for deciding an acceptable risk level. Most companies said they struggle to define their risk tolerance, the risk appetite of the organization, who makes these cost/risk trade-off decisions, and how IT risk links to business objectives.

In the current market, risk management is garnering a significant amount of attention across all industries. Boards of directors want to know that companies understand and manage key risks. And Standard & Poor's is now evaluating enterprise risk management (ERM) programs as part of its larger rating program. The Food & Drug Administration (FDA) has been promoting a risk-based compliance approach and quality by design, and Sarbanes-Oxley along with related auditing standards now promote a top-down risk-based approach.

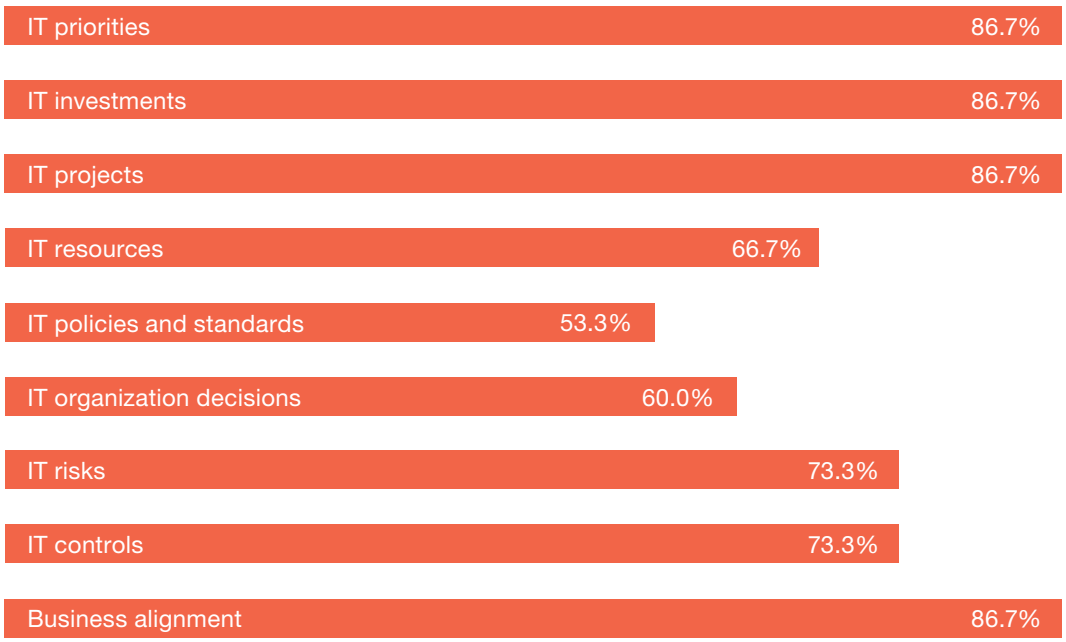
In our experience, the most successful companies across all industries have developed IT risk policies that articulate the desired or targeted IT risk level. This is supported by a sustainable governance process to establish clear accountability for managing risk to an acceptable level based on the risk tolerance of the organization. The acceptable level of risk is based on business input and the risk appetite/risk tolerance of the company as a whole.

Because IT supports the entire organization and must manage more compliance requirements than most other areas of the business, IT often makes the first attempt to define a risk management program that will streamline compliance in the absence of an overall ERM program. While linking ERM to IT risk is in the early stages at most companies in the industry, the connection between ERM and IT risk is essential to better align prioritization of and responses to IT risk with the organization's overall risk tolerance. Without this link, IT GRC programs will not succeed, and IT projects may not be prioritized based on the needs of the business.

IT governance should incorporate risk

Many companies in the pharmaceutical and life sciences industry report they have achieved excellence in IT governance, which is a critical component for establishing necessary IT risk and compliance decisions. Nearly all of the survey respondents (86.6 percent) said they have deployed a documented IT strategy and vision that clearly articulates IT goals. The same number have aligned that vision with the overall business strategy; however, only slightly more than half (53 percent) of the respondents indicated the IT governance groups include both IT and business representation. Most of the organizations (86.7 percent) said they established a governance process for timely decision making regarding IT priorities, investments, projects, and business alignment. Only half have a process to make decisions and to drive consistent IT policies and standards. Although nearly half of respondents (46.7 percent) indicated that an IT risk and compliance role has been established that reports directly to the chief information officer, only 20 percent of IT governance committees include an IT risk and compliance representative. In our experience across industries, many companies also have IT risk governance committees that are separate and distinct from their overall IT governance committees. See Figure 2.

Figure 2: Percentage of surveyed companies whose IT governance process includes timely decision making in the following areas



Source: PwC survey of IT governance, risk, and compliance among 17 pharmaceutical and life sciences companies, 2008

Despite the fact that many companies have elements of an effective IT governance process, most are immature when it comes to applying risk to the governance process. The majority of respondents interviewed said that IT governance processes have not yet evolved to formally address decision making related to risk tolerance; to align the definitions of risk across IT and the business; and to establish clear accountability and responsibility for risk management, policies, standards, procedures, controls, and compliance monitoring. Another theme identified in follow-up discussions found that larger organizations often establish duplicative committees and councils to discuss and drive decision making related to risk management; however, these committees often lack accountability and do not effectively align decision making with the overall business and IT strategy.

Many organizations also have program management offices in place to oversee projects related to a specific regulatory requirement (FDA, Sarbanes-Oxley, privacy). But most do not consistently establish common IT processes or controls that satisfy a number of regulations and IT operational requirements.

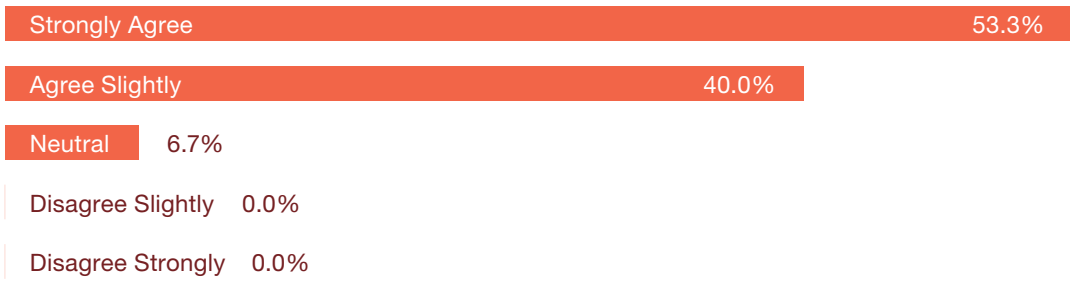
A successful governance process should include business and IT representation for decision making regarding project prioritization, portfolio management, risk management, policies, and internal controls and be the responsibility of the chief information officer.

Policies, standards, procedures, and controls must be defined and refined into a common control set

Although many companies believe they have aligned key policies, standards, procedures, and controls to IT risks, redundancies and disconnects are common.

All but one of the survey respondents said IT policies and standards have been defined based on key IT risks. Most (93.3 percent) said procedures align with and support policies and standards. And all said their controls are based on key risks to IT and the business. See Figure 3.

Figure 3: Percentage of surveyed companies that believe IT policies and standards have been defined based on key IT risks



Source: PwC survey of IT governance, risk, and compliance among 17 pharmaceutical and life sciences companies, 2008

Yet, based on our discussions with respondents, most companies have not developed a simplified framework that links to a formal IT risk management process, maps to a set of common IT controls, and defines parties accountable for each policy area. In many cases companies have established overlapping and redundant policies, standards, or procedures, and they do not follow a consistent set of documents. We also found that companies are not typically mapping IT risk, policies, standards, and control requirements to a defined set of IT capabilities to verify that appropriate skill sets are in place to manage defined risks.

We learned that many companies have inconsistent definitions for policies, standards, procedures, and controls, and that the process to keep these documents current and aligned, based on risk, do not typically exist. We noted many examples where policies, standards, and procedures have references to inaccurate, missing, or incomplete information. Mergers and acquisitions have further complicated the issue.

Across many IT organizations, different groups have established policies, procedures, and controls at varying levels of detail and structure based on their definition of risk and their specific regulatory requirements. Companies often have siloed standards and controls to meet specific FDA, Sarbanes-Oxley, privacy, Prescription Drug Marketing Act, Foreign Corrupt Practices Act, and other regulatory requirements without considering the common elements of control that cut across these regulatory requirements.

Successful technology GRC programs begin with a simple and consistent definition of policies, standards, procedures, and internal controls. Other key factors include: developing streamlined and focused IT policies that represent management's intent; establishing clear accountability for deployment and enforcement of policies, standards, and procedures; and developing a "common control set" that addresses multiple related regulatory and operational control requirements into a single company control library that is aligned with the results of the company's risk assessment activities. Once a risk-based common control set is established, successful companies embed these requirements into their systems to consistently deploy internal controls. The most successful companies across industries use Enterprise Risk Management assessments to establish a risk baseline that is periodically updated to reflect changes in the environment and the business.

Compliance and monitoring can increase business benefits

Many pharmaceutical and life sciences companies (73.3 percent) see IT GRC merely as a regulatory requirement and a nondiscretionary additional cost. Only 30 percent of respondents viewed IT GRC as a benefit that could help the business better manage its processes, increase efficiencies, and ultimately help create a competitive business advantage.

Nearly all of the survey respondents (93.3 percent) said they have a process in place to test and monitor compliance with their company policies and controls. The same number said compliance testing and monitoring processes are based on risk; however, approximately 93 percent of respondents indicated their company needs to more effectively monitor the controls in place at third-party outsourcing providers. Additionally, 80 percent expressed that a more effective compliance dashboard needs to be developed and leveraged for reporting on the health of IT risk management and compliance to company management. Improved monitoring and reporting will become increasingly important given the increase in outsourcing to third parties (73 percent have outsourced help desk, 64 percent infrastructure, 46 percent applications, and 27 percent business processes).

Although there is a trend toward metrics and compliance reporting that includes root cause analysis and corrective and preventive action programs (93.3 percent), only 26.7 percent indicated that trending is performed and monitored over time to identify emerging issues.

Data from our survey showed that, as the sharing of data across organizations increases, most of these organizations say information security, privacy, and data archiving pose the greatest challenges.

At many companies, an uncoordinated approach to governance, risk, and compliance has resulted in redundant internal and external audit groups with overlapping objectives, gaps in other areas, and inconsistent monitoring and reporting to senior management. This points to companies not having developed a common risk-based approach to conducting control audits. Often, IT staff members spend significant time responding to inconsistent audit findings, which generally do not take into account the organization's defined risk tolerance.

Once companies establish a common risk management and internal control framework, internal audit and quality groups can turn their attention to evaluating the effectiveness of the internal control framework as opposed to substantively testing whether a particular control is in place and operating effectively at a point in time. If effectively implemented, this approach can reduce judgment-based audit findings and instead focus on whether IT's internal control and compliance quality system works effectively. See Figure 4.

Figure 4: Percentage of surveyed companies that believe controls are based on key risks to IT and the business

Source: PwC survey of IT governance, risk, and compliance among 17 pharmaceutical and life sciences companies, 2008

Most companies queried have established IT compliance organizations to address Sarbanes-Oxley regulations, FDA regulations, IT risk, controls, continuity planning, compliance testing, and reporting. However, as the sharing of data across organizations increases, most of these organizations say information security, privacy, and data archiving pose the greatest challenges.

As interactions among healthcare payers, providers, and pharmaceutical and life sciences companies grow, exchanging and protecting large volumes of sensitive and confidential data will become increasingly important. While greater collaboration facilitates the necessary industry transformation, it also exposes the industry to increased risk, particularly to the integrity and privacy of information in the health IT value chain. Regulators recognize the risk. In fact, during the first seven months of 2008, the FDA issued more than 200 warning letters, and states have decided to focus more heavily on enforcement because of several industry privacy breaches.

As the number of legal and regulatory requirements increases, regulators and auditors will increasingly scrutinize IT on its ability to comply and sustain compliance with these rules, while also protecting sensitive intellectual property and personally identifiable information subject to global and state privacy laws.

The most successful technology GRC programs have initially identified the various internal and external groups responsible for auditing and monitoring compliance across the organization. The charters and scope of these groups are aligned, where possible, with the key technology risks identified by management to avoid redundant efforts. Similar to a quality management system (QMS) approach, the compliance and monitoring functions are beginning to focus on evaluating the ongoing effectiveness of the entire GRC framework rather than the effectiveness of a single control at a particular point in time. High-performing technology GRC functions also consistently use compliance dashboards across the entire organization to report risk management and compliance status to various levels of management. Many high-performing governance, risk, and compliance functions also have mapped key controls to the associated regulations to more easily identify the impact of a control breakdown or deficiency. These organizations are also beginning to automate manual compliance processes to streamline business processes, improve compliance sustainability, reduce reliance on individuals, and reduce the cost of compliance.

Data is central to IT GRC

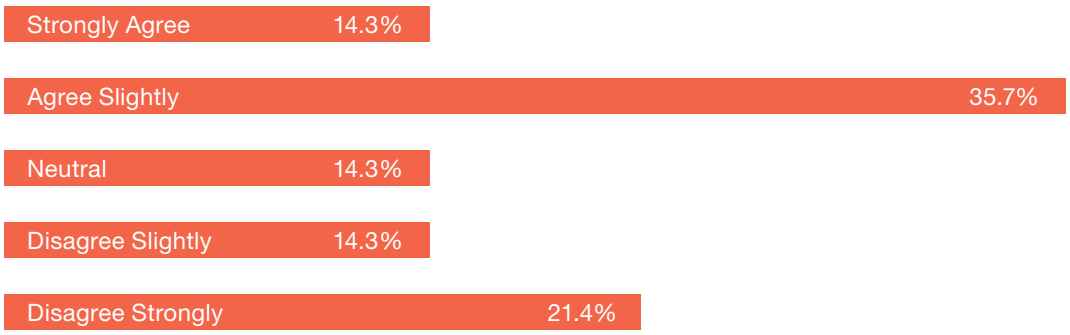
Information is the common denominator in all of the functional areas outlined above, and it is clear that data management is a significant area for improvement within the industry.

More than 85 percent of respondents indicate that improvements are necessary with respect to defining data owners for all categories of data, classifying data, establishing a sustainable data cleansing process, establishing an effective record archiving and retention program, and protecting data based on the associated business value and sensitivity.

Information must be classified and protected accordingly as it is transferred across the enterprise, maintained in structured and unstructured formats, and safeguarded when transferred outside of the organization.

However, most organizations have not named owners for all data categories, and in many cases owners are not held accountable for determining how valuable the data is to the business. Also, in many cases, it is unclear whether the business unit or IT is responsible for the data. Often, the business feels it is IT's responsibility to own and define the business value for the data, but data decisions and responsibility should reside within the business. See Figure 5.

Figure 5: Percentage of surveyed companies that have identified business owners for all categories of data



Source: PwC survey of IT governance, risk, and compliance among 17 pharmaceutical and life sciences companies, 2008

A risk-based approach helps companies consistently protect, cleanse, maintain, and archive and dispose of data. This is increasingly important as the virtual walls of the company expand, information is used in new ways, and the volume of exchanged information increases significantly. Ultimately, the data collected by pharmaceutical and life sciences companies will fuel R&D efforts, identify high-performing drugs, and track drug safety trends. In addition, automation can streamline business processes and compliance, thus saving time and money.

Understanding relationships in all areas will form a foundation for effective IT GRC

The complex layers of IT GRC cannot effectively operate in silos if companies hope to achieve the innovation that will position them ahead of the competition. The industry's transformation requires that pharmaceutical and life sciences companies first build a strong IT GRC foundation that can act as a springboard for distinctive and innovative business solutions.

An integrated IT GRC approach—one that addresses the end-to-end relationships in each of the functional areas outlined above—bridges the gap between the current technology compliance state of the industry to the future direction of the industry.

Figure 6: IT GRC components

To achieve an effective IT GRC program, companies need to:

- Establish a governance process that defines clear accountability and responsibility for the components of the IT GRC program
- Understand the strategic, operational, financial, environmental, reputational, and compliance risks that could affect business objectives
- Determine a companywide acceptable risk level based on an overall risk tolerance
- Establish succinct policies and standards that reflect management intent and are based on the organization's risk and control decisions
- Define a set of procedures to support policies and standards
- Establish a sustainable common control set that aligns with key risks and related regulatory control requirements
- Establish IT support processes to maintain the compliant state of regulated systems and their underlying supporting IT infrastructure
- Train people accordingly to ensure a common understanding and consistent compliance across locations
- Develop a compliance monitoring and reporting process that assures management that key risks are being addressed
- Assess the assurance coverage provided by different audit functions to ensure that all key risk areas are properly addressed
- Select and deploy appropriate tools to monitor the effectiveness of compliance on a consistent and ongoing basis across locations

More and more companies are now recognizing the need for automated solutions for IT GRC that unify all assessment activities, link risks to controls to regulations, to effectively require and enforce compliance activities and to improve risk aggregation and reporting.

What this means for your business

Commitment to integrated IT Governance, Risk and Compliance can boost competitive advantage

A foundational and integrated approach to IT governance, risk and compliance will be necessary to address the emerging risks companies will face as the pharmaceutical and life sciences industry increases collaboration and shares electronic information across the Health IT value chain. But this approach will be even more essential to better manage compliance costs and to drive improved, automated and controlled business processes.

Our experience working in other industries with companies that have been successful using an integrated approach to IT GRC reveals fundamental success factors that must be addressed, including:

- Don't boil the ocean. Companies successful in establishing an integrated IT GRC program execute simple steps that fit within the current structure at their organizations. For example, companies are expanding the agendas of existing IT governance meetings to include business concerns as well as discussions and decision making related to risk management and compliance.

- Define accountability. Companies should clearly define accountability through a governance process for IT risk management, policies, internal controls, and compliance within the appropriate IT functional area that aligns with how individuals are evaluated and rewarded.

- Establish a common language. Often, different GRC groups have similar objectives and initiatives but use different words to describe common activities. Having a consistent set of terms and a process to align common objectives and related terms is essential to the success of an integrated IT GRC program.

- Measure teamwork and foster collaboration. The elements of a successful integrated compliance program must include team metrics and measures to promote teamwork across the business, functional IT groups, quality assurance, and audit groups.

- Promote sustainability. Establishing a sound IT GRC program is not a single event. Building risk management into recurring natural activities, such as the strategic planning and budgeting processes, embeds desired risk management thinking into the organization and starts to build a risk-aware culture among all employees.

- Think continually about improvement. The most successful companies have a simple process in place to capture the root cause of issues, establish corrective action plans, continually evaluate trends and compliance patterns, and continually focus on improving the GRC environment.

Companies can realize several significant benefits by taking an integrated approach to IT GRC. Furthermore, once the company achieves governance, risk, and compliance in a more efficient and effective manner, it can leverage IT and automation to streamline compliance and business processes and create business value. This approach allows management to establish a defined method for decision making regarding risks, controls, and compliance that helps ensure the organization considers key risks. Companies can better anticipate and manage risks before they become problematic and thereby avoid potential reputational damage, fines, penalties, or lost revenue. Furthermore, a focused set of controls that specifically addresses risks can help manage the cost of compliance. Many companies strive to comply with redundant audit findings, but a GRC framework helps companies to align controls with the organization's risk tolerance. Additionally, improved alignment between management, internal and external audit groups can simplify the audit process and free up time for strategic initiatives and activities.

The time and money that can be saved by implementing these practices will become increasingly important as pharmaceutical and life sciences companies begin to rethink their operations as they contemplate a changing business environment where increasing interactions with payers and other organizations affect the use of data. By shoring up the governance, risk, and compliance foundation, IT can shift its focus to automating business processes, managing data, and enabling the innovation essential to discovering the preventive medications needed for the future.

Case Study 1

Challenge

PwC helped a global pharmaceutical company align regulatory controls with key financial, operational, and compliance risks so that all risks, controls, and test plans could be incorporated in an automated tool for compliance monitoring and reporting.

Benefit

The effort reduced key controls and compliance tests by more than 50 percent and allowed those involved in these compliance activities to focus on more strategic activities that were aimed at improving business value.

Case Study 2

Challenge

PwC assisted a global pharmaceutical company as it developed a proactive approach to identify and manage risk that included streamlined IT policies, standards, and procedures, a common definition for risk, and a risk register (inventory of prioritized risks). The company expanded its IT governance process to include risk decision making and enhanced its compliance reporting through a common control set.

Benefit

The approach reduced compliance efforts and costs by nearly 50 percent and reduced spending on projects to correct control deficiencies by approximately $3 million.

How PwC can help your organization

Leveraging the fundamental success factors, PwC has helped organizations execute the following steps to establish an integrated IT GRC program:

- Establish a process to identify, prioritize, and organize key risks, determine the impact and likelihood of the risk, and evaluate the adequacy of existing controls.
- Establish a governance process to decide on the level of risk that is acceptable and aligned with the organization's business objectives and the overall enterprise risk management program.
- Agree upon a set of standard risk categories and assign appropriate accountable owners for each category. In our experience, these risk categories should consider how IT-related people, process, or technology events can impact business objectives in the following areas:
  - Research and development
  - Sales & marketing
  - Manufacturing
  - Quality
  - Finance
  - Legal
  - Human resources
  - IT infrastructure
  - Sourcing
- Create a risk register (i.e., inventory of prioritized risks) by defining key risks for each category, determining existing controls, and determining the impact and likelihood of the risk occurring.
- Define a risk-based approach for the prioritization of IT projects as part of the annual IT budget exercise.
- Establish a common definition and taxonomy for policies, standards, and procedures and simplify the existing set of documents.

- Establish focused policies that represent management's intent for key risk categories along with supporting standards and procedures where necessary.

- Define a common control set of internal controls across regulations (FDA, Sarbanes-Oxley, privacy, etc.) and internal operational requirements that aligns with key risks and policy areas.

- Map IT risks, policies, standards, procedures, and controls to IT capabilities and identify any skill areas that require enhancement.

- Embed common controls into the company's system development life cycle. Then establish a consistent quality process to verify that key controls are established as part of new system implementations and support processes are established to sustain the compliant state of IT-regulated systems and their underlying IT infrastructure.

- Align the scope and objectives of internal and quality audit activities and functions to the IT GRC framework to minimize duplication and overlap of audit activities.

- Establish a dashboard reporting process that can be leveraged as part of standing IT leadership team meetings to review compliance progress and align compliance performance to individual performance measurement and rewards.

- Create a continual improvement process that evaluates the root cause of compliance gaps, anticipates and addresses potential risks, evaluates trends, anticipates risks based on emerging changes in regulation or business conditions, and establishes timely solutions.

- Select and deploy appropriate tools to monitor the effectiveness of compliance on a consistent and ongoing basis across locations and to link risks to policies, standards, procedures, controls, and compliance monitoring results.

- Employ training and communications to foster adoption of the IT governance program and to drive fundamental behavior change.

- Reinforce desired risk management behaviors with ongoing communications and performance measures to build a risk-aware culture among all employees.

Organizations are at varying levels of readiness to implement this model. And while no one-size-fits-all solution exists, PricewaterhouseCoopers has developed a maturity model that can facilitate decision making regarding where to start and how far an organization wants to go to address IT GRC. Options range from basic foundational steps to meet minimum

compliance requirements with manual, paper-based processes, to a level of maturity that automates business, IT, and compliance processes to promote sustainability and improved business performance while incorporating the company control culture and risk appetite.

A successfully implemented IT GRC program can not only reduce the cost of compliance, but also can free up valuable time and resources to focus on distinctive business solutions. Companies facing significant regulatory requirements have been able to use technology to create a competitive advantage by automating business and IT processes with embedded compliance requirements.

As industry transformation continues, technology will become more integral to company success; however, this success can be realized only if new and emerging risks created by technology innovation are proactively anticipated and managed through a defined governance process and the right behaviors. A reactive approach to risk and compliance will not be viable as transformation and increased collaboration continues. The companies that are able to quickly establish a proactive approach to IT governance, risk and compliance have the opportunity to create a competitive advantage by using that approach as a differentiator in the marketplace. A proactive risk based technology compliance approach can be leveraged to build increased trust with potential business partners regarding the integrity, confidentiality, and availability of information maintained, processed, and transferred by the organization.

Companies need to determine how far they want to go to address integrated IT governance, risk, and compliance. Those who are fully committed can transform their focus from necessary compliance requirements to a more strategic approach that can leverage technology to fuel business innovation, foster the right behaviors, manage compliance expenses, and boost their competitive advantage.

As our experience and this survey shows, the industry consistently acknowledges that an integrated IT GRC approach is necessary and beneficial. Although many companies have progressed in their efforts to establish elements of a successful IT GRC framework and many believe they have a solid foundation, we have found that considerable work still must be done to develop effective programs that consistently manage existing and merging risks.

PricewaterhouseCoopers' Global Pharmaceutical and Life Sciences Industry Group (www.pwc.com/pharma) is dedicated to delivering effective solutions to the complex strategic, operational, and financial challenges facing pharmaceutical and life sciences companies. We provide industry-focused assurance, tax, and advisory services to build public trust and enhance value for our clients and their stakeholders. We draw on the knowledge and skills of more than 155,000 people in 153 countries from across our network to share their thinking, experience, and solutions to develop fresh perspectives and practical advice.

pwc.com/pharma

To have a deeper conversation about how this subject may affect your business please contact:

Pat Roche
Partner
Pharmaceutical & Life Sciences Group
Phone: +1 (973) 236-4844
Email: pat.d.roche@us.pwc.com

Brian Riewerts
Principal
Pharmaceutical & Life Sciences Group
Phone: +1 (410) 659-3390
Email: brian.riewerts@us.pwc.com

Attila Karacsony
Director
Pharmaceutical & Life Sciences Marketing
Phone: +1 (973) 236-5640
Email: attila.karacsony@us.pwc.com