Insights on Global Compliance Practices

Benchmarking Results from Protiviti’s Global Financial Services Compliance Survey
Introduction

The financial services landscape has changed dramatically over the decade since the financial crisis. Numerous products and business practices were banned or heavily restricted, capital requirements have been increased, and thousands of pages of new regulations have been issued. There has been a dramatic increase in principles-based risk management and examiners have redoubled their focus on weaknesses identified in their regulated institutions’ risk and compliance management programs, resource levels, and internal oversight mechanisms. Risk and compliance functions drastically increased headcount and other resources to meet the challenges of the new operating environment.

More recently, however, we have observed the financial services industry begin to shift from the regulatory-focused post-financial crisis period into a more growth-oriented operating environment with an emphasis on financial innovation. As the regulatory pendulum swings back to a more balanced position, financial institutions have the ability to stand back and reassess the effectiveness of their compliance functions that have grown exponentially in line with the myriad regulations issued over the past decade. Rather than continue with the traditional practice of adding headcount to solve new problems, firms are seeking ways to cut costs by becoming more efficient and more agile to better respond to the continuing compliance challenge. Over the past couple of years, existing enforcement actions have been resolved successfully and the pace of new actions has finally started to slow. As a result, C-suite executives are scrutinizing requests for continuing risk and compliance investments more heavily, especially in an environment where regulatory pressures are reducing, creating opportunities for business innovation and top-line growth.

This set of circumstances led Protiviti to develop its Agile Risk & Compliance approach.1 Central to the Agile philosophy is the belief that every organization’s risk and compliance function can be an enabler of their firm’s business strategy, rather than being viewed as an impediment. Having a more flexible approach to risk and compliance challenges, aided by technology and a more aligned strategy, allows companies to ensure they continue to meet the constant compliance challenges and are ready to react quickly to changes in business models and the operating environment.

To be able to more objectively measure the financial services industry’s perceptions of, strategies for and progression toward Agile transformation activities, Protiviti conducted a survey of hundreds of financial services organizations around the world.

---

Collectively, our survey results strongly support our experience that the market is embracing the pursuit of Agile objectives. More than three out of four respondents (77 percent) indicated their risk and compliance organizations are facing either strong pressure to reduce costs or increased demand to manage spending levels. However, the results also indicate that financial services organizations are closer to the beginning than the end of their efforts to achieve Agile objectives on the whole.

Only 20 percent of firms consider their coordination efforts for risk and compliance activities to be fully synchronized across all three lines of defense, while just one in four respondents (25 percent) claims that the risk and compliance function has a high level of engagement in the development of the firm’s business strategy, and less than half (48 percent) claim a high level of engagement in business initiatives that impact the firm’s compliance risk profile.

The use of technology is increasing slowly. Although 75 percent of firms use data analytics for compliance purposes and have invested in dedicated software platforms for this purpose, just over one in four respondents rates the maturity of their firm’s use of these capabilities at a high level. Over half of respondents (54 percent) highlighted budget constraints as well as the difficulty in measuring the expected return on investment (ROI) to support the business case as barriers to the increased use of technology for compliance purposes. More than half have concerns about gaps in the integrity of underlying business data that would be subject to analysis. In comparison, only 41 percent of respondents cite a lack of executive-level support for such investments. This suggests there is appetite all the way to the top of most organizations to pursue these capabilities, yet there is a lack of confidence in the results of such investments.

This paper presents the results of our global compliance survey in greater detail, posing some questions for compliance executives on the path forward to a more Agile state of compliance.
Protiviti’s survey was targeted to financial services executives, directors and managers with ownership or knowledge of risk and compliance operations at their companies. The survey focused on firms in North America; Europe, the Middle East and Africa (EMEA); and the Asia-Pacific (APAC) regions with annual revenue of at least $5 billion USD. Some 300 financial services firms meeting these criteria participated in this survey.
Executive Summary

Geographic, segment and size outliers

The survey results highlighted the differences in the maturity of the compliance functions between the various financial services segments and company sizes located in different regions of the world.

- Fewer Asia-Pacific (APAC) respondents characterize the current state of regulatory scrutiny as “high” (12 percent), compared to 24 percent of North American respondents.

- The highest majority of responses that describe the current state of regulatory scrutiny as high or somewhat high are from the insurance sector (78 percent) and the asset management sector (71 percent). The largest proportion of insurers (47 percent) considers the level of regulatory scrutiny to be increasing.

- Overall, two-thirds (68 percent) of the respondents globally feel the intensity of regulatory scrutiny is currently “high” or “somewhat high,” while more than half of respondents consider the degree of regulatory scrutiny to be stable or decreasing.

- APAC respondents are significantly less likely to believe the direction of regulatory scrutiny is increasing (30 percent) compared with those in other regions, with 52 percent describing it as stable.

- APAC firms have been slower to leverage data analytics capabilities for compliance activities, with 44 percent reporting that they are not using data analytics in compliance at all, compared to 19 percent in North America. A strong majority of EMEA firms — 76 percent — currently use data and analytics for compliance.

- Most APAC respondents describe efforts to coordinate risk management activities across the three lines of defense as being underway but not yet effectively synchronized (46 percent) or only moderately synchronized (46 percent). The largest proportion of firms with risk management activities coordinated across the three lines of defense is in North America, where 26 percent of respondents said that efforts were fully synchronized. Overall, EMEA companies as well as larger companies (both those with more than 25,000 employees and those with over 2,000 full-time compliance employees) are most likely to have coordinated risk management activities across the three lines of defense.

- Financial services firms are more likely to have high levels of engagement in new business initiatives across all regions, industry segments and organization size (48 percent) rather than in business strategy (25 percent). There is a consensus that, overall, the compliance function is moderately engaged in business strategy (60 percent). APAC respondents are least likely to have high levels of engagement in business strategy (10 percent) or new business initiatives (30 percent), compared with North America and EMEA respondents.

Collectively, our survey results strongly support our experience that the market is embracing the pursuit of Agile objectives. More than three out of four respondents (77 percent) indicated their risk and compliance organizations are facing either strong pressure to reduce costs or increased demand to manage spending levels. Increased use of technology clearly plays a pivotal role in this effort, as nearly 60 percent of respondents now say their companies use enterprisewide governance, risk and compliance (GRC) software tools, and of those that are not, nearly half intend to implement a GRC platform within the next year.
That said, the results also indicate that financial services organizations are closer to the beginning than the end of their efforts to achieve Agile objectives on the whole. For example:

- Only 20 percent of firms consider their coordination efforts for risk and compliance activities to be fully synchronized across all three lines of defense.

- Just one in four respondents (25 percent) claims that the risk and compliance function has a high level of engagement in the development of the firm’s business strategy, and less than half (48 percent) claim a high level of engagement in business initiatives that impact the firm’s compliance risk profile.

- Only 11 percent of respondents noted that compliance controls are a critical and consistent consideration within the design of business processes and supporting system workflows.

- Although 75 percent of firms use data analytics for compliance purposes and have invested in dedicated software platforms for this purpose, just over one in four (27 percent) rates the maturity of their firm’s use of these capabilities at a high level.

- When asked about barriers to the increased use of technology for compliance purposes, 54 percent of respondents highlighted budget constraints, but even more (55 percent) expressed difficulty measuring the expected return on investment (ROI) to support the business case. More than half have concerns about gaps in the integrity of underlying business data that would be subject to analysis. In comparison, only 41 percent of respondents cite a lack of executive-level support for such investments. This suggests there is appetite all the way to the top of most organizations to pursue these capabilities, yet there is a lack of confidence in the results of such investments and many firms face the need to mature their own IT and MIS infrastructure elements before buying in.

**Returning to growth**

The new political and economic environment has created a moment of cautious and uncertain optimism on the part of firms’ leadership teams, who are excited about the possibility of shifting their focus to growth after a decade of cost cutting. While certain regulatory relief measures have been enacted in the United States, more significant changes continue to be debated. Leaders know that regardless of what happens on the legislative front, examiners will swiftly criticize any perceived loss of focus on risk and compliance capabilities. In turn, this could result in regulatory actions that would threaten firms’ growth strategies. Many of these executives also:

- Generally believe the greatly enlarged risk and compliance functions they have invested in over the past decade are more effective in managing the firm’s risk, but recognize that many of these enhanced capabilities were built in crisis mode, under strict regulatory deadlines, and likely are not as efficient as they could be.

- Are frustrated that they have not made more progress on preventing risk and compliance issues, even though their firms are much better at finding and fixing them quickly.

- Are concerned that additions of risk- and compliance-focused resources across all three lines of defense have created confusion within the business over which function should be consulted to approve various proposals or changes.

- Have a perception that risk and compliance efforts have become “checkers checking checkers” — these bureaucratic review processes are an increasing cause for concern, particularly as the firm’s product development and other growth initiatives ramp up.
• See increasingly innovative and sophisticated use of data and analytics by fintech companies, and are increasingly pressing their financial institutions to develop similar capabilities within their risk and compliance functions.

Leaders know that regardless of what happens on the legislative front, examiners will swiftly criticize any perceived loss of focus on risk and compliance capabilities. In turn, this could result in regulatory actions that would threaten firms’ growth strategies.

This set of circumstances led Protiviti to develop its Agile Risk & Compliance philosophy. Briefly, the Agile philosophy is founded around the belief that every organization’s risk and compliance function can be (and, in fact, increasingly must be):

• An enabler of, rather than an impediment to, their firm’s business strategy. Risk and compliance functions represent a competitive advantage when they achieve a level of effectiveness and efficiency that allows their firms to act on business opportunities more quickly than their competitors, or pursue strategies their competitors avoid because of their perceived risk levels. This can be thought of as “the fastest cars have the best brakes” analogy.

• Business experts, not just technical risk and compliance specialists, who become trusted advisers on how to embed good risk and compliance practices into business processes during the design phase rather than simply bolting on additional testing activities after the fact.

• Measured on the prevention and/or resolution of compliance failures, as well as the efficiency and effectiveness of their own processes, with an eye toward continuous improvement according to measurable key performance indicators (KPIs).

• Enabled by leading technologies and data analytics capabilities that should allow for more comprehensive insights into the firm’s risks, obtained in a more timely manner relative to when those risks occur, with far fewer resources than comparable manual processes now demand.

• Cognizant of the fact that successfully achieving a firm’s risk and compliance objectives will not only mitigate compliance risk, but also lead to more effective and consistent business practices that result in a better experience for the firm’s customers and other stakeholders.

Many of these objectives sound aspirational, at best, for firms still digging out from under regulatory settlements and simply trying to clarify the roles and responsibilities among the various risk and compliance functions that now exist within the organization. That said, these objectives — and the concept that their organization should at least be working in this direction — have resonated strongly with financial services executives.

As a result, nearly every organization Protiviti works with is pursuing one or more elements of the Agile concept, whether that takes the form of a wholesale transformation of their risk and compliance programs, or simply trying to make existing processes incrementally more efficient, such as automating activities that are performed manually today.
Geographic Observations

Our experience has been that many firms in the APAC region have not seen the same post-crisis level of regulatory scrutiny and enforcement activities that their North American and EMEA peers have. Additionally, certain areas of regulation that tend to require broad, enterprise-wide governance programs and infrastructure elements to address effectively — such as anti-money laundering requirements — have been implemented more recently in APAC.

Our survey responses confirmed this perception. Fewer APAC respondents characterize the current state of regulatory scrutiny as “high” (12 percent), compared with 24 percent of North American respondents.

Respondents from the APAC region are also significantly less likely to believe that the direction of regulatory scrutiny is increasing (30 percent) than those in other regions, with 52 percent describing it as stable. More than half of all North American respondents said that the direction of regulatory scrutiny is increasing.

Overall, two-thirds (68 percent) of the respondents globally feel the intensity of regulatory scrutiny is currently “high” or “somewhat high,” and two-fifths (44 percent) agree that regulatory scrutiny is stable, while almost half (48 percent) view it to be increasing.

As a result, we would expect APAC-based firms to be at an earlier point on the journey to Agile than those in other markets, and the survey responses bear this out as well.
APAC firms have also been slower to leverage data analytics capabilities for compliance activities, with 44 percent reporting that they are not using data analytics in compliance at all, compared to 19 percent in North America. A strong majority of EMEA firms — 76 percent — currently use data and analytics for compliance.

Although North American and EMEA firms are making headway in coordinating risk management activities across the three lines of defense, organizations in APAC have the most ground to cover, with most respondents describing efforts as being underway, but not yet effectively synchronized (46 percent) or only moderately synchronized (46 percent). The largest proportion of firms with risk management activities coordinated across the three lines of defense is in North America, where 26 percent of respondents said that efforts were fully synchronized.
Efforts to coordinate risk management activities across the three lines of defense

In addition, APAC organizations are least likely to have high levels of engagement in business strategy (10 percent) or new business initiatives (30 percent).

Overall, EMEA companies as well as larger companies (both those with more than 25,000 employees and those with over 2,000 full-time compliance employees) are most likely to have coordinated risk management activities across the three lines of defense.

Overall, EMEA companies as well as larger companies (both those with more than 25,000 employees and those with over 2,000 full-time compliance employees) are most likely to have coordinated risk management activities across the three lines of defense.
Survey Results and Observations

Business line expertise

Most respondents regard the level of compliance expertise and maturity of processes within their organization’s business units as moderately mature (see chart below). Interestingly, just 6 percent of organizations — primarily large firms with revenue over $10 billion and with more than 25,000 employees — perceive their business units to have compliance expertise at a fully mature and best-in-class level. A larger proportion of consumer finance and banking respondents rated their first line of defense compliance expertise and maturity as fully mature compared to other sectors.

Compliance expertise/maturity in first line of defense (by region)

Respondents assessed the level of compliance expertise and maturity of processes within their organization’s business units, the first line of defense in risk management (i.e., lines of business/process owners/revenue-generating function), on a scale of 1 to 5, where 1 = immature/undefined and 5 = fully mature/best-in-class.

These results are consistent with what we have observed in the market. Following the crisis, many firms dealt with simultaneous and significant regulatory criticism of their first (business), second (risk and compliance) and third (internal audit) lines of defense. In many cases, the third and the second lines — in that order — were able to mature their functions and resolve the regulatory matters that pertained to them more quickly than the first line.

Larger firms have also implemented, or are in the process of implementing, “1 1/2” or “1(b)” lines of defense. We define these as fully dedicated groups of risk and
compliance professionals who sit within and report through the leadership teams of a particular line of business and are responsible for centralizing risk identification, assessment, control implementation, and monitoring and oversight activities for their lines of business (LOBs). The chief arguments behind this model are that it brings critical mass, focus, consistency and dedicated expertise to risk management issues that historically were managed by employees in the business who had other primary responsibilities. It also provides a more efficient interaction model by establishing a single point of contact for the business to face off with the second and third lines, external regulators, etc.

The survey results suggest, however, that most organizations feel they have some distance to go in terms of maturity and expertise before these functions are fully effective. This creates risk in the short term, as we are seeing efforts underway across the industry to “push out” from the second into the first line a significant percentage of key risk management activities like monitoring and testing. This would return the second line to a more traditional (and more lightly resourced) standard-setting and oversight role. There are concerns, though, that pushing out responsibilities more quickly than the 1.5 lines of defense are able to pick them up could lead to risk and compliance failures in the interim.

We have spoken with a number of regulatory agency officials who, having become comfortable with large-scale centralized capabilities now resident in the second line, are skeptical of the 1.5 model in general. It would not take much, in terms of regulators seeing quality diminish for activities that have moved to the 1.5 line, to begin pressuring firms to recentralize them in the second line.

---

### Compliance expertise/maturity in first line of defense (by organization revenue)

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>1 - Immature/undefined</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 - Fully mature/best-in-class</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5 billion to $9.9 billion</td>
<td>12%</td>
<td>54%</td>
<td>34%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>$10 billion or more</td>
<td>9%</td>
<td>38%</td>
<td>45%</td>
<td>8%</td>
<td>5%</td>
</tr>
</tbody>
</table>

---

protiviti.com  
Global Compliance Survey Insights • 11
Compliance expertise/maturity in first line of defense (by industry)

- **Banking**
  - 5: Fully mature/best-in-class: 10%
  - 3: Mature: 48%
  - 1: Immature/undefined: 10%

- **Insurance**
  - 5: Fully mature/best-in-class: 6%
  - 3: Mature: 34%
  - 1: Immature/undefined: 13%

- **Broker-Dealer**
  - 5: Fully mature/best-in-class: 58%
  - 3: Mature: 37%
  - 1: Immature/undefined: 5%

- **Asset Management**
  - 5: Fully mature/best-in-class: 35%
  - 3: Mature: 54%
  - 1: Immature/undefined: 11%

- **Consumer Finance**
  - 5: Fully mature/best-in-class: 13%
  - 3: Mature: 42%
  - 1: Immature/undefined: 10%
  - 4: Partially mature: 2%

- **Payments**
  - 5: Fully mature/best-in-class: 43%
  - 3: Mature: 57%
Compared to the first line of defense, internal audit scores lower on the expertise and maturity scale, with nearly half of all responses from compliance executives (49 percent) rating their third line of defense at the midpoint on our 5-point maturity scale. Broker-dealers rated their internal audit functions as higher than average, with 10 percent rating them as fully mature and best-in-class. However, this may be an anomaly since this segment has a much lower total number of responses than other industries.
Regulatory scrutiny

Privacy is the foremost area of regulatory scrutiny for respondents overall and for those located in North America and EMEA. Only respondents in the APAC region did not consider it a top area where regulatory attention was rising.

For most banks, regulatory scrutiny over sanctions is decreasing, with a renewed focus on anti-corruption being perceived by all firms, large and small, and in all regions. However, these results pre-date recent sanctions programs being imposed (or reimposed) by the U.S. government against countries such as Russia and Iran, so any sense of relief in this area on the part of the financial services industry may be short-lived.

Compliance risk management program governance is an increasing area of regulatory focus across all three global regions.

AML and financial crime is a continuing focus for all regulators around the world, but it is named as a top item in APAC for both small and large firms.

In this digital age, cybersecurity remains top of mind for regulators but the intensity seems to be more pronounced in North America and for banks with revenues over $10 billion.

Regulatory attention on executive compensation is perceived to be falling in North America and EMEA, as well as for larger firms.

Although overall, third party risk management is shown to be the fifth area where regulatory attention is decreasing, this is not reflected by our experiences in the marketplace.²

What is your view on the current direction of regulatory scrutiny in each of the following areas?

<table>
<thead>
<tr>
<th>OVERALL RESULTS</th>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Sanctions</td>
<td>Anti-corruption</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance culture and accountability models</td>
<td>Compliance risk appetite framework</td>
</tr>
<tr>
<td>Compliance risk management program governance</td>
<td>Compliance risk appetite framework</td>
<td>Executive compensation</td>
</tr>
<tr>
<td>AML</td>
<td></td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td></td>
<td>Compliance risk appetite framework</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NORTH AMERICA</th>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Sanctions</td>
<td>Anti-corruption</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Compliance risk appetite framework</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance culture and accountability models</td>
<td>Executive compensation</td>
</tr>
<tr>
<td>Compliance risk management program governance</td>
<td>Compliance culture and accountability models</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Compliance culture and accountability models</td>
<td>Executive compensation</td>
<td>Third party risk management</td>
</tr>
</tbody>
</table>

### EMEA

<table>
<thead>
<tr>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Sanctions</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Compliance risk management program governance</td>
<td>Third party risk management</td>
</tr>
<tr>
<td>Insurance capital standards (ICS)</td>
<td>Executive compensation</td>
</tr>
<tr>
<td>Proposed short-term lending rules</td>
<td>Compliance risk appetite framework</td>
</tr>
</tbody>
</table>

### APAC

<table>
<thead>
<tr>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance risk management program governance</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance risk appetite framework</td>
</tr>
<tr>
<td>AML</td>
<td>Heightened prudential standards</td>
</tr>
<tr>
<td>Compliance risk appetite framework</td>
<td>Compliance risk management program governance</td>
</tr>
<tr>
<td>Third party risk management</td>
<td>Anti-corruption</td>
</tr>
</tbody>
</table>

### $5 BILLION TO $9.9 BILLION

<table>
<thead>
<tr>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Sanctions</td>
</tr>
<tr>
<td>Compliance risk management program governance</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance risk appetite framework</td>
</tr>
<tr>
<td>Proposed short-term lending rules</td>
<td>Anti-corruption</td>
</tr>
<tr>
<td>AML</td>
<td>Third party risk management</td>
</tr>
</tbody>
</table>

### $10 BILLION OR MORE

<table>
<thead>
<tr>
<th>TOP 5 AREAS – INCREASING REGULATORY SCRUTINY</th>
<th>TOP 5 AREAS – DECREASING REGULATORY SCRUTINY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Sanctions</td>
</tr>
<tr>
<td>Anti-corruption</td>
<td>Compliance culture and accountability models</td>
</tr>
<tr>
<td>Compliance risk management program governance</td>
<td>Compliance risk appetite framework</td>
</tr>
<tr>
<td>AML</td>
<td>Executive compensation</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Third party risk management</td>
</tr>
</tbody>
</table>
Coordinating risk management

As mentioned above, following the global financial crisis, nearly all large financial services organizations added significant levels of risk and compliance resources to all three lines of defense. Many of these additions came during fire drills brought on by remediation of regulatory enforcement actions and often through reactive additions of testing capabilities to make sure that, going forward, someone was — or multiple people were — testing that same risk to make sure it didn’t happen again.

As firms start to put these regulatory actions in the rearview mirror, there is significant pressure to rationalize the number of resources deployed in these efforts and to make sure they are optimized in terms of which line of defense should perform them, when in the business process lifecycle they should be conducted, the extent to which they can be automated, etc.

However, our survey results strongly suggest that more work remains for most firms in this area. Overall, only one-fifth of all financial services organizations (20 percent) report their efforts to coordinate risk management activities across the three lines of defense are fully synchronized, with slightly more (22 percent) stating that efforts are underway but risk management activities are not yet effectively synchronized. A majority (58 percent) perceive these efforts to be moderately synchronized.

How would you characterize efforts within your organization to coordinate risk management activities across the three lines of defense?

- Efforts are synchronized fully: 20%
- Efforts are underway but not yet effectively synchronized: 22%
- Efforts are synchronized moderately: 58%
Large companies (with more than 25,000 employees) are significantly more likely to report that their efforts to coordinate risk management activities across three lines of defense are synchronized fully (43 percent). Banking, broker-dealer and consumer finance firms rated their efforts to coordinate the three lines of defense higher than other financial services organizations.

---

**Coordination of risk management activities across three lines of defense**

![Bar chart showing the percentage of efforts synchronized fully, underway but not yet effectively, synchronized moderately, and no efforts underway to coordinate across various industries.]

- **Banking**
  - Efforts synchronized fully: 31%
  - Efforts underway but not yet effectively synchronized: 51%
  - Efforts synchronized moderately: 18%

- **Insurance**
  - Efforts synchronized fully: 26%
  - Efforts underway but not yet effectively synchronized: 59%
  - Efforts synchronized moderately: 23%

- **Broker-Dealer**
  - Efforts synchronized fully: 54%
  - Efforts underway but not yet effectively synchronized: 25%
  - Efforts synchronized moderately: 18%

- **Asset Management**
  - Efforts synchronized fully: 63%
  - Efforts underway but not yet effectively synchronized: 31%
  - Efforts synchronized moderately: 6%

- **Consumer Finance**
  - Efforts synchronized fully: 59%
  - Efforts underway but not yet effectively synchronized: 23%
  - Efforts synchronized moderately: 21%

- **Payments**
  - Efforts synchronized fully: 79%
  - Efforts underway but not yet effectively synchronized: 7%
  - Efforts synchronized moderately: 14%

---
In our experience, there are several roadblocks to effective coordination across the three lines of defense. Among the most challenging of these — but also the most important to solve — are:

- Lack of a uniform taxonomy or data model for risk management information (e.g., what is considered a process, risk, control or issue; how are all of these items documented and at what level of granularity; and which data elements are mapped to one another?).

- Disparate systems used to house risk management data (e.g., operational risks maintained in one system while compliance obligations are stored in another or multiple sources of identified issues or risk events) that contain duplicative information and/or can’t be consolidated effectively.

- Different risk management priorities (and prioritization methodologies) across the three lines of defense and lines of business.

In particular, we have found that developing a uniform data model and converting existing data to the newly agreed-upon standard is a painful and time-consuming exercise, but ultimately a highly valuable one. The almost universal reaction from firms that have developed a uniform data model is, “I never want to do that again, and I wish we’d done it years ago.”

Attempting to standardize systems by, for example, moving to a GRC platform to be used by all three lines of defense without first rationalizing the data model is almost guaranteed to fail altogether, at worst, or not deliver most of the anticipated benefits, at best. And even if a firm chooses not to consolidate risk management systems, a standardized data model at least makes it easier and more consistent to communicate across systems and makes centralized data warehouse approaches possible.

We are also seeing that many firms have created chief data officer-type positions, with the goal of centralizing and standardizing the management of business data in a fashion similar to what we describe above for risk management information. Risk and compliance organizations should absolutely play a significant advisory and stakeholder role in chief data officer initiatives and think creatively about how they can use the output of these efforts to optimize and increasingly automate risk management efforts.

One of the tenets of the Agile philosophy is that baking good risk management and compliance practices into the design of business processes and systemic workflows results not only in better compliance performance, but also in more consistent execution of business processes and a better customer experience. More accurate and easily accessible business data is one of the key building blocks necessary to achieve this objective.

The almost universal reaction from firms that have developed a uniform data model is, “I never want to do that again, and I wish we’d done it years ago.”
New business engagement

A majority of regional and industry responses describe the level of engagement of the compliance function with business strategy as moderate. We view this as the “seat at the table” model — compliance is made aware of the strategy and has the opportunity to weigh in but is not typically considered a critical input to or a driver of the strategy. Responses are slightly more divided for new business initiatives, with 46 percent of all respondents reporting a moderate seat-at-the-table level and slightly more (49 percent) saying there is a high level of engagement.

Compliance engagement with business strategy (by region)
These results are generally unsurprising and track well with earlier findings in this survey. As noted previously, North American and EMEA firms have faced higher levels of regulatory scrutiny over the past decade that have caused them to elevate the stature of the compliance function within their organization to prevent similar issues from reoccurring. As APAC regulators begin to pursue the same types of regulatory actions that their peers in other regions have, we would expect compliance functions in APAC financial services industry firms to be given a stronger voice within their organizations as well.

Also notable is the fact that a much larger percentage of respondents claimed a high level of engagement in specific new business initiatives (e.g., marketing campaigns or launch of a specific new product within an existing product line) than they did related to their firm’s business strategy as a whole (e.g., decisions to enter an entirely new line of business, merge with or acquire other firms, or expand the firm’s geographic footprint). We are not suggesting that the compliance tail should wag the business dog in the form of setting business strategy. However, we have seen critical compliance failures result from firms pursuing business strategies that materially increased
their compliance risk profile without effectively evaluating whether their existing compliance infrastructure was up to the task of mitigating those additional risks.

A common practical example of this dynamic occurs as a result of mergers and acquisitions. We’ve seen that the compliance costs of acquisitions are routinely underestimated and, in many cases, the compliance organization of the acquired firm is viewed as a redundant function that can be eliminated by transferring its responsibilities to the existing compliance resources of the acquirer. Although some level of consolidation efficiencies is typically and eventually possible following an acquisition, firms often fail to consider and effectively address the realities that:

- The process of digesting the acquisition creates significant one-time resource demands on compliance organizations that were typically at or near capacity to begin with.

- Even if the acquiring and acquired firms share similar business models, the additional volume caused by the acquisition nearly always creates some level of incremental and essentially permanent work for the acquiring firm (e.g., additional transaction volumes and/or process points that should be subject to monitoring and testing).

- Even if the organization feels the current level of compliance resources is adequate to manage the acquired risks, the existing compliance function might not have the appropriate degree of expertise to care for unique products offered by the acquired firm, understand geographic or licensing differences, or possess “tribal knowledge” associated with things like legacy systems that will continue to be used by the consolidated organization for some period of time after the deal closes.

For these types of reasons, it is important that compliance leaders are meaningfully engaged in the setting of their firm’s business strategy. Although the strategy should ultimately be set by the C-suite, compliance should have the opportunity to ensure that inherent regulatory risks created by the proposed strategy are effectively considered by the firm’s leaders. Additionally, when the chief compliance officer has deeper insights as to the firm’s strategic direction, he or she is better equipped to ensure the strategic plan for the compliance function itself (e.g., investments in necessary infrastructure or mix of skill sets that are targeted within compliance’s human resources plan) is appropriate to help make the business strategy successful.
Resources and Costs

Compliance costs

Overall, almost half of financial services companies (45 percent) state that risk mitigation is important but also agree that there is increased emphasis on managing spending, while 32 percent of respondents say there is strong pressure to reduce compliance costs. Only 23 percent of respondents affirm a continued willingness to approve and/or fund whatever budget is necessary to address compliance risks. Spending patterns differ by region and at firms with different reporting structures. In North America, most respondents agree that although risk mitigation is important, there is pressure to manage spending. By comparison, a majority of respondents from the APAC region report strong pressure to reduce compliance costs. For companies where the head of compliance reports to the CEO, the results show a marked reduction in pressure to reduce compliance costs compared to firms where compliance reports to the chief risk officer (see the following charts).

• • • Appetite for compliance spend (by reporting relationship)

<table>
<thead>
<tr>
<th>Reporting Relationship</th>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
<th>60</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel/Chief Legal Officer</td>
<td>57%</td>
<td>29%</td>
<td>14%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>40%</td>
<td>38%</td>
<td>22%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Executive Officer</td>
<td>46%</td>
<td>26%</td>
<td>28%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td>50%</td>
<td>20%</td>
<td>30%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Risk mitigation is important, but there is increased emphasis on managing spend
- Strong pressure to reduce compliance costs
- Willing to approve/fund whatever budget is necessary to address compliance risks
**Appetite for compliance spend (by region)**

- North America:
  - Risk mitigation is important: 50%
  - Strong pressure to reduce compliance costs: 23%
  - Willing to approve/fund whatever budget is necessary: 27%

- Europe/Middle East/Africa:
  - Risk mitigation is important: 32%
  - Strong pressure to reduce compliance costs: 40%
  - Willing to approve/fund whatever budget is necessary: 28%

- Asia-Pacific:
  - Risk mitigation is important: 36%
  - Strong pressure to reduce compliance costs: 46%
  - Willing to approve/fund whatever budget is necessary: 18%

**Compliance personnel**

- **Full-time employees (or equivalent) in compliance function (by region)**

- North America: 2,275
- Europe/Middle East/Africa: 1,950
- Asia-Pacific: 1,800
The comparison of headcount trends by region is reflective of the broader trends noted in this survey and that we’ve observed in the market. Generally, regulatory pressure ramped up earliest and most significantly in the United States following the financial crisis, and so U.S. firms have had a longer period of time over which to increase their compliance headcounts. In the years ahead, we would expect staffing levels in the United States to moderate or decrease, in the EMEA region to grow modestly or stabilize, and in the APAC region to start to catch up with the rest of the world.

### Full-time employees (or equivalent) in compliance function (by organization revenue)

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10 billion or more</td>
<td>2,300</td>
</tr>
<tr>
<td>$5 billion to $9.9 billion</td>
<td>1,360</td>
</tr>
</tbody>
</table>

### Full-time employees (or equivalent) in compliance function (by industry)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>2,500</td>
</tr>
<tr>
<td>Insurance</td>
<td>1,815</td>
</tr>
<tr>
<td>Broker-Dealer</td>
<td>2,000</td>
</tr>
<tr>
<td>Asset Management</td>
<td>2,250</td>
</tr>
<tr>
<td>Consumer Finance</td>
<td>2,000</td>
</tr>
<tr>
<td>Payments</td>
<td>1,875</td>
</tr>
</tbody>
</table>
**Reporting lines**

For most firms, the compliance function has reported historically either to the legal function in the form of the general counsel, through the risk organization (i.e., chief risk officer), or less frequently, to a business leader such as the CEO or chief operating officer. Over the past decade, we have seen many firms in which compliance reported to either the general counsel or a business leader reconsider this model and make compliance part of the risk organization.

The survey results confirmed this trend is well under-way. In all regions and most industry segments, the head of compliance is most likely to report to the chief risk officer (CRO).³

Although there is no single best answer applicable to all financial services firms, our experience has been that having compliance report through the risk organization, rather than the legal department or a business leader, typically leads to the best results, because:

- The risk and compliance lifecycles (e.g., risk identification, prioritization, control, monitoring and remediation) are more similar to one another than the other potential combinations are. This makes it more practical for risk and compliance to establish shared standards, which is more efficient and cost-effective and limits the impact of duplicative risk and compliance activities on the business.

- Similarly, pairing risk and compliance creates critical mass to justify investments in infrastructure such as a GRC platform or advanced data analytics capabilities, which might be harder to win approval for — and would be far less efficient to support on an ongoing basis — if they were proposed separately by each function.

- A decade’s worth of painful and costly regulatory remediation exercises has caused a shift in strategy across the industry where compliance is primarily viewed no longer as a legal risk to be avoided, but rather as an operational one to be measured, controlled, and subject to regular monitoring and oversight. For example, the old lawyers’ adage says, “Never ask a question to which you do not know (or may not like) the answer.” Such a mindset, if taken to its extreme, can lead to a reluctance to proactively address signs of emerging risks. Although the risk of litigation is an important consideration in the design and execution of compliance monitoring and compliance issue management programs, it cannot be the only consideration. In some cases, we have found that having these types of functions report through the legal department negatively impacts their depth and quality of coverage, as well as speed to identification and resolution, due to concerns about discoverability.

³ The only exception is broker-dealers, where the head of compliance is more likely to report to the chief executive officer (CEO). Due to the unique regulatory regime applicable to broker-dealers, and more prescriptive requirements around the role of the compliance function specifically in these organizations, the fact that compliance has a higher profile in broker-dealers than in other industry segments is not surprising. In many cases, the head of compliance for a broker-dealer is also the general counsel, which helps explain the ultimate reporting line to the CEO.
At the same time, many firms in which compliance historically reported to a business leader have encountered challenges such as:

- **Focus and expertise:** Quite naturally, many business leaders who came up through the operational, sales or financial ranks are more comfortable dealing with those matters than compliance ones, and often view the former as more important and deserving of their time and attention, at least until a major compliance issue occurs.

- **Lack of independence:** As regulatory standards and enforcement activities related to compliance governance processes have ramped up, it is more important than ever that compliance plays an effective credible challenge role. In order to do this well, compliance needs to be comfortable answering not only the question, “Can we?” (i.e., is what we are proposing to do permitted by law or regulation?), but also, “Should we?” (e.g., is this a good product that will add value to and be understood by our customers, and do we have the right processes and systems in place to deliver this product in a consistent and sustainable manner?). When revenue-generating and compliance functions report to the same leader, it can be more difficult for compliance considerations to get a fair hearing and be effectively addressed.

- **Starvation of resources:** Along the same lines, investments in compliance are often more difficult for business leaders with revenue targets to justify, particularly in down cycles. A good practical example of this is the underinvestment in operations and compliance capabilities that occurred in loss mitigation and foreclosure units prior to and during the early stages of the global financial crisis. This ultimately played a major role in the “robo-signing” and other compliance failures that led to numerous consent orders, billions of dollars in regulatory penalties and substantial new regulations imposed on U.S. mortgage servicers.

Some firms have also experimented with dual reporting lines, in which compliance reports equally to two functions, or has a hard line to one and a dotted line to others. The following graphics show the use of these structures among our survey respondents:

```
Compliance operates in a dual or matrixed reporting structure
```

![Compliance Reporting Structure](image-url)
Compliance operates in a dual or matrixed reporting structure (by region)

- North America: 53% No, 47% Yes
- Europe/Middle East/Africa: 56% No, 44% Yes
- Asia-Pacific: 48% No, 52% Yes

Compliance operates in a dual or matrixed reporting structure (by industry)

- Banking: 51% No, 49% Yes
- Insurance: 53% No, 47% Yes
- Broker-Dealer: 54% No, 46% Yes
- Asset Management: 55% No, 45% Yes
- Consumer Finance: 50% No, 50% Yes
- Payments: 71% No, 29% Yes
To which of the following executives/leaders does the head of compliance report in a “dotted-line” relationship? (Multiple responses permitted)
Although dual reporting lines are well-intentioned in attempts to mitigate the inherent trade-offs associated with the models described above, our experience is that they rarely work well in practice. Many firms struggle to articulate effectively exactly what the dual reporting structure means in reality (i.e., for what topics is the dotted reporting line accountable instead of the hard line, how are disagreements or conflicts of interest between the two lines to be navigated, etc.?). Over time, the dotted reporting line often evolves into little more than a recipient to be copied on key reports, accountable if something goes wrong but without a lot of practical responsibility to prevent that from happening.

Organizations often find it more effective to identify the specific aspects of the compliance program that seem like they should be subject to a dotted-line reporting structure, and address those instead through risk management committee governance membership structures and roles and responsibilities rather than via reporting lines.

To reiterate one final point: None of the above should be read to suggest that having compliance report to the legal department or elsewhere isn’t necessarily the right answer for a particular firm, but should rather point to the inherent pros and cons of alternative structures. Organizations should also consider their firm’s culture, as well as the strengths and weaknesses of and interpersonal dynamics among the leadership team members who would be considered as candidates to oversee compliance.
Measuring the value of compliance

Many organizations have historically measured the success of their compliance functions by the absence of issues (i.e., the function is effective if we’re not in hot water with the regulators) or using remediation metrics such as how quickly they are able to resolve issues once identified. However, with the trends noted above showing rapid increases in compliance headcount over the past several years, as well as increased scrutiny of compliance resource levels generally, compliance functions are facing pressure to demonstrate their value in new and deeper ways.

How value provided by the compliance function is measured (multiple responses permitted)

- Coverage and efficiency of compliance activities (e.g., what percentage of compliance risks are subject to monitoring and testing) - 66%
- Remediation (i.e., how quickly and effectively known issues were resolved) - 51%
- Responsiveness (e.g., time required for compliance to review marketing campaigns or new product proposals) - 43%
- Early detection (i.e., how long issues existed before they were detected; what percentage of issues were detected by the first, second or third line of defense vs. regulators) - 35%
- Prevention (i.e., the absence of regulatory issues) - 22%
- Coverage and efficiency of compliance activities (e.g., what percentage of compliance risks are subject to monitoring and testing) - 66%
- Remediation (i.e., how quickly and effectively known issues were resolved) - 51%
- Responsiveness (e.g., time required for compliance to review marketing campaigns or new product proposals) - 43%
- Early detection (i.e., how long issues existed before they were detected; what percentage of issues were detected by the first, second or third line of defense vs. regulators) - 35%
- Prevention (i.e., the absence of regulatory issues) - 22%

Some of the trends we have observed in this area and expect are likely to continue and/or accelerate are:

- Compliance will face increased pressure to demonstrate effectiveness and responsiveness in supporting business objectives, not just preventing issues. This is likely to include, for example, greater use of service level agreements for things like turn-around time on review of marketing materials.

- Compliance functions should also seek opportunities to demonstrate how they’ve gone beyond simply discharging their own responsibilities by better enabling business process owners to execute against compliance objectives. For example, many organizations are seeking to make better use of preapproved marketing terminology, automated workflows and decision trees that help ensure required content is included in marketing materials at the content.
development stage. These organizations are measuring the effectiveness of these activities, in part, based on the percentage of marketing materials that are approved by the compliance function and/or the legal department at first pass, rather than being returned to the marketing function for revisions. An increasing first-pass rate is a great indicator of:

- Business process owners taking effective ownership of their compliance responsibilities
- An effective and more efficient compliance oversight process
- The organization’s ability to get useful materials into its customers’ hands more quickly, while remaining confident that compliance needs have been addressed

Or, in summary, this success is exactly what organizations pursuing the Agile philosophy are trying to achieve.

- Compliance organizations will increasingly need to demonstrate how they’re maximizing the utilization of the resources that they have and, in many areas, will face pressure to do more (or at least the same) with fewer resources. A specific example of how this is being done can be seen in analyzing the coverage of compliance monitoring and testing activities. Leading organizations are able to:
  - Demonstrate an accurate, complete and up-to-date inventory of the requirements they are subject to globally.
  - Show how those requirements map to their business processes, with each regulatory requirement that is mapped to a business process representing a compliance assessment point.
  - Conduct inherent and residual risk assessments at the assessment point level.
  - Map all of their first- and second-line compliance monitoring and testing activities to their universe of assessment points.
  - Show their compliance monitoring and testing coverage by requirement type, inherent and residual risk level, business unit, etc.

Having done all of this, the organization can, relatively easily, build a series of very useful KPIs for compliance monitoring and testing coverage. For example, if the organization is subject to 10,000 compliance assessment points and has at least one monitoring and testing procedure in place against 6,000 of those assessment points in a given year, its current overall coverage ratio is 60 percent. If it has 10 full-time-equivalent (FTE) staff dedicated to compliance monitoring and testing, on average, the assessment point coverage ratio per FTE is 600 (6,000 assessment points tested divided by 10 monitoring and testing resources).

Those metrics provide the baseline to sustain or increase the overall coverage ratio over time while continuously increasing the coverage ratio per FTE. The firm can do this, for example, by eliminating unnecessary duplicative testing activities (keeping the coverage ratio the same while reducing the number of FTEs dedicated to those activities), restructuring the design of certain testing procedures to cover more assessment points within a single test, etc. In that way, the organization can demonstrate to regulators that it is preserving the completeness and effectiveness of its monitoring and testing program and demonstrate to leadership and shareholders a focus on efficiency.

- Finally, compliance organizations will increasingly be challenged to show that their work adds value by improving business processes and/or leads to better customer experiences, beyond simply preventing
compliance risks. Many organizations, for example, struggle with time-consuming and burdensome processes to refresh know-your-customer (KYC) data on existing clients on a periodic basis for anti-money laundering compliance purposes. This often requires client-facing personnel to contact customers directly to obtain the necessary information. These processes are disruptive to business activities, disliked by customers who feel they intrude on their privacy, and difficult to execute consistently and accurately due to their manual and distributed nature. As a result, leading organizations are seeking ways to automate and make KYC refresh processes more continuous and seamless using transaction histories, consumer report information or other third-party data sources.

Other firms are seeking creative ways to integrate KYC refresh processes into client satisfaction surveys and/or client relationship management activities, limiting duplicative points of contact with the client and using an activity performed primarily for compliance purposes to help the organization understand how to better serve its customers.

Technology and Data Enablement

Use of data analytics

While 75 percent of respondents report that their compliance departments are using data and analytics, only 6 percent consider their data and analytics compliance capability to be close to fully adopted and integrated. Moreover, just over one in four (27 percent) of those using analytics rates their firm's use of these capabilities at a high level of maturity.

Banking firms' compliance functions are more advanced than those of other industries, with half rating their function in the top tier for usage of data analytics.

Geographically, the trends noted earlier in this survey continue here. North American firms have invested more heavily in compliance data analytics due to having faced a higher degree of regulatory scrutiny for a longer period of time.
• • • Use of data analytics (by region)

- North America: 81%
- EMEA: 76%
- APAC: 56%

• • • Use of data analytics (by industry)

- Banking: 76%
- Insurance: 72%
- Broker-Dealer: 87%
- Asset Management: 65%
- Consumer Finance: 83%
- Payments: 79%
Over the past few years, many organizations have recognized that some of the enhanced compliance controls they have added since the financial crisis have been built in firefighting mode and bolted on to existing business processes as quickly as possible, often in the form of back-end, manual transaction testing. The effect of this has been duplication, inefficiencies that slow down business processes and a compliance “solution” that often entails issuing refunds to consumers after errors have occurred rather than preventing them in the first place. These firms are realizing that this model isn’t sustainable and are working to more effectively embed compliance controls into the design of business processes and supporting workflow systems.

- Effort to automate/integrate compliance controls in business systems (by region)

![Bar chart showing the percentage of organizations by region and their efforts to automate/integrate compliance controls.](chart)

- 36% in North America
- 52% in Europe/Middle East/Africa
- 3% in Asia-Pacific

Legend:
- Orange: Controls are integrated but we are still refining them
- Blue: Efforts underway but not yet implemented or optimized
- Green: Minimal integration – we are just starting the journey
- Brown: Optimized and automated compliance controls are a critical and consistent part of system and process design
Financial institutions are eagerly adopting a subset of fintech known as regulatory technology, or regtech. Regtech refers to automating or digitizing manual regulatory compliance processes to add speed, security, accuracy and agility. Part of a broader trend toward digital transformation in financial services, regtech typically refers to the application of existing technology for regulatory compliance purposes, not the technology itself.

The appeal of regtech is obvious from, and consistent with, the results presented in the rest of our survey. It represents an opportunity to make compliance processes more effective while at the same time drastically more efficient, freeing up personnel for other, more value-added tasks, and it saves money in the long run. Consequently, the forms of regtech that are most quickly gaining traction in the marketplace are those directed at compliance functions that have seen the largest increase in headcount over the past decade, and are staffed by large teams of people performing high-volume and generally repeatable functions. Two particular examples of these areas include anti-money laundering (especially transaction monitoring for suspicious activity and customer due diligence and risk rating processes) and compliance transaction testing functions.

In our experience, the particular regtech solutions that are being adopted most quickly and are demonstrating the most value in the short term include the following.

**Robotic process automation (RPA)** is defined as the use of software to work alongside human operators to perform high-volume repetitive tasks. It is most commonly encountered in the automated menus most large companies use to route incoming calls, or schedule an automatic callback at times of high call volume. Increasingly, financial institutions are using RPA to perform compliance tasks, specifically in AML transaction monitoring, OFAC screening and KYC activities.

In particular, the application of RPA techniques to the process of gathering information from disparate third-party search utilities and other sources necessary to build an AML transaction monitoring case file or perform customer risk rating has yielded outstanding results. These capabilities can reduce several hours of manual work to a matter of minutes, increase the accuracy and consistency of case files, and free up time for more seasoned reviewers to focus on analysis and decisioning rather than data gathering. More information about this type of capability can be found at www.protiviti.com/regtech.

**Automated risk reporting and visual analytics** are another form of technology gaining widespread adoption. Dashboards and other graphic representations of real-time data with drilldown capabilities and cross-tabulation provide at-a-glance insights that were functionally impossible to achieve previously with manual-based reporting. Many firms are coupling the development of these types of capabilities with investments in RPA for risk reporting to build automated linkages between source data systems and reporting platforms. These combined capabilities dramatically increase the accuracy of reports, speed to users, and ability to create tailored views for various stakeholders. Examples of these capabilities can be found at www.protiviti.com/riskindex.

**Artificial intelligence** and the application of machine learning (AI/ML) to compliance processes is also generating great interest in the marketplace and is being adopted at an increasingly rapid rate, although the effectiveness and reliability of these capabilities are generally not yet as consistent as more basic RPA and automated risk reporting techniques. As AI/ML continue to mature and the data supporting these capabilities becomes richer, they hold the promise of not simply reducing the time required to perform manual processes, but eliminating them altogether. In the more immediate term, AI/ML capabilities are being applied to automate repeatable testing activities and make existing AML processes, such as transaction monitoring software tuning, more efficient.
We are confident that the next 10 years will see more change and innovation within compliance functions than has occurred in the entire history of the profession up to this point.
Barriers to technology

Even as firms see huge opportunities to use technology more effectively to meet compliance objectives, many struggle to execute effectively on or realize the benefits of this strategy.

Barriers to effective use of technology for compliance risk management purposes (shown: percentage of critical/significant barrier response)

The three top barriers to the effective use of technology in compliance risk management are inadequate business case based on uncertain return on investment (55 percent), lack of budget (54 percent) and data integrity (51 percent). Forty-seven percent of respondents said that the company’s focus on remediation and firefighting is a barrier to entry because it limits time to reengineer systems.

In comparison, only 41 percent of respondents cite a lack of executive-level support for such investments. This suggests there is appetite all the way to the top of most organizations to pursue these capabilities, but there is a lack of confidence in the results of such investments and many firms face the need to mature their own IT and MIS infrastructure elements before buying in.
Conclusion

Financial institutions are entering a new environment where the influx of post-financial regulatory enforcement actions has finally slowed. Rather than continue to grow compliance functions, firms are seeking to drive efficiencies and coordinate compliance efforts, while leadership teams are cautiously shifting their focus to business innovation and growth. Mindful of the likelihood that examiners will swiftly criticize any perceived loss of focus on risk and compliance capabilities, firms are determined to remain compliant, but they recognize that many functions were built in crisis mode and so are not as efficient as they could be.

The increasingly innovative and sophisticated use of data and analytics by fintech companies is compelling traditional firms to develop similar capabilities within their risk and compliance functions. In addition, the rise of regtech has the potential to drastically cut compliance costs while actually enhancing effectiveness.

The results of our survey clearly support that risk and compliance functions across large financial services organizations have recognized the need to transform in pursuit of efficiency and agility. Our results also indicate that while most of these firms have started this journey and are making meaningful investments in transformation, relatively few consider this process to be complete or have thus far fully achieved their intended objectives. With that in mind, we close our report with a few specific, practical suggestions that we have seen can make key differences in whether Agile transformation efforts succeed or fail.

01

The transformation initiative should be captured within a documented strategic plan and timeline to ensure there is leadership visibility into and support of the objectives, approach, investments, and risks of the effort, as well as how the intended benefits will be realized and measured. For nearly all firms captured within our survey, a truly Agile model represents a drastic departure from the status quo, which requires time and substantial investment to achieve. Firms that view the pursuit of Agile objectives as a business-as-usual/continuous-improvement effort are unlikely to achieve the degree of meaningful and sustainable change required, and subsequently they risk falling behind competitors that make more dedicated investments and measure progress toward these objectives.

02

Establishing a common language, taxonomies and frameworks for foundational program components such as processes, risks, controls and issues is one of the first, most challenging and most critical elements of a successful transformation program. This effort usually requires a fair amount of compromise among the various stakeholders, each of whom is used to and comfortable looking at these topics the way they have in the past. But, if this does not occur, the organization will achieve many fewer efficiencies as a result of its Agile efforts than it otherwise might have.

03

Access to comprehensive business process information and customer transactional data represents perhaps the single biggest roadblock that could prevent the revolutionary potential of regtech capabilities from being realized in practice. Leading firms have started to establish dedicated tollgates in business process and system design activities (as well as change management activities for those same areas) to comprehensively and consistently evaluate what information a particular process or system workflow will generate that may be relevant to risk and compliance objectives. Process and system owners are then made accountable for ensuring this data is captured according to a common framework and taxonomy, supported by a consistent audit trail, subject to data integrity checks, and made available in real time to the necessary risk and compliance functions.
In summary, the financial services industry has entered an uncertain and challenging but ultimately exciting era of risk and compliance management. Most professionals should feel a sense of optimism and relief at the opportunity to shift from endless remediation exercises to optimizing their processes and driving business value within their firms. At the same time, numerous structural, data and system, and business process obstacles put these efforts at risk, while this all must be done in a regulatory environment that never remains static. We hope that the information shared in this report is helpful in describing where peer organizations stand on that same path and has highlighted practical and creative opportunities to face this future with more confidence.
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

UNITED STATES

Patrick Scott  
Executive Vice President  
+p1.312.476.6397  
patrick.scott@protiviti.com

Carol Beaumier  
Executive Vice President  
+1.212.603.8337  
carol.beaumier@protiviti.com

Cory Gunderson  
Executive Vice President  
+1.212.708.6313  
cory.gunderson@protiviti.com

Michael Brauneis  
Managing Director  
+1.312.476.6327  
michael.brauneis@protiviti.com

Matthew Moore  
Managing Director  
+1.704.972.9615  
matthew.moore@protiviti.com

Joanne Granata  
Managing Director  
+1.212.603.5405  
joanne.granata@protiviti.com

Adam Hamm  
Managing Director  
+1.312.476.6334  
adam.hamm@protiviti.com

Shelley Metz-Galloway  
Managing Director  
+1.571.382.7279  
s Shelley.metz.galloway@protiviti.com

Matthew Perconte  
Managing Director  
+1.212.479.0692  
matthew.perconte@protiviti.com

Steven Stachowicz  
Managing Director  
+1.312.931.8701  
Steven.stachowicz@protiviti.com

UNITED KINGDOM

Peter Richardson  
Managing Director  
+44.207.0247.527  
peter.richardson@protiviti.co.uk

Bernadine Reese  
Managing Director  
+44.207.0247.589  
bernadine.reese@protiviti.co.uk

ITALY

Luca Medizza  
Managing Director  
+39.02.6550.6301  
lucamedizza@protiviti.it

GERMANY

Nicolas Fandrey  
Director  
+49.69.963.768.154  
nicolas.fandrey@protiviti.de

HONG KONG

Suneet Gorawara  
Managing Director  
+852.2238.0486  
suneet.gorawara@protiviti.com

AUSTRALIA

Mark Burgess  
Managing Director  
+61.408.506.411  
mark.burgess@protiviti.com.au
### THE AMERICAS

**UNITED STATES**
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale

- Houston
- Kansas City
- Los Angeles
- Milwaukee
- Minneapolis
- New York
- Orlando
- Philadelphia
- Phoenix
- Pittsburgh
- Portland
- Richmond

- Sacramento
- Salt Lake City
- San Francisco
- San Jose
- Seattle
- Stamford
- St. Louis
- Tampa
- Washington, D.C.
- Winchester
- Woodbridge

**ARGENTINA**
- Buenos Aires

**BRAZIL**
- Rio de Janeiro
- Sao Paulo

**CANADA**
- Kitchener-Waterloo
- Toronto

**CHILE**
- Santiago

**COLOMBIA**
- Bogota

**COLOMBIA**
- Bogota

**EUROPE**

- **FRANCE**
  - Paris

- **GERMANY**
  - Frankfurt
  - Munich

- **ITALY**
  - Milan
  - Rome
  - Turin

- **NETHERLANDS**
  - Amsterdam

- **UNITED KINGDOM**
  - London

- **BAHRAIN**
  - Manama

- **KUWAIT**
  - Kuwait City

- **OMAN**
  - Muscat

- **QATAR**
  - Doha

- **SAUDI ARABIA**
  - Riyadh

- **UNITED ARAB EMIRATES**
  - Abu Dhabi
  - Dubai

### ASIA-PACIFIC

**CHINA**
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

**JAPAN**
- Osaka
- Tokyo

**SINGAPORE**
- Singapore

**INDIA**
- Bengaluru
- Hyderabad
- Kolkata
- Mumbai
- New Delhi

**AUSTRALIA**
- Brisbane
- Canberra
- Melbourne
- Sydney

*MEMBER FIRM*