KPMG
cutting through complexity

The Convergence Evolution

Global survey into the integration of governance, risk and compliance

kpmg.com

In cooperation with

Economist Intelligence Unit | The Economist

About this research

KPMG International engaged the Economist Intelligence Unit in June 2011 to conduct a global survey that would assess the extent to which companies are adopting a coordinated approach to their governance, risk and compliance (GRC) activities. The research explored the costs and challenges associated with GRC and benefits that companies can expect to gain from better alignment of their risk and compliance functions within an overall governance framework. It also tracks progress in GRC by comparing sentiment against a survey conducted by the Economist Intelligence Unit in 2010 – also on behalf of KPMG – that was published as *The Convergence Challenge*.

The Economist Intelligence Unit surveyed 177 respondents from a wide range of industries and regions. Approximately one third were based in North America, 28 percent in Western Europe, 24 percent in Asia, and the remainder in the Middle East, Africa, Eastern Europe and Latin America. More than one-half of respondents represented companies with annual revenues in excess of US$500m, and 50 percent were C-level or Board-level executives. All respondents had responsibility for, or influence over, strategic decisions on risk management.

To supplement the survey, the Economist Intelligence Unit conducted a series of in-depth interviews with senior executives and industry specialists from a number of major companies. We would like to thank all the participants for their valuable time and insight.

The findings expressed in this survey do not necessarily reflect the views of the sponsor.

Interviewees (arranged alphabetically by organization)

Paul Hopkin Technical Director, AIRMIC
Shane Hogan Director of Risk Management, Alliance Data
Simon Oxley Managing Director, Citicus
Nick Hirons Vice-President and Head of Audit and Assurance, GlaxoSmithKline
Cristina Tate Director of Enterprise Risk Management, HP
Evgueni Ivantsov Head of Portfolio Risk and Strategy, HSBC
Dr. John Lee Group Chief Risk Officer, Maybank
Norman Marks Vice-President of Governance, Risk and Compliance, SAP
Sam Harris Director of Enterprise Risk Management, Teradata

[1]In this report, governance, risk and compliance refer to the overall governance structures, policies, technology, infrastructure and assurance mechanisms that an organization has in place to manage its risk and compliance obligations.

Contents

Foreword

In our 2010 publication – The Convergence Challenge – we examined how large global companies dealt with the decision-making process within their organizations around governance, risk and compliance. What we discovered was that individuals took unnecessary risks that damaged their firms' business and reputation.

Fast forward, and we are now in a situation where many countries have recovered, or are trying to recover from the financial crisis, sovereign bailouts and an environment where businesses are under more regulatory scrutiny. Have we seen an evolution of governance, risk and compliance (GRC) management? That is a pivotal question for discussion in this research document.

During the financial crisis, organizations were fearful about their longevity and the ramifications of non-compliance with regulatory demands. This environment led to a surge in GRC activities that were costly and had an uncoordinated approach, which nay-sayers believe has led to inefficiencies and a lack of improved performance.

This report examines whether there has been an emergence of GRC at the Board level of big business and whether GRC has become an integrated group that permeates all departments and functional levels within an organization, putting risk at the top of the agenda, rather than as an afterthought.

Specialists throughout the globe have provided commentary to the key questions of inefficiency, performance improvement, strategy direction, perceived costs of GRC, and where we need to go from here.

John Farrell
Global Governance Risk & Compliance Leader

Executive summary

Companies are increasing their focus on governance, risk and compliance issues. The financial crisis has raised the profile of GRC. Before the crisis, 10 percent of respondents thought that their Boards took GRC extremely seriously. Today, this proportion has risen to about 40 percent. Executives are also sharpening their focus on GRC. Asked which stakeholders are exerting pressure on the organization to improve its convergence of GRC, respondents point to senior management as the main driving force.

Despite pressure for change, most companies remain at a fairly early stage of GRC convergence. Although many respondents recognize the benefits of improved convergence, only 49 percent label it a priority for their organization. Most are still at a fairly early stage of maturity in their convergence initiatives. Just 12 percent have fully integrated their GRC activities across oversight functions and 9 percent across business units. An important barrier for many is the perceived complexity of GRC convergence. Respondents also point to a lack of expertise or resources to make the necessary transition as a key challenge.

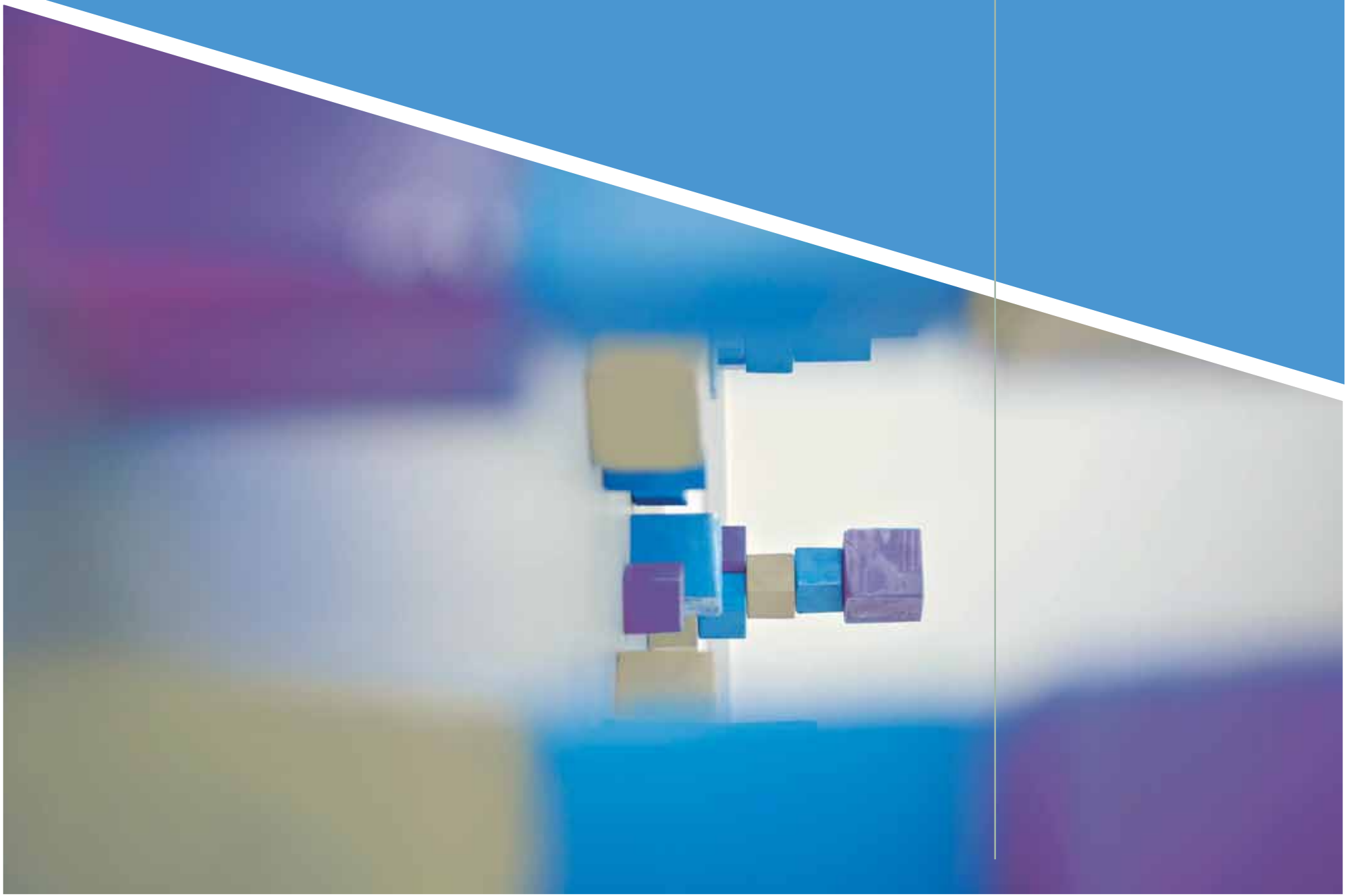
Poor coordination of governance, risk and compliance leads to inefficiency and a lack of consistency. Many organizations continue to have a fragmented and overlapping approach to their GRC obligations. More than one-half of respondents agree that it is difficult to know who has responsibility for specific functions, and it seems to be getting worse. The proportion of respondents who agree that it is difficult to know who is responsible is higher than in our 2010 research. Inefficiency is another common problem, with 41 percent rating themselves as effective at minimizing duplication of effort. This lack of coordination also leads to inconsistency and a lack of transparency. Only 38 percent of respondents say that their organization is effective at sharing information and resources across functions, and 34 percent are good at ensuring that their approach is consistent across borders.

Companies struggle to make the link between risk and compliance activities and overall corporate strategy. Despite the rising profile of risk in many organizations, only a minority of companies involve risk teams in key strategic decisions. Just 45 percent of respondents say that the risk function plays a formal role in providing analysis to support corporate strategy, and only 40 percent are involved in performance management. Weak links between GRC and overall corporate performance are likely to hamper the effectiveness of these activities for many organizations.

Many companies struggle to ensure the free flow of risk information and awareness across the business. A lack of coordination among GRC activities means that many companies find it difficult to build risk awareness across the organization and to ensure that the Board receives accurate, up-to-date risk information. A slim majority (52 percent) of respondents say that their company is effective at ensuring Board-level awareness of key risk and compliance issues, and only 46 percent are effective at instilling an awareness of those issues across the organization.

The cost of GRC activities is increasing for the vast majority of companies. One-third of respondents report that the annual cost of their GRC activities consumes more than 6 percent of their annual revenues. The vast majority have seen an increase in this expense over the past two years, and expect it to increase even further in the next two years. And the proportion that thinks the cost is increasing is higher than in the 2010 KPMG report, The Convergence Challenge. Yet understanding the true cost of risk and compliance appears to be challenging, with one-third claiming to be effective at measuring the cost of these activities. This suggests that the real cost may be much higher than is currently estimated.

The perception that GRC is already consuming a large proportion of revenues may be deterring companies from investing to improve coordination of these activities. Despite admitting significant weaknesses in their current approach, many companies struggle to build a business case for improving the co-ordination between their GRC activities. Almost two-thirds of respondents consider GRC convergence as a cost, rather than an investment (a higher proportion than last year), and only 31 percent say they are effective at quantifying the benefits of these activities.



01 Drivers of change

As the past few years have so dramatically shown, no business is immune to crisis. In the financial services industry, business empires built up over decades have been severely compromised and even destroyed, seemingly overnight. Likewise, the oil and gas sector and the media have suffered high-profile disasters that have caused significant financial and reputational damage.

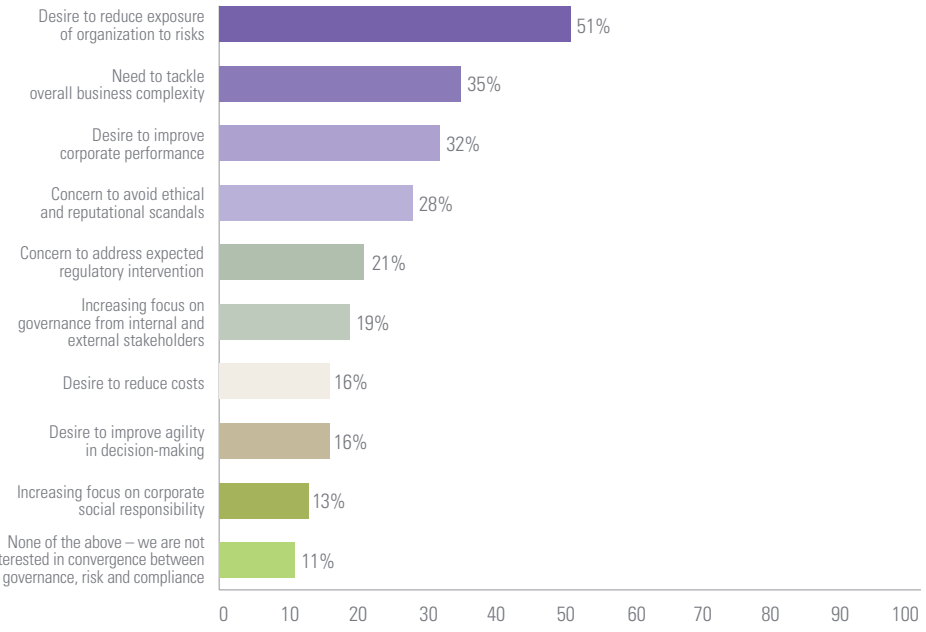
The threats and risks that can devastate companies are many and varied. But despite the diversity of potential hazards, there is often a consistent thread running through most major business crises. Boards and senior management lack visibility into business operations, and there is insufficient rigor in the way in which risks are identified, prioritized and acted upon across the organization.

High-profile disasters are undoubtedly a catalyst for companies to pay closer attention to their GRC activities. Indeed, when asked about the factors that exerted the greatest influence over their organization's interest in GRC, survey respondents pointed to their desire to reduce risk exposure as the leading driver (see chart 1).

But a widening risk exposure is far from the only driver of change. Respondents cite increased business complexity as the second most influential factor (see chart 1). As companies enter new markets and construct increasingly complex supply chains, they are exposed to new and unfamiliar threats. Managing these risks requires a clear line of sight across the entire value chain in order to give senior management the confidence that a consistent and rigorous approach is being taken.

By improving their visibility of risk across the value chain and enabling timelier, more risk-conscious decisions, companies stand to benefit from improved corporate performance. **"Your GRC controls are like the brakes on a car,"** says Nick Hirons, Vice-President and Head of Audit and Assurance at GlaxoSmithKline, the UK's largest pharmaceutical company. **"The better the quality of the controls, the more effective the brakes. And the more effective the brakes, the faster the business can go."**

Chart 1: Which of the following factors play the strongest role in influencing your organization's interest in converging its governance, risk and compliance?



Source: Economist Intelligence Unit, June 2011

An ever-increasing compliance burden also creates pressure for change. In response to the financial crisis, governments and regulators are becoming more intrusive and prescriptive in their approach to rules and legislation. While most evident in the financial services industry, other sectors are also feeling the impact of this more stringent environment. Corporate governance legislation, for example, is being strengthened in a number of jurisdictions as governments seek to place business under a tighter rein. In the UK, for example, the Bribery Act has strengthened legislation governing corrupt business practices.

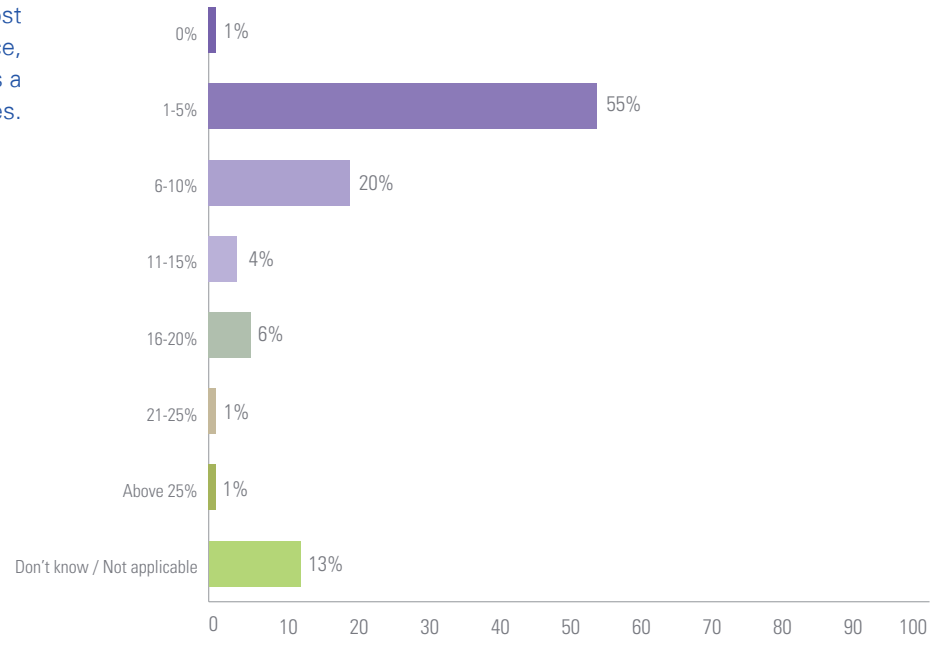
Simon Oxley, Managing Director of Citicus, a risk and compliance software developer, worries that this focus on regulation, while important, comes at the expense of broader, day-to-day risk activities. "What compliance initiatives tend to do is force companies to prioritize regulatory risk rather than looking at risk management as a whole," he says.

Time to catch up

The rate at which risk and compliance obligations are expanding means that many companies find it difficult to keep pace. Over the years, they have responded to a new regulatory requirement by bolting on an extra process or function. This ad hoc approach may address the immediate issue, but it inevitably leads to overlapping responsibilities, inconsistent processes and duplication of effort.

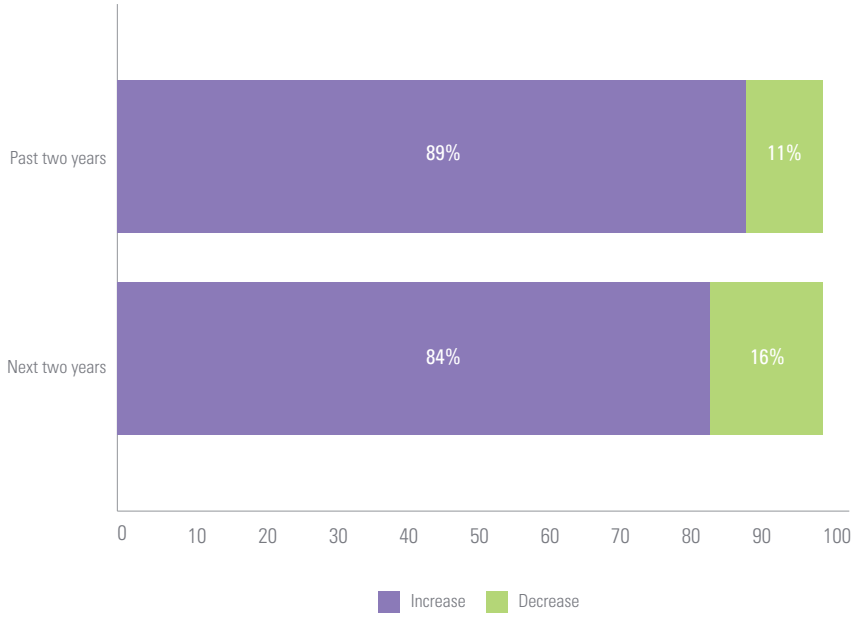
It also leads to ballooning costs. Among our survey respondents, almost one-third say that they spend more than 6 percent of their organization's annual revenues on GRC activities (see chart 2). There is also near-universal agreement that the cost of these activities is on the rise. Over the past two years, 89 percent say that the cost has increased, and 84 percent expect it to grow further in the next two years (see chart 3).

Chart 2: Please estimate the annual cost of your organization's overall governance, risk and compliance activities, as a percentage of annual revenues.



Source: Economist Intelligence Unit, June 2011

Chart 3: What change has there been to the cost of your governance, risk and compliance efforts over the past two years, and what change do you expect over the next two years?



Source: Economist Intelligence Unit, June 2011

For any moderate-sized bank, you're probably looking at hundreds of man years of effort to comply with Basel III, but that cost is spread among large numbers of departments and employees…

In reality, however, it can be very difficult for companies to know how much they spend on this diverse – and frequently fragmented – set of responsibilities. **"This is a classic example of something that's difficult to measure, just because of the way it's spread out across the business,"** says Sam Harris, Director of Enterprise Risk Management at Teradata, an analytics specialist. **"GRC involves different business units, it involves different systems, so it's very difficult to do activity-based costing and identify all of the costs that are associated with a GRC effort."**

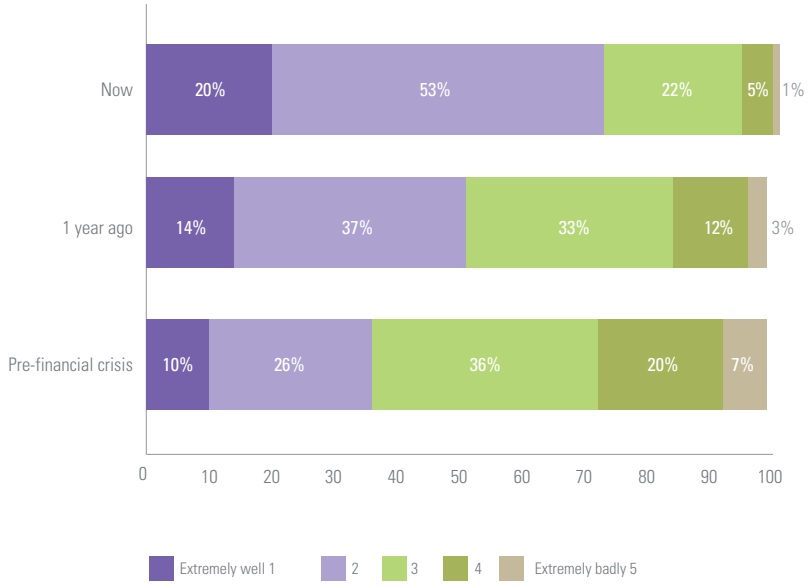
Surveys conducted over the past two years on behalf of KPMG suggest that the cost of GRC is increasing. In our 2010 report, 80 percent of respondents said that the cost of their GRC efforts had increased over the previous two years. In our most recent survey, 89 percent said that the cost had increased.

Coming up with an accurate total figure may be difficult, but it is certain to be high, especially in sectors with a heavy compliance burden. In financial services, for example, banks will incur eye-watering costs to comply with new regulations such as Basel III.

"For any moderate-sized bank, you're probably looking at hundreds of man years of effort to comply with Basel III, but that cost is spread among large numbers of departments and employees," explains Mr. Harris. **"You also have to consider the opportunity costs. If some of those employees are also engaged in a client-facing role, then you have to take into consideration the fact that their regulatory responsibilities mean that they will not be available to form revenue-creating opportunities."**

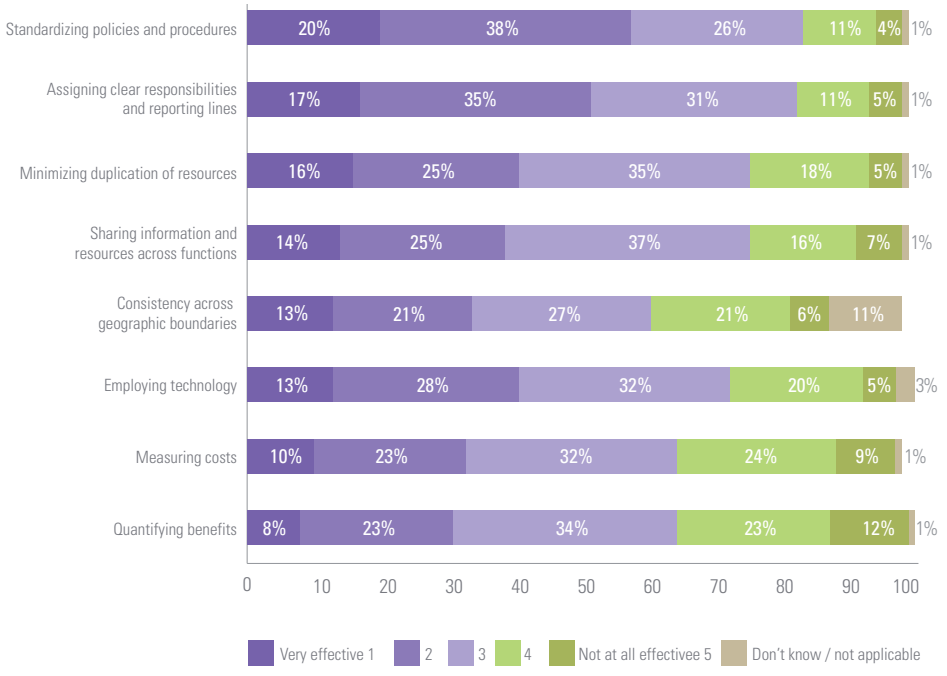
A large proportion of the senior executives questioned for our survey admit that their existing risk and compliance processes leave a lot to be desired. More than one-half agree that their current approach makes it difficult to know who has ultimate responsibility for particular functions (see chart 4). Many also struggle with embedding consistency and efficiency across organizational and geographical boundaries. For example, only 39 percent think that their company is effective at sharing information and resources across functions, while 41 percent are effective at minimizing duplication of effort (see chart 5).

Chart 4: On a scale of 1 to 5, how well does your company manage risk issues?



Source: Economist Intelligence Unit, June 2011

Chart 5: How would you rate the effectiveness of your organization at managing the following aspects of governance, risk and compliance?



Source: Economist Intelligence Unit, June 2011

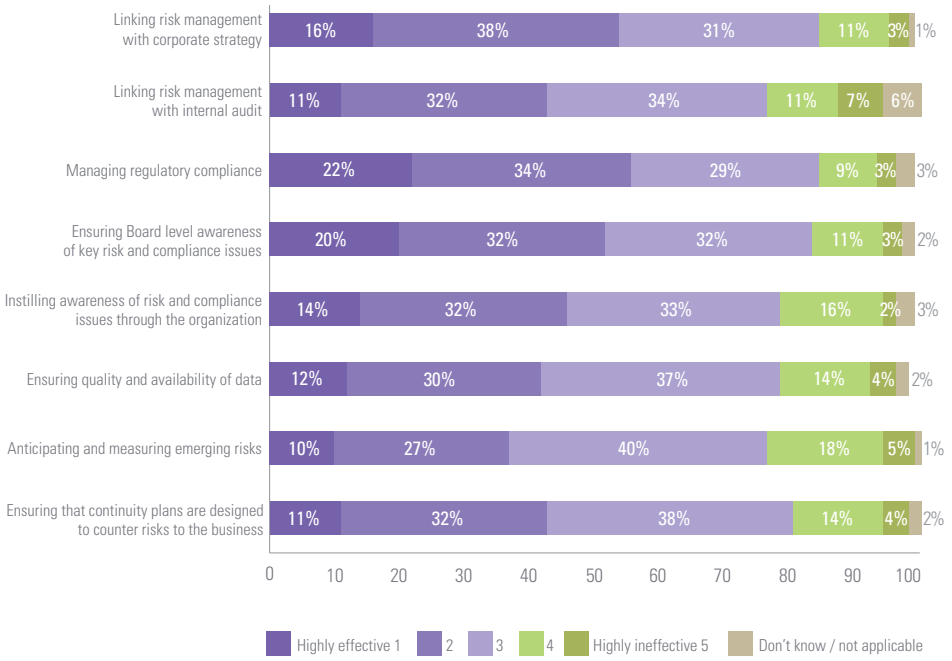
02 The link with strategy

Minimizing overlap and improving the flow and consistency of communication within the organization has become a key objective for many companies. GRC convergence is a priority for just under one-half of respondents.

"If you can identify areas of overlap between different regulatory regimes, that creates an opportunity to drive out cost by putting in place a common infrastructure and common resources in terms of personnel," says Mr. Harris of Teradata. **"By taking a more integrated approach, companies can also ensure that they don't inadvertently generate inconsistencies and errors in their compliance."**

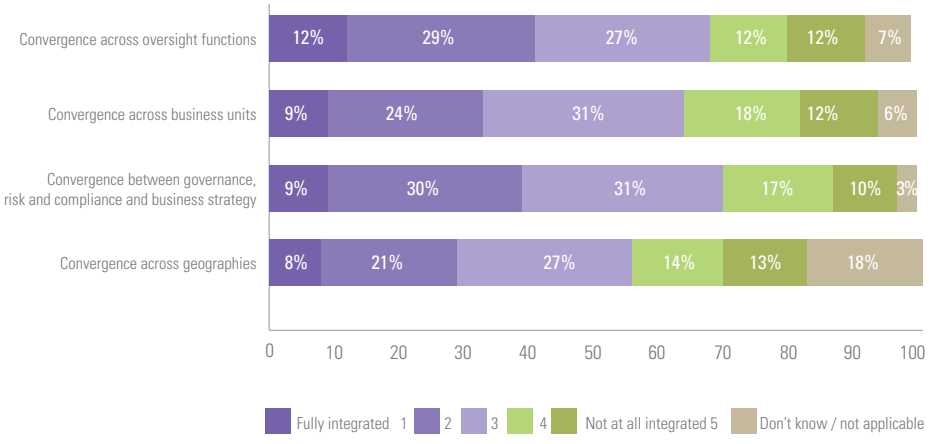
But addressing fragmentation across risk and compliance activities is just one piece of the puzzle. To be effective, GRC convergence has to link risk and compliance with the overall strategic decision-making and performance of the organization. This is another area where many companies continue to face difficulties. A slim majority of 54 percent are effective at linking risk management with corporate strategy (see chart 6), and only 9 percent have fully integrated their GRC activities with business strategy (see chart 7).

Chart 6: How would you rate the effectiveness of your organization at the following activities?



Source: Economist Intelligence Unit, June 2011

Chart 7: How would you rate the degree of convergence between governance, risk and compliance across the following entities in your organization?



Source: Economist Intelligence Unit, June 2011

Convergence of GRC helps to strengthen the link with strategy. Among those respondents who say they have fully integrated their GRC activities across oversight functions, 85 percent are effective at linking risk management with strategy, which is considerably higher than the proportion among the overall group.

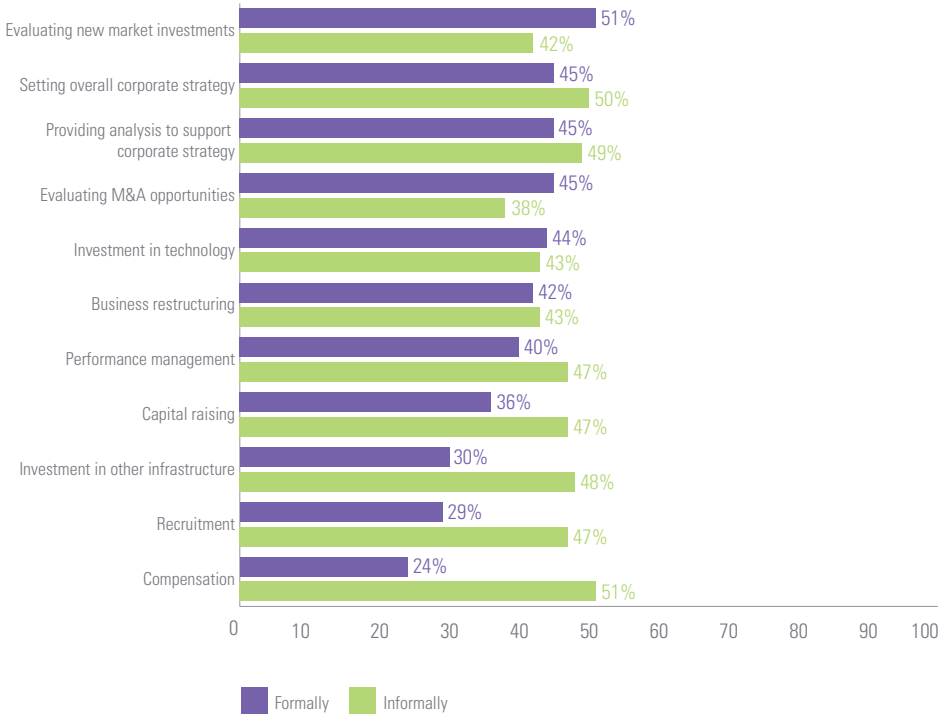
Outdated perceptions of risk departments as support functions can be a barrier to making the link with strategy more explicit. **"Risk departments need to be transformed from the function that says 'no' to the department of 'how',"** says Norman Marks, Vice-President of Governance, Risk and Compliance at SAP. **"The companies that derive the maximum value from GRC are those that not only eliminate fragmented risk and compliance but also integrate the consideration of risk into how they run the business."**

The link between risk and compliance, and strategic decision-making remains relatively weak in many organizations. For example, only 40 percent involve their risk function in performance management, 44 percent when investing in technology and 45 percent when evaluating merger and acquisition (M&A) opportunities (see chart 8). Again, however, respondents who have fully integrated their GRC across oversight functions are far more likely to involve risk functions in these activities.

By getting risk functions more involved in these activities, experts questioned for this report believe that better business decisions will follow. **"Risk is present whether you acknowledge it or not, but if you acknowledge it, then you can take advantage of the opportunities and make better decisions by understanding the whole picture,"** says Cristina Tate, Director of Enterprise Risk Management at HP.

> The notion that GRC needs to be a separate department within an organization is antiquated – GRC needs to be embedded across all functional areas of a business to be effective."
>
> **Oliver Engels**,
> KPMG's European Head of Governance, Risk & Compliance

Chart 8: In which of the following activities does your organization's risk function play a formal role?



Source: Economist Intelligence Unit, June 2011

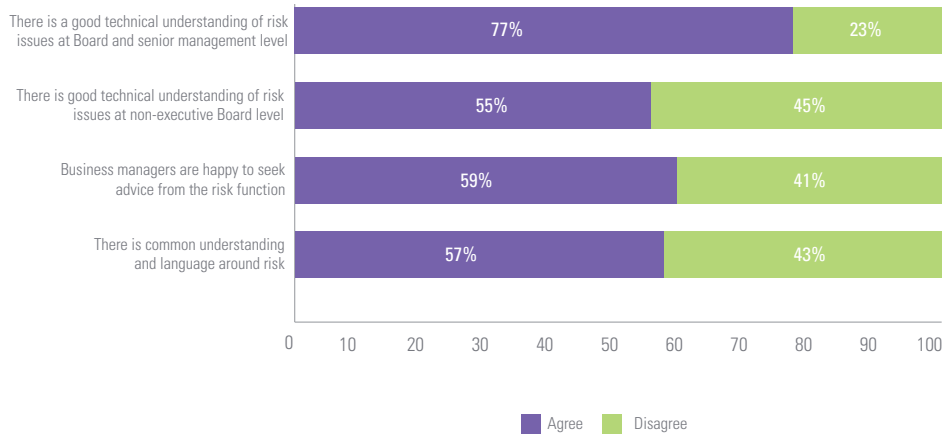
Even if risk executives are not actively participating in strategy formation, they would at least be expected to provide the analytical input to enable those decisions to be made from a position of risk awareness. Yet this does not always seem to be the case. Only 45 percent say that their risk function plays a formal role in providing analysis to support corporate strategy, although the proportion among financial services respondents is somewhat higher at 57 percent. **"If you talk to Chief Risk Officers and ask them how often they are invited to executive sessions when strategy is being discussed, you will find that a surprisingly low proportion is involved," says Mr. Marks.**

"But if risk management is not focused on where the company is going in terms of its strategy, and then optimizing the strategy as new risks emerge, it is spending time addressing the wrong things."

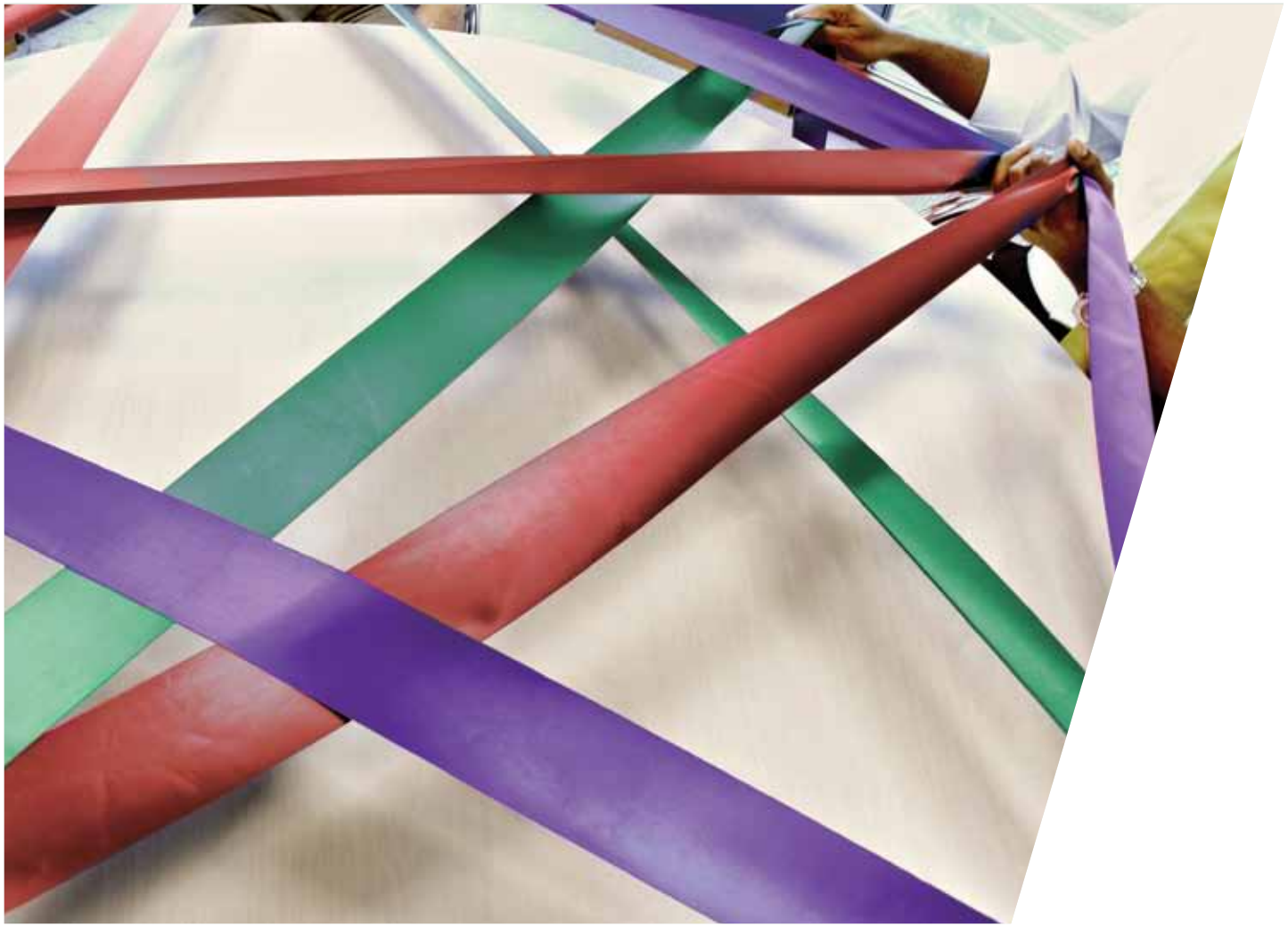
In addition to forging stronger links between risk and strategy, companies should ensure that there is a more proactive dialogue between risk managers and business units. Not all businesses have mastered this channel of communication. Around six out of ten respondents agree that their business managers are happy to seek advice from the risk function and a similar proportion say that there is a common understanding and language around risk (see chart 9). Among financial services respondents, these proportions are slightly higher.

By coordinating their GRC activities more carefully, risk functions can create a smoother relationship with the business units. **"A more integrated approach means that we can reduce the burden on the businesses so that multiple groups are not asking them about the same things,"** says Ms. Tate. **"It also makes us more effective because we're learning about risks from different angles. By sharing those perspectives, we're getting smarter in the way we deal with the risks that the business groups are facing."**

Chart 9: Please indicate whether you agree or disagree with the following statements, as applied to your organization.



Source: Economist Intelligence Unit, June 2011



CASE STUDY

A group-wide risk perspective on growth at Maybank

As banks in North America and Europe continue to recover from the shock of the financial crisis, they must look with some envy at their peers in fast-growing Asian markets. Most came through the crisis with only minor damage, and are fortunate in being based in some of the fastest-growing economies in the world.

Maybank, the Malaysian bank, is one financial institution that is reaping the rewards from this rapid growth. Already the largest bank in its domestic market, Maybank has ambitious plans for the future. It is expanding across South-East Asia, and has made several acquisitions in recent years as part of a strategy to become a regional powerhouse across a broad suite of financial activities.

But this rapid expansion also creates new risks. As it grows, Maybank must get to grips with new regulatory regimes and risk environments, and ensure that it embeds a risk culture among an expanding workforce. Rather than take a domestic perspective on risk, it must also understand the impact of regional and global events on its business, from the euro zone crisis to the potential risk of a slowing economy in China.

The need to obtain an integrated, overarching view of risk encouraged Maybank to create a new role of Group Chief Risk Officer. In April 2010, the Board appointed Dr. John Lee to the position. "*The Board and Senior Management felt that we needed a group perspective on risk across our different markets and my role is really about connecting the dots between risk activities and gaining an integrated view,*" says Dr. Lee.

In addition to providing this integrated view, Dr. Lee sees his role as being to partner with the business and add value to the institution. *"We need to move away from a compliance perspective to working with our business and ensuring that what we do from a risk management perspective adds value while still maintaining our independence,"* he says.

To facilitate this partnering process, Dr. Lee has developed what he calls a *"total banker"* concept, which aims to build bridges between risk and the business and ensure that there is mutual understanding between the two sides. A talent management program encourages risk professionals to gain direct experience of the business, and also gives business managers the opportunity to learn about risk. "*As they move up their career, business managers need to spend some time in risk to build awareness and embed a strong risk culture before they go back to the business to assume a more senior position,*" says Dr. Lee.

Maybank is adopting a similar approach with its risk management professionals. As the business moves into new markets, Dr. Lee is keen to ensure that best practice in risk spreads in tandem with this expansion. A knowledge management platform provides a means for risk professionals to share information, and the bank is also creating a talent competency framework to ensure that there is consistency in the way that risks teams are trained.

Dr. Lee hopes that this open approach to learning and career development will help to break down the silos that can easily build up between different risk competencies in financial services. *"We want to make our resources mobile so that we can deploy people from various centers where we have best practices and move them to other locations,"* he explains. *"The word I use is that we want to 'virtualize' our risk management, so that we are not constrained by physical location and everyone can talk and work with each other."*

03 Pressure from the top

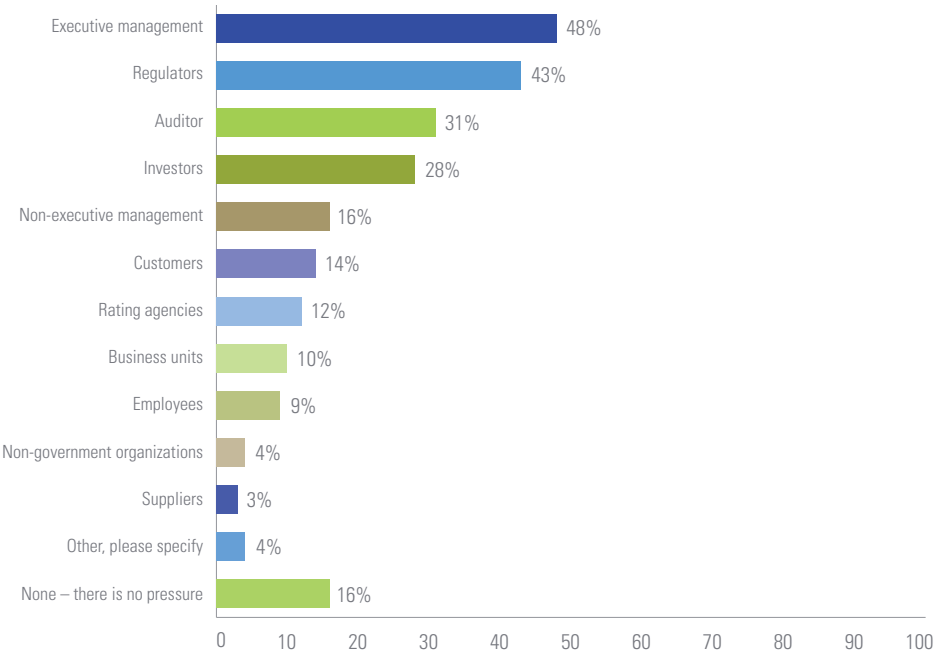
Despite a lack of alignment between risk and strategy, greater interest in governance, risk and compliance is undoubtedly of more interest than ever among the most senior individuals in organizations. According to respondents, executive management is the stakeholder that is exerting the most pressure on the business to improve its convergence of GRC functions (see chart 10).

Senior managers want assurances that risk and compliance activities are being run effectively and are looking for confidence that everything is being done to minimize the likelihood of key risks derailing the organization. **"Surprises are expensive, and a good GRC system helps to prevent them,"** says Teradata's Mr. Harris. **"You're always going to have unexpected events, but if you can minimize their impact and support what I call 'the principle of least astonishment,' then you will be in a stronger position overall as an organization."**

Investors and non-executive directors are also becoming much more interested in the concept of GRC. "**As shareholders and Board of Directors take on increasing governance accountability, they are demanding a more holistic approach to risk management through GRC,"** says Mr. Hirons of GlaxoSmithKline.

In the wake of the financial crisis, Boards were criticized for not performing their oversight role as thoroughly as they should. Although Boards in financial institutions were the main target for this criticism, non-executives in every sector have come under pressure to demonstrate that they are taking their role seriously and meeting the expectations of investors and other external stakeholders. **"Board oversight of the governance structure is a non executive director responsibility,"** says Paul Hopkin, technical director of AIRMIC. **"But if you look at recent corporate disasters, a common problem is that the non-executives were asleep at the wheel."**

Chart 10: Which of the following stakeholders are exerting pressure on your organization to improve its convergence of governance, risk and compliance functions?



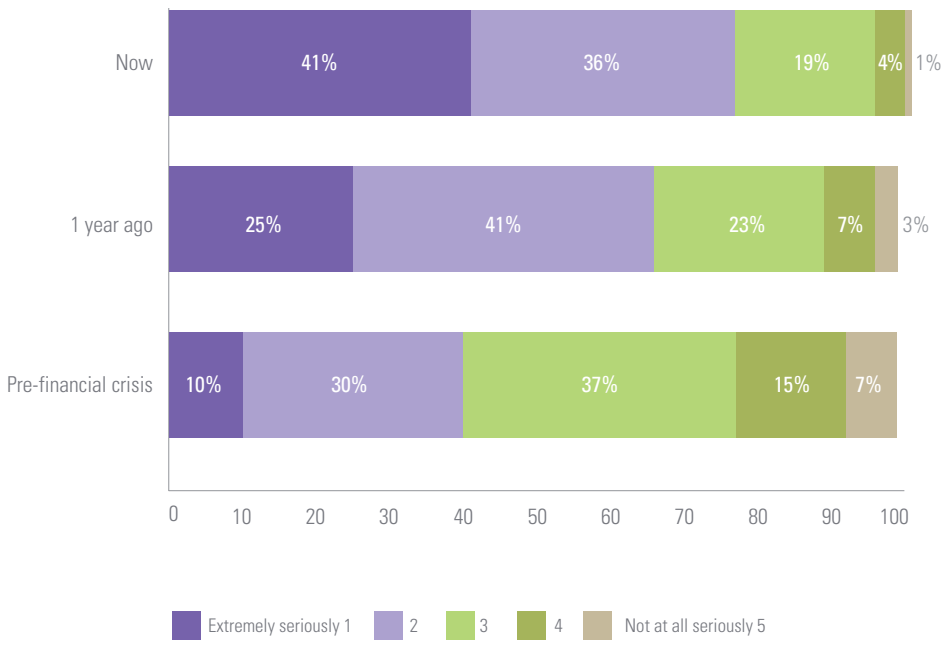
Source: Economist Intelligence Unit, June 2011

The difference between the level of interest in GRC among Board members pre-crisis and post-crisis is striking. In the run-up to the crisis, just 10 percent of respondents say that their Board members took the challenges of governance, risk and compliance extremely seriously. Today, that figure has risen to 41 percent (see chart 11). Among respondents from North America, it is 51 percent.

"One of the key outcomes from the financial crisis is that Board members have realized that they have greater responsibility to understand what's happening in the business," says Mr. Harris. **"As a result, they are demanding more information that is also of higher quality. That, in itself, has been a key driver for investment in GRC implementation."**

If executive management can demonstrate that a company has good GRC processes in place, then Boards and other external stakeholders can take this as a proxy for good overall management and performance. This leads to enhanced reputation and, in turn, superior financial performance. **"If you look at a company that has robust risk management practices, you'd infer that company is going to be able to reduce their volatility and be more stable, because they are making the effort to understand the risks and manage them appropriately,"** says Ms. Tate.

Chart 11: On a scale of 1 to 5, how seriously do you think the challenges of governance, risk and compliance are taken at Board level in your organization?



Source: Economist Intelligence Unit, June 2011

04 The current landscape

In 2006, the analyst firm AMR proposed a maturity cycle for GRC convergence consisting of four stages: reaction, anticipation, collaboration and orchestration.

Reaction stage

In the reaction stage, companies are taking an ad hoc approach to individual compliance or risk requirements. They may be compliant with a specific regulation, but there is no overall strategic approach to the company's obligations.

Anticipation stage

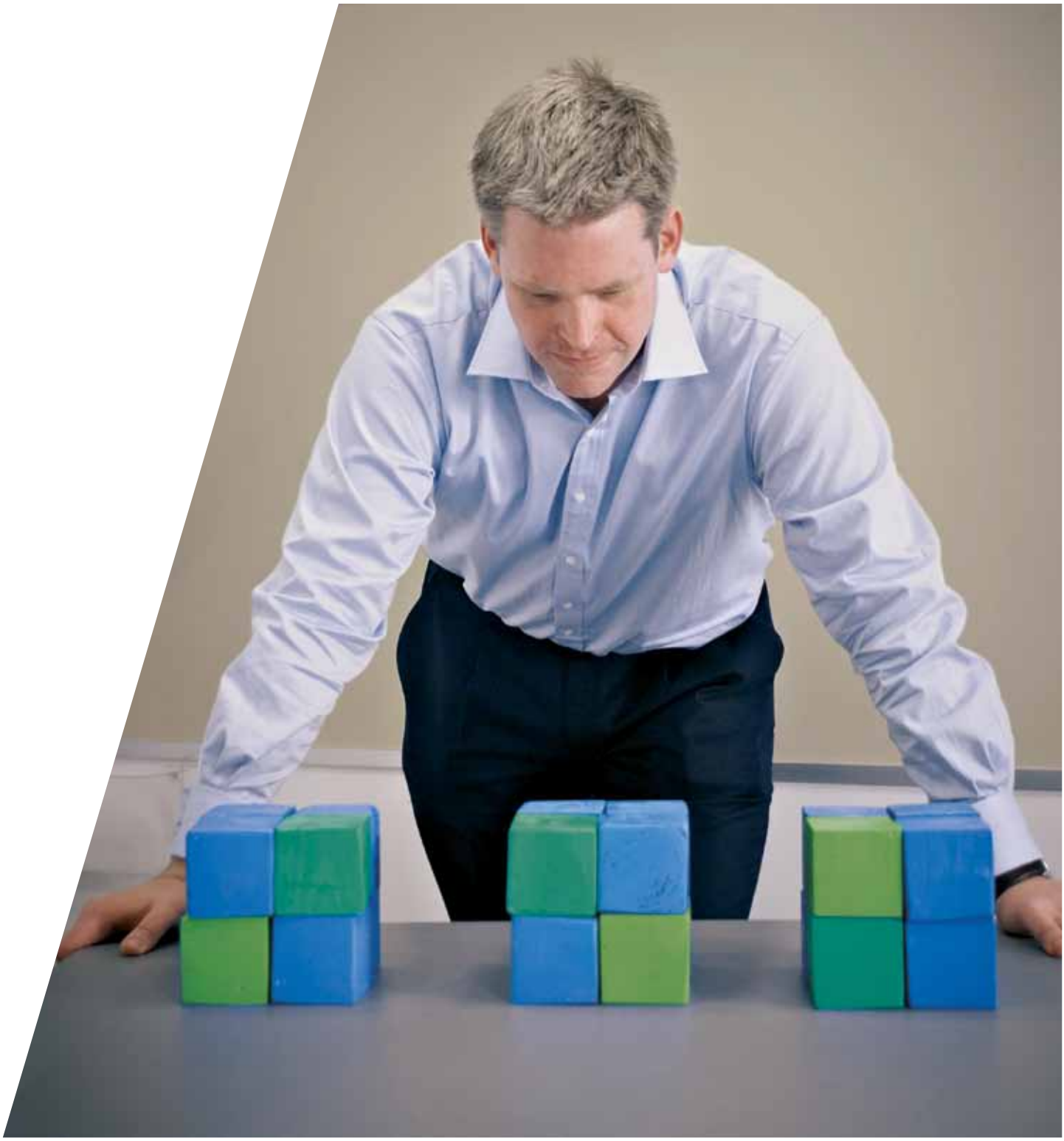
In the anticipation stage, companies are starting to look ahead to see what new obligations or risks they might need to address. They are also thinking about the way in which they should respond, which helps to increase efficiency.

Collaboration stage

By the collaboration stage, companies are starting to see the links between different risk and compliance activities, and taking a more holistic approach to meeting their obligations. They are prioritizing risks and looking at ways of standardizing their approach.

Orchestration stage

In the final orchestration stage, the company's risk and compliance activities are working in unison. They have adopted a consistent approach to dealing with obligations, set and monitor overall enterprise objectives, and have complete visibility across all risk and compliance activities.



Our survey suggests that most companies are still at a relatively early stage of the maturity cycle. Just 12 percent have achieved fully integrated convergence across oversight functions and only 9 percent have achieved full convergence of GRC across business units (see chart 7).

"In general, GRC adoption is still pretty immature in most industries," says Mr. Oxley.

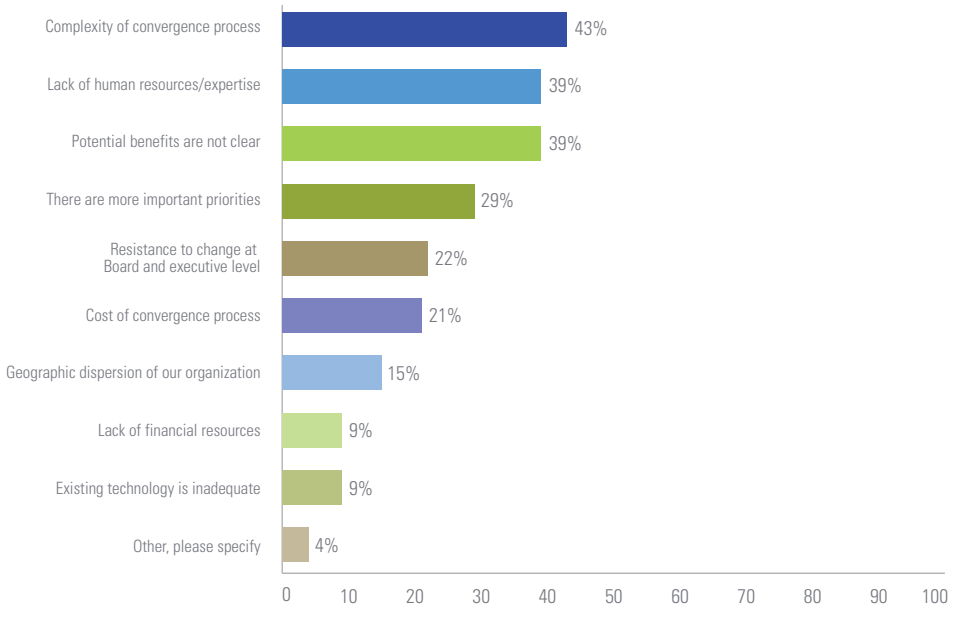
"A lot of organizations still have quite a fragmented approach with a large dependence on spreadsheets and a siloed approach to tackling different risk and compliance activities."

Despite growing stakeholder and business pressure to improve the coordination of their GRC activities, many companies still seem to struggle with convergence initiatives. This is due to a number of reasons. The biggest challenge of all, according to respondents, is the sheer complexity of the process (see chart 12).

With governance, risk and compliance responsibilities scattered around the organization and conducted by a wide variety of different functions, improving this co-ordination takes time, effort and patience. **"It's an evolutionary process,"** says Mr. Harris.

"You can't make this change quickly. It's a cultural shift that may take several years, and, even then, evolving obligations mean that you can never say the process is really complete."

Chart 12: Which of the following do you consider to be the most significant barriers to greater convergence of governance, risk and compliance at your organization?



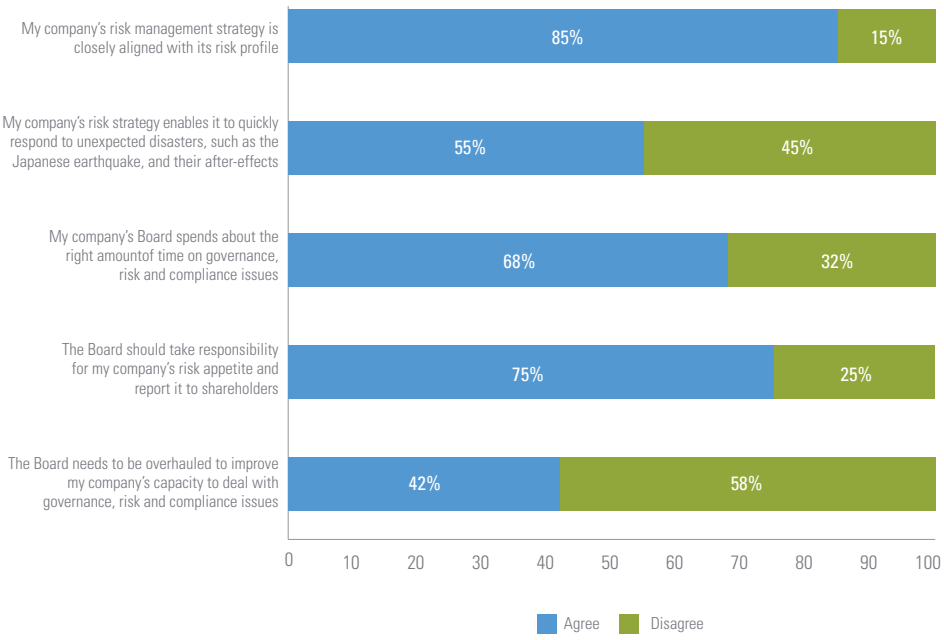
Source: Economist Intelligence Unit, June 2011

Many companies also encounter cultural resistance when trying to achieve consistency in their GRC processes. There may also be a perception that spending on GRC is costly and yields uncertain benefits. Among the survey respondents, almost two-thirds agree that convergence of governance, risk and compliance is seen as a cost, rather than an investment (see chart 4). This sensitivity to costs at the expense of recognizing the benefits is likely to be especially prevalent in the current economic environment, when many companies are still reeling from the impact of the financial crisis and remain keen to keep a tight rein on any capital expenditure.

But even if they did focus on the benefits, many companies find them difficult to measure. Only 31 percent of respondents say that their organization is effective at quantifying the benefits of GRC (see chart 5). This can certainly be challenging – particularly when trying to measure the potential impact of risk events that were prevented by improved coordination – but the quantification of benefits can be a vital part of building a business case for GRC investment.

Mr. Oxley suggests that companies should spend more time gathering data about incidents to enable a better assessment of the effectiveness of their risk management. **"By measuring even minor incidents and tracking how their frequency changes over time, companies can get a better picture of their progress and support the business case for a continuing focus on a GRC initiative as a management priority,"** he explains.

Chart 13: Please indicate whether you agree or disagree with the following statements.



Source: Economist Intelligence Unit, June 2011

If it's done properly, we can identify weaknesses in the current business and risk management that we can immediately fix. And we can also come up with a robust contingency plan that can be used if a particular tail risk unfolds."

CASE STUDY

Responding to the unexpected at HSBC

Identifying and responding to unexpected events and emerging threats is a key responsibility for risk management, yet it is one with which many companies continue to struggle. Just 37 percent of respondents say that their organization is effective at anticipating and measuring emerging risks (see chart 6). They also find it difficult to react promptly when the unexpected strikes. Only a slim majority of 55 percent say that their company's risk strategy enables it to respond quickly to unexpected disasters, such as the Japanese earthquake, and their after-effects (see chart 13).

More effective GRC convergence improves this performance. Among those respondents who have fully integrated GRC across oversight functions, 62 percent are able to react quickly to the unexpected and 58 percent are good at anticipating and measuring emerging risks.

In the wake of the financial crisis, the ability of risk professionals in the banking sector to deal with the unexpected has come under intense scrutiny. As events unfolded following the collapse of Lehman Brothers in September 2008, many institutions found that they were unprepared to deal with the scale of the crisis.

Although there is no easy solution to predicting tail risks, or *"black swans,"* ensuring that the organization is prepared to respond has become a key priority. Regulators have played their part by requiring that banks undergo frequent stress tests to assess the strength of their balance sheet against various pre-determined scenarios.

"At the moment, we don't have many ways of estimating tail risk, so stress testing has become an important tool," says Evgueni Ivantsov, Head of Portfolio Risk and Strategy at HSBC. *"If it's done properly, we can identify weaknesses in the current business and risk management that we can immediately fix. And we can also come up with a robust contingency plan that can be used if a particular tail risk unfolds."*

There are challenges with stress testing, first, it can be difficult to choose the right scenarios to test because tail risk inherently involves planning for the highly unexpected. *"The problem is that tail risk is largely about unknown unknowns,"* says Mr. Ivantsov.

A second challenge is that, even if the right scenarios are chosen, there is often limited analytical data on which to base them. In the absence of historical data, Mr. Ivantsov suggests that banks should instead rely on a more qualitative approach. *"When we run scenarios for tail risks for which we have very limited analytical data or experience, we need to focus more on the thought process rather than on number crunching,"* he explains.

Although financial markets and the global economy have started to recover from the shock of the financial crisis, the debt problems in the euro zone and the United States serve as a reminder that unexpected volatility remains a concern. *"Complexity and volatility will not come and go,"* says Mr. Ivantsov. *"They will stay with us for a long time. This is why we need to combine a robust risk management system to deal with everyday risks with an approach that allows us to react quickly, flexibly and in a non-standard way to tail risk events."*

05 Implementation

Any GRC initiative is a complex, multi-year project that requires input from a wide variety of stakeholders across multiple functions and geographical locations. Although the process by which companies achieve this convergence will vary from company to company, research conducted for this report suggests that there are ten useful principles that can help guide thinking and maximize the chances of success.

01 Consider the big picture first

The scale and long-term nature of a GRC convergence initiative can be daunting. For organizations embarking on a project for the first time, it can be difficult to know where to start. Mr. Marks of SAP recommends that companies look at the big picture first rather than be dragged down into detail. **"The most successful convergence programs start by thinking about the issues from 30,000 feet up, identifying the big problems and then prioritizing,"** he says. **"Companies may decide that their first priority is a need for consistent and reliable information. If you have multiple ERP (enterprise resource planning) systems and are relying on spreadsheets to manage risk, you can't do very much until you solve that problem."**

02 Form a cross-functional team or committee

Given the cross-functional nature of GRC, it makes sense to put in place a committee or group with senior-level support and representation from risk, internal audit, compliance and any other assurance functions that might be affected by the convergence process. This helps to provide a forum for airing issues and exploring best practice, and ensures that the initiative does not come to be regarded as being owned by a particular function. **"The different functions involved need to communicate, share experiences and develop good practice in order to break down the silos and get people working together across organizational boundaries,"** says Mr. Hopkin.

03 Define roles and responsibilities early in the process

Effective GRC convergence requires executives from a range of different functions to collaborate, share information and co-ordinate with each other. This can be challenging, not least because individual functions may be comfortable with existing processes and view a more open approach as eroding their closely guarded fiefdoms. **"You have to sit down and define your boundaries before you can start to collaborate across them,"** says Ms. Tate. **"Each function has a different reason for existing, but by coordinating and talking to each other, we can be more efficient in our work because we don't need to all ask the same question or go down the same road."**

04 Beware of building another silo

Building a GRC framework should not be about empire-building or creating an additional layer of bureaucracy. The danger of this approach is that it defeats the purpose of convergence by creating a new silo. "**It's important to build as little infrastructure as possible,"** says Mr. Hogan. **"It's more about creating the scaffolding that supports the flow of information and processes across the business."**

05 Get the processes worked out before investing in the technology

Although technology is an important part of the GRC program, experts questioned for this research advise against getting locked into technology solutions too early in the convergence process. **"You really have to work out how your organization makes decisions and how information flows around the business,"** says Mr. Hogan. **"That takes time to understand and, when you've done that, you can start to build systems and processes around everything."**

Companies should also ensure that they take a holistic view of technology. Although there are plenty of technologies available that provide a platform for risk and compliance, there is a danger that this creates an additional silo and makes it difficult for the organization to then link this platform with broader strategic goals. **"If you buy a separate technology to handle risk and compliance, you may be introducing more fragmentation and more cost,"** says Mr. Marks. **"Instead, you need to take a broader view and think about where the company as a whole needs to go with its IT applications."**

06 Seek out overlaps and build efficiencies

Mr. Harris compares GRC convergence to the post-integration phase that a company goes through when it has completed an M&A deal. **"When one company acquires another, there will be an analysis of where there are duplicate capabilities and a decision taken over which to keep and which to remove,"** he explains. **"The same logic applies to GRC. You look at where there is overlap in roles and infrastructure, and use the opportunity to create efficiencies and reduce cost while still ensuring that you don't inadvertently generate inconsistencies and errors in your compliance."**

07 Create a common language and understanding around risk

Fragmentation of risk and compliance across multiple functions leads to an inconsistent approach to describing and measuring risks. If one department measures risk differently from another, the Board and senior management will find it difficult to gain an accurate overall picture of their risk exposure. Standardization of the language and controls can help to increase consistency and support an enterprise-wide view of risk. **"Having a common taxonomy or category structure for risks is helpful when working with other risk functions because it means that you are thinking about risks and their categorization in a consistent way,"** says Ms. Tate.

08 Look for ways of converting compliance expenses into broader business benefits

Investment in risk and compliance need not be a sunk cost. Often, companies can reapply processes that they use for compliance purposes to support a business objective. In financial services, for example, a bank may find that data collected notionally for compliance may also have value from a customer relationship perspective. **"It's possible to just comply, but it's also possible to put in a better system that aligns with the objectives of the firm and will help with creating revenue and value for shareholders,"** says Mr. Harris.

09 Don't lose the detail in the convergence process

By converging diverse risk activities that may be at very different stages of maturity, companies run the risk that they lose the detail and expertise that exists across these functions. It is therefore important when converging GRC activities that companies do not end up with a lowest common denominator approach by forcing different risk functions to report in a standardized way. **"If you talk to safety risk experts or IT risk experts, they will have a really good understanding of the drivers of risk in their areas, so it's very important that the convergence of these activities does not lose that detail,"** says Mr. Oxley.

10 Remember that GRC is a gradual process

Companies should not see a GRC initiative as involving a wholesale change to existing risk and compliance processes. Instead, they should adopt an evolutionary approach by picking one project initially, and then gradually moving new and existing capabilities over to a central platform. **"The way forward is not to throw everything out and put something brand new in—that's too difficult, too complicated, takes too long and is too expensive,"** explains Mr. Harris. **"Instead, companies should pick one project—perhaps a new, material compliance obligation—and use that as a launching point, to create a 'store once, use many times' infrastructure for GRC. Over the course of several years, you can achieve a single, consistent data store, and reporting and management tools across all of your GRC activities."**

CASE STUDY

Convergence and growth at Alliance Data

As a company expands overseas, opens new offices and recruits new employees, ensuring that there continues to be a clear focus on risk and compliance is a major priority. For Shane Hogan, Director of Risk Management at Alliance Data, these are becoming familiar challenges. Alliance Data, a company that provides loyalty marketing solutions, credit services and analytics to customers in sectors, including retail and financial services, grew by 11 percent in 2010 and has revenues of US$2.8bn.

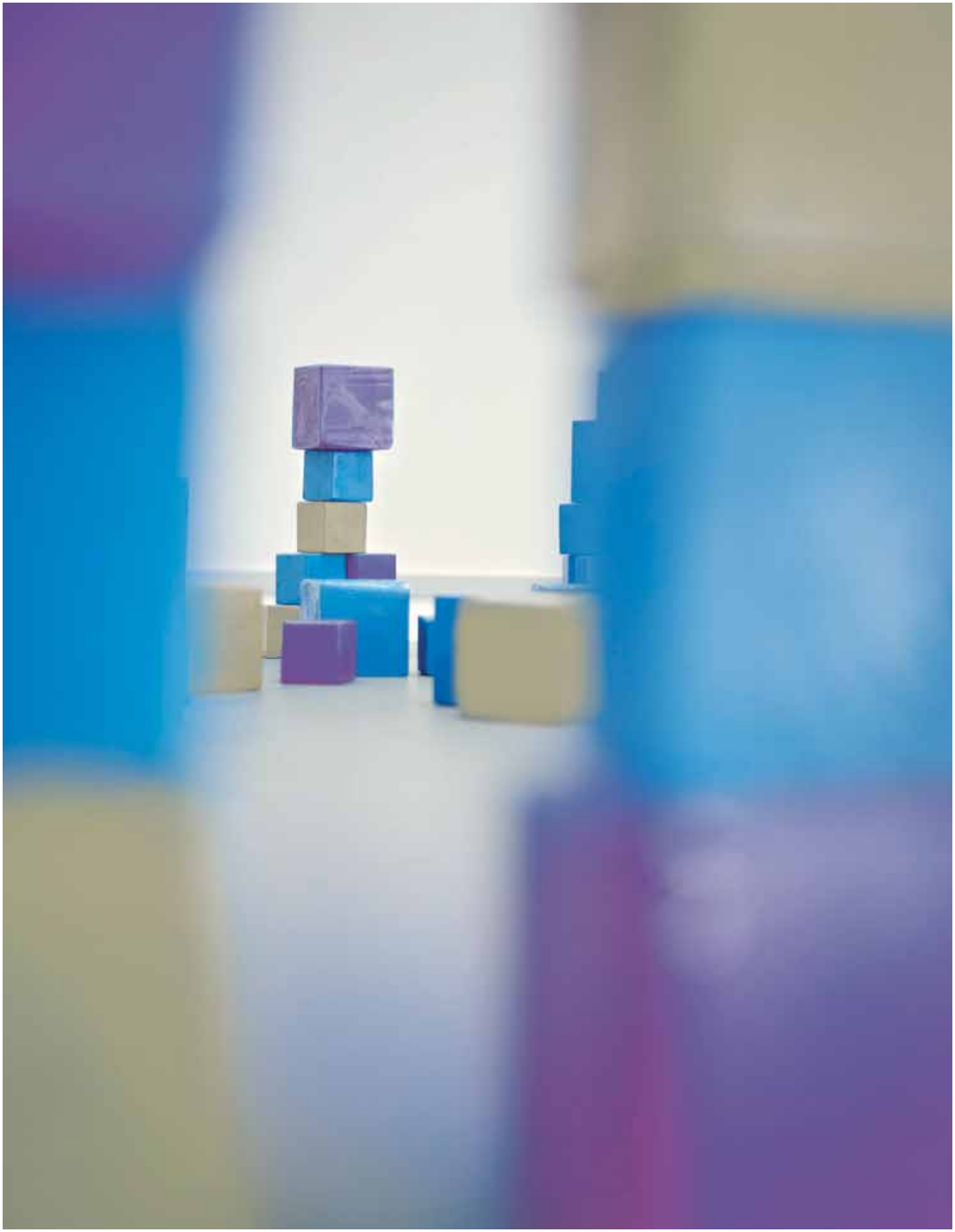
Greater co-ordination of risk and compliance functions is seen as a key component of the company's growth plans. *"As we start to move across the atlas, it is important to know how different functions in the business are acting,"* says Mr. Hogan. *"We need to capture the key risks we are facing and respond to them appropriately. We need to co-ordinate the activities of the various assurance functions, and ensure that they are doing the right things to protect their data."*

Mr. Hogan emphasizes that this more rigorous approach to coordination must not place the business under unnecessary constraints. *"You need to be careful that you are not simply creating more bureaucracy,"* he says. *"The key is to change behavior, processes and information flows, not build a new infrastructure. In our organization, we have risk officers in lines of business and they speak constantly. But we don't have a large staff and probably never will."*

Convergence of risk functions requires companies to take a more coherent approach to their risk information and databases. *"If different risk functions have different databases then you'll never talk to each other effectively,"* says Mr. Hogan. *"You need to get everyone on the same page so that they are using the same vocabulary and infrastructure."*

Improved co-ordination of risk and compliance functions not only provides greater confidence that exposures are understood. It also improves the quality of information that is being passed to the Board. *"The one thing a Board member wants is a line of sight into the opportunities and challenges of the organization,"* says Mr. Hogan. *"If they start to feel they are not getting consistent information, that's the time when you need to start thinking about new processes and structures. We need to make that line of sight as robust as possible."*

But impressing the need for focus on convergence is not always easy. A *"not invented here"* mentality can make it difficult for some functions to accept the need for change, while there may be a perception among affected departments that greater convergence implies loss of control. *"Any time you bring change to a multinational organization you will meet resistance,"* says Mr. Hogan. *"The key is that senior management have endorsed it and feel like it is important as part of their growth plans to build out your risk management capabilities. Without that support, you won't accomplish much."*



Contact us

John Farrell
KPMG in the US, Global Governance,
Risk & Compliance Leader
T: 1 212 872 3047
E: johnmichaelfarrell@kpmg.com

Oliver Engels
KPMG's European Head of Governance,
Risk & Compliance
T: 49 69 9587 1777
E: oengels@kpmg.com

Deon Minnaar
KPMG in the US, National Governance,
Risk & Compliance Leader
T: 1 212 872 5634
E: deonminnaar@kpmg.com

25640NSS | November 2011 | Printed on recycled material.

kpmg.com