



# The convergence challenge

Global survey into the integration of governance,  
risk and compliance

February 2010

KPMG INTERNATIONAL



In co operation with

AUDIT ■ TAX ■ ADVISORY

**Economist Intelligence Unit**

**The  
Economist**

# About this research

In September 2009, the Economist Intelligence Unit carried out a global survey on behalf of KPMG International, assessing the convergence of governance, risk management and compliance (GRC). The research looks at the driving forces behind convergence, the costs and perceived benefits and the barriers to achieving this goal.

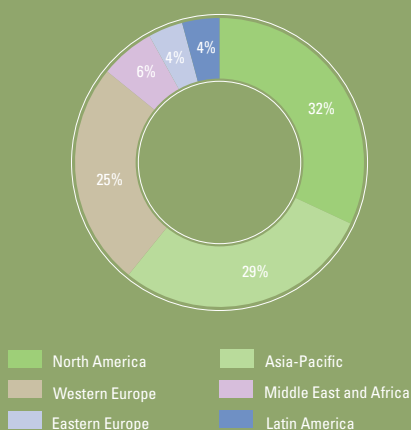
The Economist Intelligence Unit surveyed 542 executives from a wide range of industries and regions, with roughly a third each from the Asia Pacific, Americas, and Europe, Middle East and Africa regions. Approximately 50 percent of respondents represent businesses with annual revenue of more than US\$500 million. All respondents have influence over or responsibility for strategic decisions on risk management and more than one half of respondents are C level or board level executives.

In this survey, governance, risk and compliance refers to the overall governance structures, policies, technology, infrastructure and assurance mechanisms that an organization has in place to manage its risk and compliance obligations.

To supplement the survey, the Economist Intelligence Unit interviewed 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.

## Geographic representation



All graphs in this report are sourced from research conducted by the Economist Intelligence Unit, 2009. Due to rounding, graphs may not equal 100 percent.

# Foreword



**As large, global companies have become ever more complex, they have found it increasingly difficult to exercise control over decision-making around their organization. In some cases this has resulted in individuals taking unnecessary risks or making ill-judged choices that have damaged a business and its reputation.**

The emergence of governance and risk management is a response to such complexity, yet this has failed to prevent a spate of corporate scandals or, more recently, the near collapse of the banking system. At various points in the past decade, regulators at both the global and country level have felt compelled to step in, passing a number of new laws. Some of these aimed to improve corporate governance (Sarbanes Oxley Act) and others to tighten risk management (Basel II and Solvency II). In the wake of the global financial crisis, more regulation may well be on the way.

Fearful of both business failure and the penalties of non compliance, many organizations have reacted by swelling their governance, risk management and compliance (GRC) departments. This has

led to a costly and complex web of often uncoordinated structures, policies, committees and reports, creating duplication of effort. Worse still, GRC has lost sight of its prime objective: to improve performance and efficiency. In short: the solution has become part of the problem.


In recent years, internal auditors, risk officers, compliance officers and information technology chiefs have begun to work together more closely, finding commonality between disparate GRC projects. Some organizations even formed GRC committees, and an increasing number of software vendors entered the GRC market to ease the burden of administration. Such efforts have increasingly come under the banner of GRC convergence.

To explore the extent to which organizations are integrating GRC, KPMG International commissioned the Economist Intelligence Unit to carry out a global survey of over 500 major companies.

The results – which are augmented by comments provided by specialists from experienced advisors from KPMG member firms around the world – provide valuable insight for organizations looking to get the most from their investment in GRC.

**Mike Nolan**

**Global Risk & Compliance  
Service Group Leader**



GRC convergence is an idea whose time has come. It is not simply a technology tool; it is a way to rationalize risk management and controls, giving management the information they need to improve business performance and achieve compliance.

**Oliver Engels**  
KPMG in the UK  
European Head of Governance,  
Risk & Compliance

# Contents



Executive summary



The changing landscape



Internal and external influences



Rising costs – and perceived benefits



The long road to convergence



In summary



Appendix – Survey results

With the exception of the KPMG Comment and KPMG Final Thought sections, the views and opinions expressed herein are those of the Economist Intelligence Unit and the entities surveyed and do not necessarily represent the views and opinions of KPMG International or KPMG member firms. The information contained is of a general nature and is not intended to address the circumstances of any particular individual or entity.

# Executive summary

**Many companies are showing an increased appetite for the convergence of governance, risk and compliance.**

Almost two thirds (64 percent) of survey respondents say that this is a priority for their organization, driven by business complexity, a desire to reduce risk exposure and a need to improve corporate performance.

**There is still some way to go before companies achieve full integration of governance, risk and compliance across different functions and regions.**

While desire for integrated GRC may be widespread, the survey suggests that for many organizations, such an ambition is still in the very early stages of development. Of those surveyed, only 11 percent report full convergence across geographies, and barely more claim integration across business units, oversight functions and strategies.

**The cost of GRC is significant and rising by the year.**

Half of those taking part in the survey estimate that governance, risk and compliance is costing their business around 5 percent of annual revenue, and a vast majority (77 percent)

expect to see an even greater outlay over the next two years. Respondents from heavily regulated industries, such as financial services and energy, were more likely to anticipate increased expenditure. Despite this growing investment and interest in GRC convergence, only a quarter (26 percent) feel that this will actually help bring down costs through a reduction in duplication and identification of synergies.

**Many organizations struggle to realize the benefits of convergence.**

Just a third (34 percent) of those taking part in the survey believe that expenditure on GRC represents an investment rather than a cost, while 45 percent say it is challenging to build a business case for greater convergence. Even fewer believe that convergence would help improve corporate performance; the single biggest benefit was felt to be an ability to identify and manage risks more quickly (chosen by 59 percent of respondents).

**People – not technology – present the greatest barrier to successful convergence.** Integration is likely to involve a major transformation program,

so perhaps, unsurprisingly, resistance to change is considered the single biggest obstacle (44 percent), followed by complex convergence processes (39 percent) and a lack of available experts (36 percent). Less than one in ten mentioned inadequate technology as a hurdle to overcome.

**The executive management team and regulators are exerting the greatest pressure on organizations to improve their convergence of governance, risk and compliance functions.**

There are a number of reasons executive management is pushing for change, among them a need to reduce risk exposure and a desire to improve corporate performance. The survey indicates that the influence of non-executive directors is considerably less strong. And when it comes to publicly-listed companies, only a quarter (25 percent) feel that non-executive management is pushing hard for convergence, which is surprising given the higher governance responsibilities and fiduciary duties facing such individuals in the wake of Enron and other scandals.





**64**  
percent

of respondents say GRC convergence  
is a priority for their organization

**Half of  
respondents**

believe that investment in GRC is  
equal to 5 percent of annual revenue

Only  
**39**  
percent

believe convergence helps improve  
corporate performance

Resistance to change  
is considered the

**single biggest  
obstacle**

to convergence



The severe economic conditions have created an environment of intense uncertainty, with companies increasingly concerned about the risks facing them and the effectiveness and adequacy of the controls in place to manage these risks. This landscape, along with a huge rise in complexity, has put a big strain on the processes, customs and policies through which many global businesses govern themselves.

## The changing landscape



## 39 percent of respondents say their organization creates a new initiative for each new regulatory challenge

**“The word governance has morphed from being focused a number of years ago on the world of corporate secretariat, that is, primarily concerning company law structures, to being a term that covers all the moving parts in an organization,”**

says Brian Harte, Group Head of Compliance, Europe and Asia, at the Royal Bank of Canada.

And a clearer view of those “moving parts” is critical to better risk management and hence corporate performance. As the saying goes: what can be measured, can be managed. GRC is not just an exercise in finding synergies between IT projects, it is an active approach to better governance by providing a clearer picture of risk across the entire organization – and that includes the risk of non-compliance.

Mr. Harte took his first role in regulatory compliance 21 years ago. “I was given a mandate and told all of this regulation would go very quiet after about 18 months, and that would be the end of it,” Mr. Harte recalls. “It is 21 years later and we’re now in another enormous uptick again.”

Fuelled by a desire for greater certainty along with a fear of non-compliance, many companies are devising tighter rules and procedures for running their organizations, and external regulators are doing the same. Lord Adair Turner, chairman of the UK Financial Services Authority (FSA), told City bankers last year that the days of soft-touch regulation are over. Similar sentiments are being expressed by the US Securities and Exchange Commission (SEC) and other financial regulatory authorities around the world.

The G-20 (a group of finance ministers and central bank governors from 20 economies: 19 countries, plus the EU) has also had much to say in its efforts to promote international financial stability, which may create further regulatory pressure.

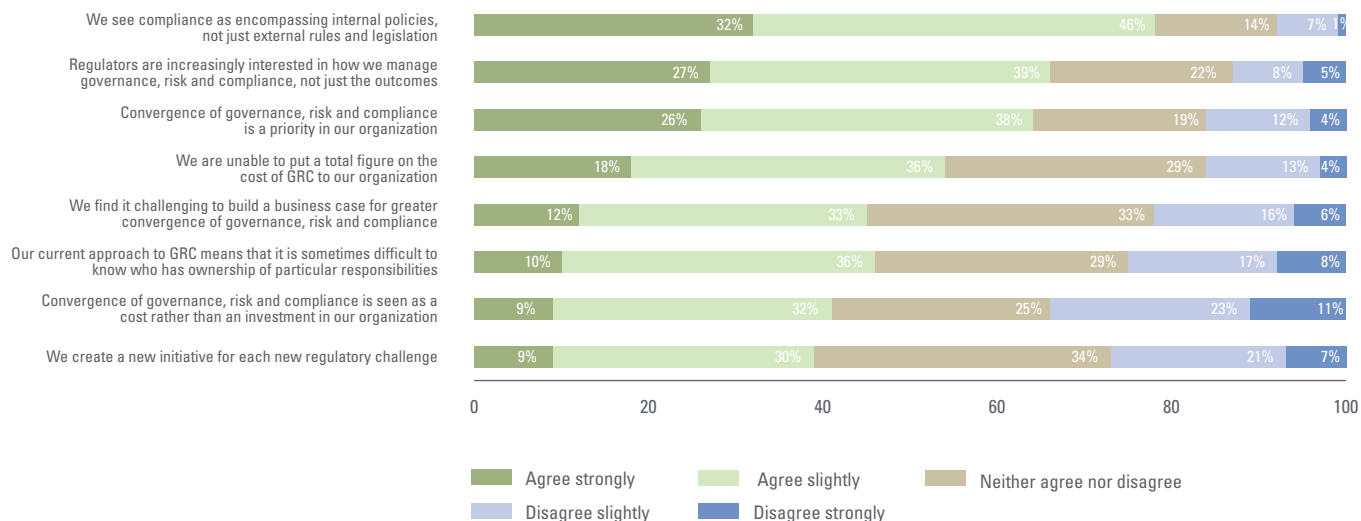
**“I’ve heard several people say: ‘I’m working so hard on compliance, I can’t get any work done.’”**

says Dr. George Westerman, research scientist, at the Center for Information Systems Research at MIT’s Sloan School of Management.

It is not just those in the financial services industry who are feeling the burden. Indeed, over one-third (39 percent) of respondents to our survey, drawn from a range of sectors, highlight the fact that their organization creates a new initiative for each new regulatory challenge it comes across.



## Organizational attitudes to governance, risk and compliance (GRC)



Information technology (IT) departments often find themselves swamped with requests for new regulatory compliance systems and risk management systems. The fact that there is often an overlap between these systems has not escaped the notice of the chief information officer, the chief risk officer and the heads of internal audit and compliance, so much so that senior managers have attempted to

rationalize these projects under the banner of GRC (governance, risk and compliance).

“The severe recession and problems in the financial sector have increased the importance of effective GRC to all the stakeholders,” says Mike Temple, chief risk officer at Unum, a US insurance firm. “Firstly, management and boards have increased pressure to navigate through this challenging economic environment.

Secondly, headlines about executive compensation have damaged companies’ reputations with regulators and ratings agencies. And, thirdly, in the US and UK, there has been talk of expanding the role of government in the financial services sector. All of those stakeholders are pushing for stronger governance, more effective risk management and strict compliance with regulation.”



## The growth of convergence

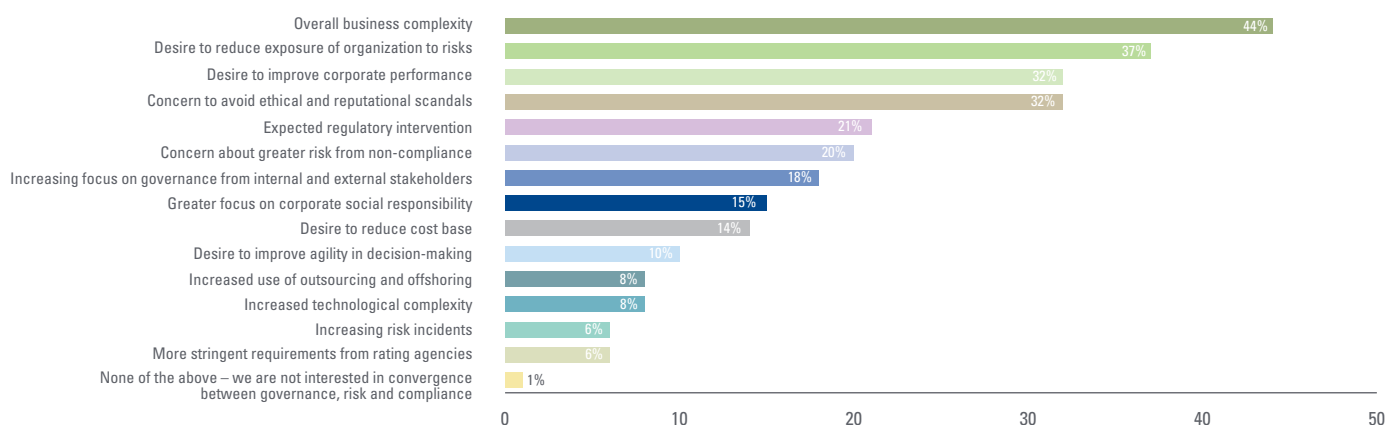
More and more, companies are looking at reducing risk, cutting costs and improving performance by adopting a more integrated approach to managing their governance, risk and compliance

activities. In our survey, 64 percent of respondents consider this to be a priority for their organization.

When asked what is fuelling this interest in convergence, 44 percent cite overall business complexity, followed by a desire

to reduce organizational risk exposure (37 percent) and improve corporate performance (32 percent). Only 14 percent feel that cost reduction is a driver – which is surprising given the growing investment in GRC.

### What is influencing your organization's interest in GRC convergence?



Respondents were allowed up to three responses.

### "If something is more complex, it is just more risky,"

says Dr. Westerman of MIT's Sloan School of Management. "But when companies go beyond that, to actively manage unnecessary complexity out of their business processes and technologies, they benefit not only from lower risk but also higher efficiency and agility." In a bid to unravel this complexity, many firms are looking to consolidate risk management to create simpler, more effective governance structures and rationalize regulatory compliance.

One tool being employed is enterprise risk management (ERM), which places a greater emphasis on cooperation between departments to manage the organization's full range of risks. Interestingly, nearly half of the larger firms<sup>1</sup> taking part in the survey (45 percent) were particularly concerned with avoiding scandals that could damage their reputation this is the single most important factor influencing their interest in the convergence of governance, risk and compliance.

Bigger organizations may find it harder to keep track of every employee, as Royal Bank of Canada's Mr. Harte observes:

**"In my experience, the most dangerous areas are often quite small and overlooked and on the margin. Companies have to make sure they have the appropriate intelligence flows feeding up and the appropriate feedback, and that they have captured everything."**

Of course, a more comprehensive view of risk management and regulatory compliance doesn't just keep your name out of the newspapers; it also simplifies business processes and systems. Such a process has worked well for US-based Ventura Foods, a manufacturer of vegetable-oil based

<sup>1</sup> For the purposes of this report, organisations with annual revenue in excess of US\$10bn

# Case study

## Ventura Foods: Convergence across disparate practices

The experience of California-based Ventura Foods, which manufactures vegetable oil-based products, may be familiar for many executives designing and implementing coordinated GRC policies for the first time. Ventura Foods is privately held, and the company has grown rapidly through acquisitions over the past decade. This has resulted in decentralized decision-making, un-coordinated processes, inconsistent policies, disparate practices and duplicated efforts.

Now, though, the company is tackling these issues. That job has fallen to Jason Mefford, Vice President of Business Process Assurance, who joined Ventura Foods in 2006 with the mandate to set up an internal audit function. "There had been some internal auditing but not a fully robust department," he recalls. "A lot of these GRC-related items that we should be auditing against were not in place."

As a first step, Mr. Mefford opened the Red Book, a guide to GRC produced by the Open Compliance and Ethics Group, a non-profit organization that helps companies align their GRC activities. He identified the components of a GRC program, determined which were already in place at the company, and decided whether these needed to be refined. He also singled out those elements the company did not have in place, and asked whether, as a private company, it needed them.

**"It's a question of how much internal audit and compliance do the owners want," Mr. Mefford says. "It depends on how much they want to spend and how comfortable they want to be, that everything is buttoned down."**

Ventura Foods then developed a code of conduct, including defining the organization's core values, of which every employee has a copy. The company also

set about coordinating disparate GRC practices that were already underway across the organization. "We're joining up all these activities and getting some committees together," explains Mr. Mefford. "This means different people talk with each other, see what they are actually doing and have some kind of a reporting mechanism."

He says the company's ultimate goal for GRC is to have integrated policies, practices, and structures in place, including a compliance committee or compliance task force. Among other things, such a committee will be responsible for the co-ordination of GRC-related events and the timing of meetings. Ultimately, it will handle routine reporting to the board. "We're about a third of the way there and we have a long way to go," he says.

# KPMG Comment

## Survival of the most informed

**We believe that GRC convergence is an idea whose time has come. It is not simply a technology tool; it is a way to rationalize risk management and controls, giving management the information they need to improve business performance and achieve compliance.**

In bigger companies at least, the expansion of governance, risk and compliance activity has created a number of large, unwieldy and often autonomous groups. It is not uncommon to have dozens of committees dealing with different aspects of risk – many of them overlapping yet not communicating.

In the midst of this bureaucracy and duplication, many organizations are drowning in a sea of complexity. They have been unable to distinguish the critical business risks at both group and entity level, and have come to mistrust some of the business intelligence they are receiving.

The disproportionate focus on regulatory demands has been driven largely by fear of non-compliance. The typical reaction to a regulatory directive is to form new layers of risk, control and compliance structures (including new risk committees) and produce new measurements. This is costly, cumbersome and does not necessarily lead to better governance or risk management; indeed it may even distract management from important business issues. Arguably the credit crisis was caused in part by such an approach; financial institutions were churning out quantitative reports, yet failing to apply sound business judgment on the decisions made by their staff.

Although it is of course vital to establish a sound reputation in the eyes of regulators, shareholders and investors, compliance should preferably be a natural consequence of a well-governed company that has a common approach to managing risk – and makes individuals accountable for their decisions.

Rather than asking, “What do regulators want to see?” organizations should be looking at the real risks facing them, and the controls necessary to keep such risks in check. At a time when mere survival is a prerogative for many companies, this should bring a renewed emphasis on business performance, access to capital, efficiency and cost reduction.

In the current economic turmoil, GRC convergence has come of age. It seeks to bring together complex and disparate risk and compliance activities and directs these efforts more efficiently, in alignment with corporate strategy and supported by organizational culture. Such an holistic approach can give leaders the intelligence and insight they need to build greater business resilience and be better prepared for ongoing change.







Our survey suggests that both executive management and regulators are the main driving force behind GRC convergence. This is not too surprising, as the ultimate responsibility for executing such change on a practical level lies with senior management. This picture remains consistent across publicly-listed companies, state-owned and not-for-profit organizations.

## Internal and external influences

# Executive management and regulators are among the main influences behind GRC convergence

Recent economic events have rekindled interest in corporate governance and operational risk management amongst regulators, ratings agencies, politicians, the media and the public. Our survey responses suggest that executive management is rising to this challenge, at least in part as a pre-emptive strike to ward off further criticism – and prevent additional regulation.

**GRC integration should lead to better reporting up the hierarchy and hence a more complete view of critical risks facing the organization. A lack of such oversight was arguably a major cause of the current financial crisis.**

With this in mind, it is understandable that regulators should be taking such an interest in convergence. Two thirds of survey respondents agree that regulators are increasingly interested in how they manage governance, risk and compliance – and not just in the outcomes.

**“The concept of supervision is changing,” says Mr. Harte of Royal Bank of Canada. “There is greater supervision from regulators. It is becoming increasingly more outcomes-based supervision rather than tick-the-box supervision.”**

A glaring absentee from those pushing for convergence is the non-executive board – only 17 percent of respondents say that this group is the main influence. Even customers are more likely to influence levels of GRC integration than non-executive directors. And the picture is largely the same at publicly listed companies, with non-executive directors less influential than executive directors, regulators, auditors and investors. This is quite a surprise given that, in the UK at least, non-executive directors share the same legal duties and responsibilities, as well as the potential liabilities, of their executive counterparts.





Governance, risk management and compliance are proving to be a costly matter for many companies. Half the respondents say it may be costing them as much as five percent of annual revenue and a fifth estimate it could even stretch to 10 percent. When questioned further, however, a sizeable proportion (54 percent) are unable to put a precise figure on this outlay.

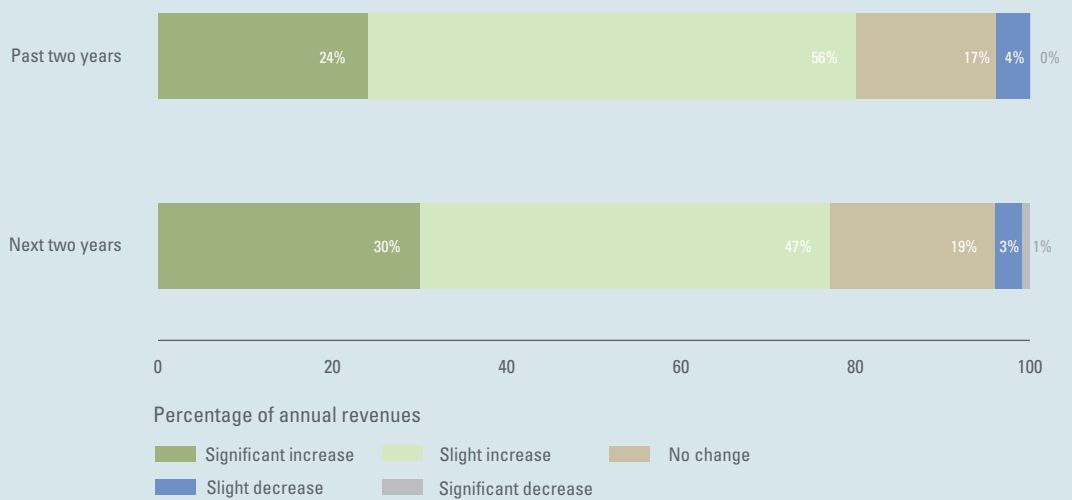
## Rising costs – and perceived benefits

# Half the respondents say investment in GRC may be as much as five percent of annual revenue

Regardless of their inability to pin down a number, a large majority of survey participants (77 percent) expect to see costs mirror recent trends and rise further over the next two years. This

expectation was even more pronounced in heavily regulated industries, such as financial services and energy, where around four in ten think GRC investment will grow “significantly” by 2011.

## Changes to the cost of GRC



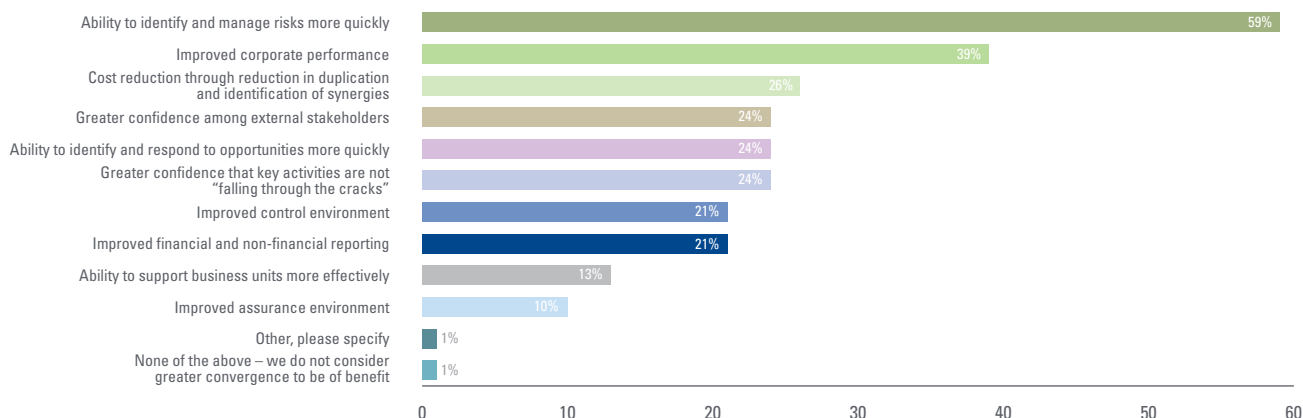
## Just 39 percent of respondents believe GRC convergence will improve corporate performance

This substantial and growing investment suggests that companies are taking GRC very seriously – yet many appear to be uncertain about what they're getting in return. Just one third (34 percent) of those taking part in the survey believe that expenditure on GRC represents an investment rather than an expense. And 45 percent find it challenging to build a business case for greater convergence.

"It [regulation] is still generally viewed as the cost of doing business," says Royal Bank of Canada's Mr. Harte. "But it's not all a burden – some of it is strength and capability." Indeed, the tighter regulation in Canada meant that the country's banks – with their generally more restrictive leverage, relatively high capital ratios and more conservative approach to mortgage lending – were in better shape to cope with the global recession than their counterparts in many other countries.

When asked to list the benefits of convergence, the ability to identify and manage risks more quickly is singled out by 59 percent of respondents. "It's important for GRC to be integrated to see the whole picture," says Nick Hirons, Vice President, Head of Audit and Assurance at GlaxoSmithKline (GSK). "Without integration it's impossible to fully aggregate risk across the entire business."

### Main benefits of better GRC convergence



Respondents were allowed up to three responses.

However, there appears to be less confidence in the wider benefits of integrating governance, risk and compliance. Less than four in ten (39 percent) believe this can improve corporate performance and only 26 percent feel it will help reduce the costs of duplication. Even fewer believe it will help them support business units more effectively.

Dr. Westerman of Sloan School of Management certainly feels that convergence can bring rewards: "When you get in there and try to put controls in your business processes to see where you need to control every element of it, sometimes you just realize you have got a bad process. Instead of sinking money into protecting a bad process, you can rework it and get all kinds of savings. Some firms tell me their compliance activities have

partially paid for themselves by identifying new business process efficiencies."

**Improved business processes have fewer controls and are therefore easier to manage from a risk perspective. They are also more efficient and more agile, which should help the business perform better.**



# KPMG Comment

## Getting the most out of your investment in GRC

**Through a renewed focus on performance, organizations can simplify existing policies and controls, gain greater visibility over the risks they face, and realize greater efficiency from GRC.**

The rush to satisfy regulatory requirements has clouded many companies' memories of why they invested in governance, risk management and compliance management in the first place. Some are worried that they cannot see a measurable return on their expenditure, and in the current climate of financial prudence, may give preference to alternative projects with more tangible outcomes. In other cases, GRC integration activities may be turned down on the grounds that they do not meet any immediate regulatory needs.

Forward-thinking leaders, on the other hand, do the opposite: they first consider the corporate benefits, realizing that what is good for the business is often good for the regulator.

The apparent vast sums being spent on GRC should provide a wake-up call to seek greater cost-efficiency. For example, if the survey respondents' estimates are accurate, a company with US\$1 billion annual turnover may spend as much as US\$50 million of this on GRC. Rationalizing GRC through effective integration could go a long way to reducing this figure.

By revisiting the objectives of GRC, organizations can clarify what they are trying to achieve and how they can measure success. Many survey respondents are keen to reduce complexity, so it is helpful to break down the various activities into bite sized practical steps. This could involve integrating risk within strategic planning, so that any major initiatives take account of the accompanying risks and receive the appropriate challenge.

Companies could also determine how well positioned they are to mitigate key risks, and review the usefulness of any group

level risk policies and controls – discarding any that are not critical. Last, but not least, an attempt should be made to simplify the often unwieldy committee and reporting structures. All of this should go a long way towards bringing down the cost of GRC.

As the global economy moves out of recession, effective GRC is likely to be seen more and more as a pre-requisite for business success. With greater visibility and control over risk, organizations can gain a real competitive edge, enabling them to take decisions in the knowledge that they are unlikely to exceed their risk appetite, and that there is inbuilt resilience within their systems.

Such a robust approach to risk could also be an advantage in any efforts to complete transactions. An effective, sustainable risk and compliance framework should be looked on favorably by rating agencies, as well as speeding up the ability to successfully fulfill due diligence criteria.

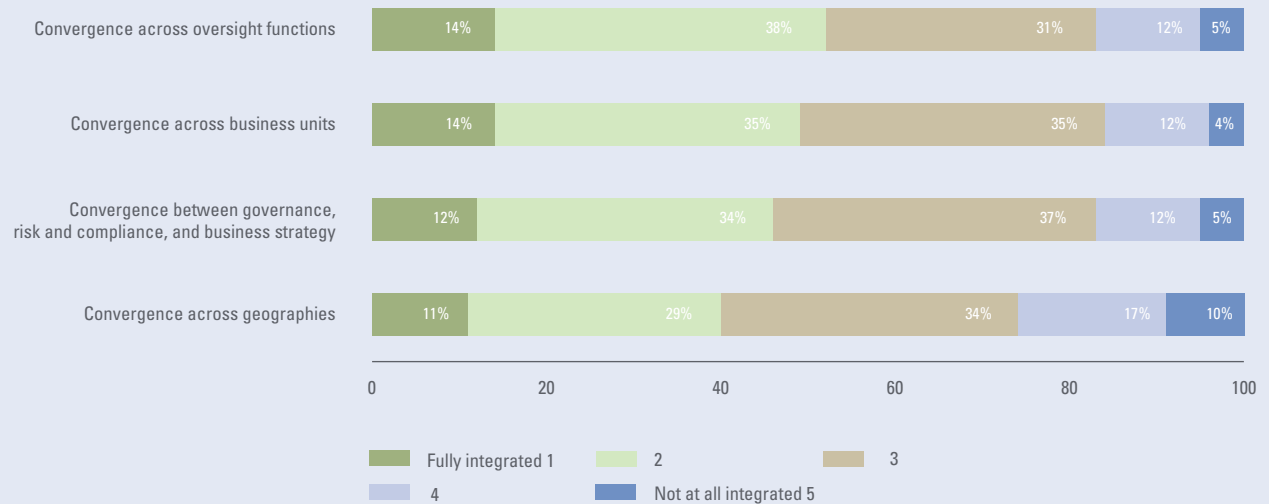




While many companies are clearly showing an increased appetite for a converged approach to GRC, there is a long way to go before such practices are fully implemented and operational. Only around one in ten executives responding to our survey could boast of full integration across oversight functions, geographies, business units or strategies.

## The long road to convergence

### Degree of GRC convergence across the following entities in your organization



Geographical convergence in particular appears a tough challenge: 27 percent of respondents have made little or no headway in this respect. "Convergence needs to happen across all areas, and must be by risk, by business unit and across geographical boundaries," says GSK's Mr. Hirons. "Businesses are becoming more complex, and without this multidimensional approach it will be difficult to spot the gaps."

GSK has embedded risk management processes within its operating businesses and Mr. Hirons says that awareness of risk and compliance issues are widespread across the entire organization.

The convergence of governance, risk and compliance is not necessarily an attempt to create a single, monolithic GRC structure with one reporting line leading to the top. Rather, it is a common approach to eradicating duplicated effort, complexity

and cost. Integration is really about communication and cooperation.

Unum, for example, has four separate functions for handling GRC. Two of the functions report to the CFO and two report to general counsel. There is also a degree of autonomy in local markets.

**"We've chosen to use decentralized models, by and large," says Mr. Temple from Unum**



---

**“We think decisions are made on the ground in local markets on a day-to-day basis. But we want the ability to have consistency and to be able to aggregate them up, so we have a local and global approach. What we try to do is embed compliance and a culture of risk management and continuous improvement into our organizations and have common processes and tools and nomenclature so that we can aggregate up.”**

At GSK, there are risk management and compliance boards in all business units as well as a corporate-level risk oversight and compliance council. “The first important principle is that no one single person or committee can own risk,” says Mr. Hirons. “Risk management needs to be embedded and owned within the business or there is a danger it will become a paper exercise with no real value.”



# Case study

## GlaxoSmithKline: Embedding best practice

**As Head of Audit and Assurance at GlaxoSmithKline (GSK), a pharmaceutical company, Nick Hirons is used to working in a highly regulated sector. The company meets financial regulatory requirements set out by Sarbanes-Oxley in the US and the Combined Code in the UK, and also works within the stringent regulatory framework required by pharmaceutical regulatory authorities across the world, such as the US Food and Drug Administration and the Medicines and Healthcare products Regulatory Agency in the UK.**

Since the merger of Glaxo Wellcome and SmithKline Beecham in 2001, which created GSK, the company has designed, implemented and followed coordinated governance, risk and compliance (GRC) policies. This has meant that risk management processes have long been embedded within the operating

businesses at GSK – and awareness of risk and compliance issues are widespread across the organization. Nevertheless, says Mr. Hirons, “as with many large organizations, these systems haven’t always been joined together. Businesses are becoming more complex, which is increasing the need to develop a framework for the convergence of GRC systems. Without this multidimensional approach, it will become increasingly difficult to operate effectively.”

GSK has been moving towards governance, risk and compliance convergence to ensure it can manage and mitigate risk globally. Building on independent systems and processes, the firm has developed a group-wide GRC structure. At the top is the group Risk Oversight and Compliance Committee – the firm’s “ROCC”; as it is referred to internally – to which all salient GRC-related information is reported. Beneath, embedded in the organization, is a

structure that allows information to be filtered, aggregated and reported. Included in this are risk management and compliance committees in each of GSK’s operating businesses that review, measure and manage risk exposure. This structure is flexible, allowing GRC processes and practices to be tailored to each business unit – ensuring implementation and usage by the operating businesses.

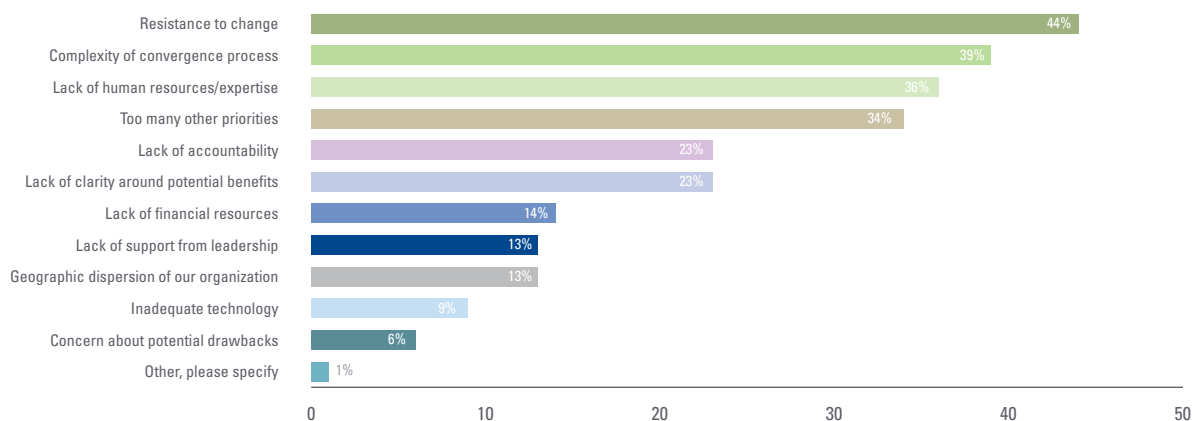
Indeed, such acceptance is crucial, according to Mr. Hirons. For him, the most important factor in implementing the existing company-wide GRC structure is that it is embedded within the business. “The business should pull, rather than having it pushed upon it,” he says. “If GRC is going to be of value, the business units should be part of this process [of implementing it] and this should be perceived as adding value to their business. This should not be a bureaucratic compliance process which is pushed on to the business units.”



Any major transformation program encounters opposition and GRC convergence is no exception, with 44 percent of respondents acknowledging “resistance to change” as the main barrier. Such a gap between desire and action is perhaps understandable given the number

of structures, processes and committees that are often put in place to deal with GRC. This probably explains why the larger organizations involved in the survey consider complexity to be the number one barrier.

### Significant barriers to greater GRC convergence



*Respondents were allowed up to three responses.*

Convergence is all the more difficult in organizations with poor communication between functions and the business. Where such a “silo” culture exists, persuading staff to share information and resources can be an uphill task.

Integration of GRC does not appear to be held up by technical factors, but rather by ‘softer’ issues involving people. Only nine percent of respondents say inadequate technology is a barrier to successful convergence. “Companies should think as much about the process change and the

organizational change as the IT change,” says Dr. Westerman of Sloan School of Management. “When projects fail, it’s usually not the technology that is the problem.”

Ultimately, any move towards GRC convergence is likely to be a lengthy process that requires an accompanying shift in corporate culture. This is exactly what Ronald Van Den Berg, risk and compliance officer at ArcelorMittal, experienced when he looked to implement coordinated GRC activities. Mr Van Den

Berg has made great strides, but an indication of the scale of the task is that four years after joining he feels that there is still much work to be done.

He also believes that external events can affect attitudes to change. At ArcelorMittal, for example, the global financial and economic crisis diverted attention away from GRC onto more immediate matters. In addition, cost saving measures instigated across the group meant there were fewer staff to deal with GRC issues.

# Case study

## ArcelorMittal: Towards coordinated GRC activities

**When Ronald Van Den Berg joined Indian steelmaker Mittal in 2005, he set out to tackle the group's Sarbanes-Oxley compliance, after its listed US subsidiary had fallen short of compliance three years running. Just a year after he joined and following the merger with Arcelor that created ArcelorMittal, the world's largest steel producer, he faced a new surprise: the former Arcelor business had even less of a compliance framework in place.**

As risk and compliance officer at the merged group's Flat Carbon Europe division, Mr. Van Den Berg set about ensuring SOX compliance across the division, the largest in the group. His efforts started at the top.

"You have to make senior management aware of this requirement," he says. "It was new to Arcelor, because the company had been listed only on European stock exchanges." Then it was time to involve operational departments and middle management. "If you want to have well-embedded processes, you need people on site, who work with the rest of the staff, on a day-to-day basis," he added.

When the global financial and economic crisis hit, however, Mr. Van Den Berg found that the attention to GRC topics shrunk dramatically, making it harder to get GRC back onto the company's agenda. Furthermore, cost-saving measures instigated across the ArcelorMittal group (in response to unfavourable economic conditions) meant he had fewer staff and other resources at his disposal.

Nevertheless, his efforts have borne fruit. "Today, we have much more structure in many of our processes and we have more visibility, in terms of what the individual production sites are doing," he explains. But there's still plenty to do. In particular, he is hoping to improve the quality of compliance processes, which he feels has suffered as a result of staffing constraints.

Mr. Van Den Berg is not stopping there. Next, he has his sights set on an even more ambitious target. Using the internal network he has developed whilst implementing his division's SOX compliance, he plans to merge all the division's separate policies and practices spanning compliance, audit certification and risk management. "My main focus is to integrate all these separate compliance processes," he says. "The group's GRC policies and practices are becoming more co-ordinated."

# KPMG Comment

## Back to basics

**To survive and thrive in today's difficult economic climate, companies require a strong risk culture backed up by effective, well monitored controls and overseen by firm governance.**

To make GRC convergence happen, organizations should cut through the complexity of the existing structures. As with any change program, there is likely to be a political element in challenging the status quo of established groups, all of whom feel that their roles are valuable.

First and foremost is the need for a clear vision and a common culture oriented toward good governance and risk management. To do this, every organization has to clarify its own unique risk appetite by asking: "What level of risk do we want to take in pursuit of our objectives?" The credit crisis showed what happens when organizations fail to define and control such an appetite.

Of perhaps equal importance are universal standards of behavior, or "how we do things around here." These should reflect your fundamental brand values and turn

every employee into a brand ambassador. One of the reasons for Arthur Andersen's collapse was the failure of a few individuals to uphold their most precious asset: its integrity.

Thus risk management becomes the responsibility of everyone, rather than a separate department. Management tasks such as strategic planning, budgeting and compensation should be closely aligned with this wider vision.

It is vital to uncover and understand the main risks facing an organization and to ensure that these are understood by everyone. These risks lie primarily in the main business processes, such as research and development, sourcing of materials, manufacturing of materials, processing of transactions, accounts payable and receivable, procurement, vendor management, and similar functions. By quantifying and measuring these risks in a consistent fashion, the subsequent reports should be reliable enough to support daily decision-making.

Of course, a strong risk culture alone will not always prevent people from making ill-

informed or risky choices. Clear controls provide limits to individuals' decision-making and create greater accountability and awareness of the consequences of one's actions. Any controls should of course be consistent across the organization.

Management, stakeholders and, increasingly, regulators require assurance that these controls are working and having a positive impact on behavior. A comprehensive evaluation, monitoring, and reporting of controls can help ensure their effectiveness, and keep them aligned with the broader strategy. By concentrating only on important risks, organizations can cut out unnecessary controls and avoid duplication. This not only saves money but also reduces the workload for internal audit.

The glue that holds all these activities together is governance. This encompasses both board and management activities and is dependent upon leaders having a clear oversight of risk and compliance across the organization. Such a single, company-wide view of risks and controls can

provide much needed assurance to increasingly attentive stakeholders. Creating a governance structure involves clarifying roles, responsibilities and resource capabilities and escalation procedures, as well as the information and reporting systems that govern business processes. It also entails the use of tools and systems to enable analysis, efficient monitoring, and reporting.

Technology serves as the backbone of an effective risk/compliance architecture, providing timely access to consistent, accurate, and comprehensive information as well as intelligent reporting.

By getting back to basics, organizations can lay a foundation for better performance and greater efficiency, while also meeting regulatory demands. All of this should help strike the right balance between risk management, governance and compliance – within a performance-based culture.





The survey suggests that the relatively new discipline of GRC is well recognized by executive management as a route to reducing organizational complexity, as well as the problems associated with complexity. While many companies are displaying an interest in the area, they also appear to be concerned about the return they are seeing on the vast sums being spent on governance, risk and compliance. Only a third believe that this represents an investment rather than a cost and only a quarter feel it will reduce costs.

## In summary



Yet the appetite for convergence appears to be strong, with a healthy majority saying that this is a priority for their organization. Unfortunately, many companies have been unable to translate this appetite into appropriate action. Very few of those companies taking part in the survey have managed to achieve integration across business units, geographies or functions, with resistance to change cited as the single greatest barrier.

For some at least, the task of simplifying and streamlining governance, risk and

compliance appears to be a step too far at a time when they're focused on surviving the recession and coping with increasing regulatory demands. And although respondents believe that business complexity is considered the biggest driver behind integration, much of the growing cost of GRC ironically appears to be feeding rather than reducing this complexity.

The big question seems to be: how to make convergence happen? The executive team arguably needs greater support from its non-executive counterparts. And

compliance should not be the driving force for change; this has the potential to simply add layers of complexity while shifting the focus away from performance, efficiency and ultimately good governance.

Bringing about such momentous change will not be easy, however, it is better to act now as the complexity of convergence will only be that much greater two or three years time.



# KPMG

## Creating a more certain future

The past 18 months have challenged much accepted business wisdom, forcing many companies to reassess how they operate. The regulatory and business environment has caused a fundamental change in organizational culture, governance and risk management as leaders seek greater certainty and assurance to give their businesses more resilience.

Management is being asked to improve the way it oversees its operations and provide greater transparency to stakeholders, while simultaneously driving performance and profitability. The current model for GRC fails to meet

such needs, having become distended and over-complex. In the worst case this can give leaders a false sense of security and a limited ability to control risks.

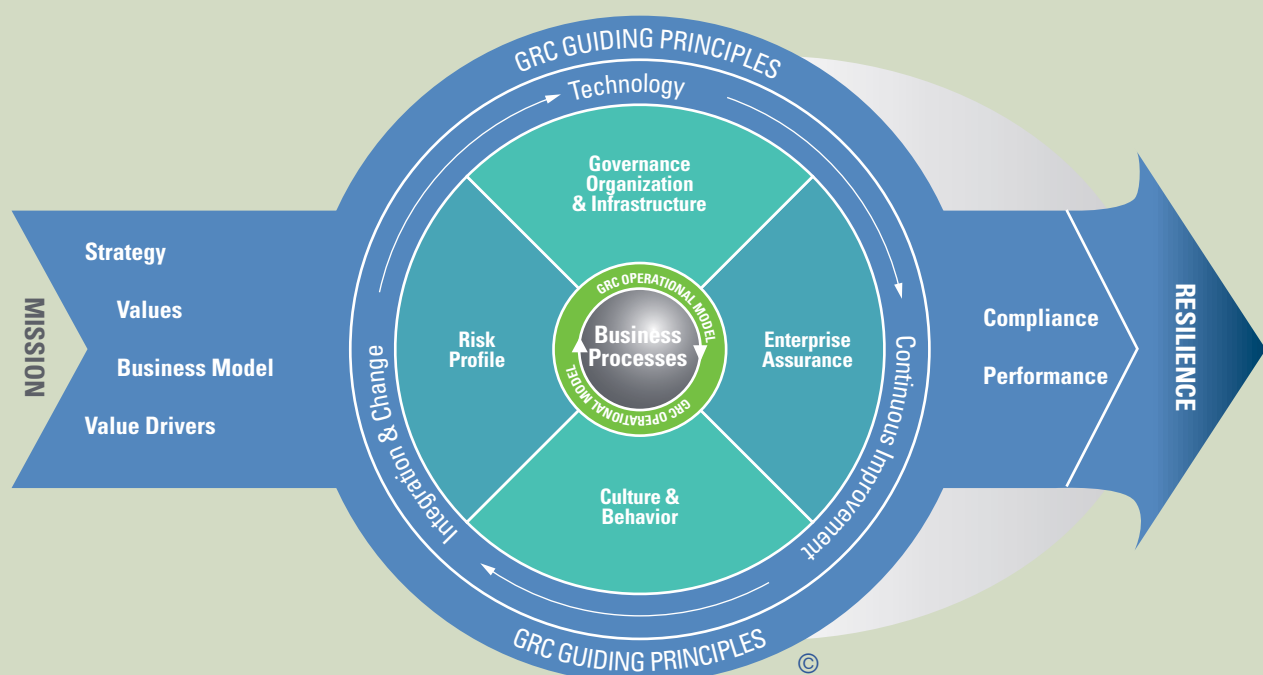
Rather than treat each GRC initiative in isolation, organizations should connect business strategy with governance and risk management, with a renewed focus on performance and efficiency, out of which compliance should fall naturally.

By establishing a clear risk appetite, along with global standards of behavior, companies can create a culture and an infrastructure that supports risk management and governance – and gives

assurance that risks are being managed appropriately. Although it is important to set the tone from above, integrating governance, risk and compliance requires involvement and commitment at all levels to maintain momentum during what can be a lengthy process.

With the right GRC model in place, leaders should get the information they need to understand and respond to the risks facing the business, as well as anticipating and meeting changing stakeholder and regulatory demands. The result is an increasingly resilient, informed and performance-oriented organization that can thrive amidst the uncertainty.

### KPMG's GRC Holistic Model



Source: KPMG International 2009

### Making it happen: KPMG's holistic model

Although the survey suggests that there is a genuine willingness to achieve GRC convergence, many organizations are uncertain where to begin. The framework opposite is designed to provide a clear structure for aligning risk management and compliance activities with governance efforts, organizational culture, and assurance and reporting.

The first step is to link GRC with the mission of the organization, which is in turn translated into strategic objectives including:

- **Strategy:** What do we want to achieve?
- **Values:** What do we stand for?
- **Business model:** How do we organize?
- **Value drivers:** What factors are influencing organizational success?

The **business processes** are at the core of the organization and the holistic model. These processes should have strong controls and reporting capabilities. Surrounding the business processes is the **GRC operational model**, the layer at which the governance, risk management, and compliance management is put into practice to drive enterprise assurance.

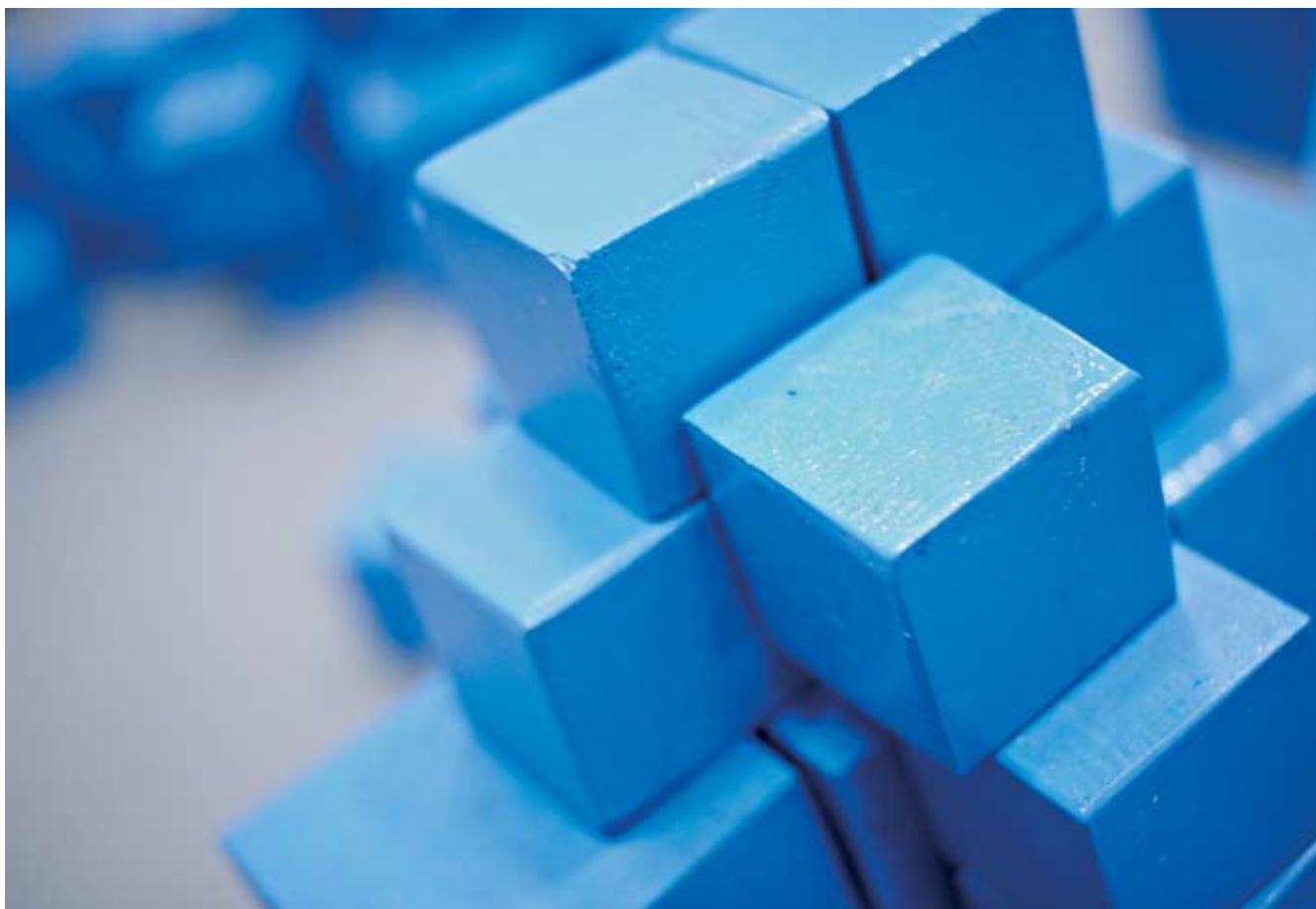
Surrounding the business processes (and the GRC operational model) are four key components that must be in balance to enable resilience.

- **Risk profile:** understanding and quantifying risks facing the organization
- **Culture and behavior:** embedding risk management within everyday behavior
- **Governance, organization and infrastructure:** giving oversight on business processes and decision-making

- **Enterprise assurance:** evaluating, monitoring, and reporting on the effectiveness of controls

When the various elements of the model are working in harmony, an organization should achieve the necessary compliance and continuously improve performance, helping it move towards the goal of resilience, which puts it in a strong position to be able to deal with ongoing change and adapt quickly to unforeseen circumstances.



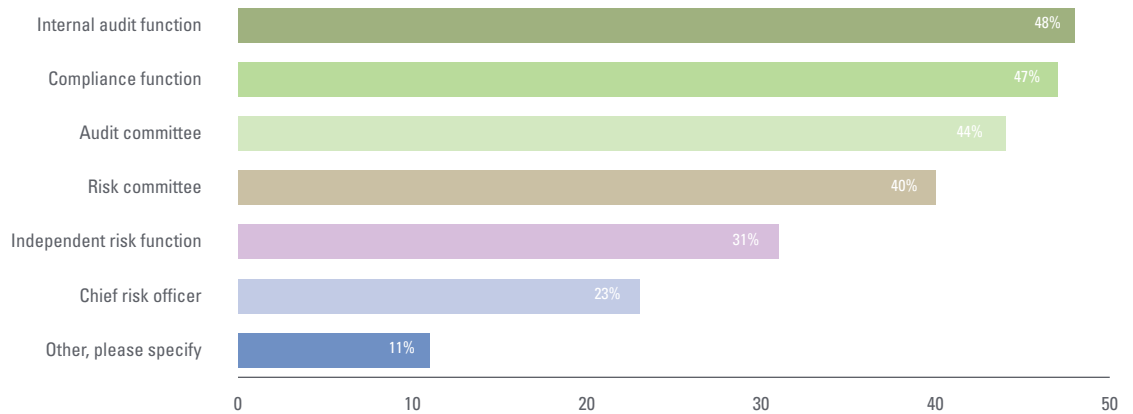


The research on which this report is based was conducted by the Economist Intelligence Unit in 2009. The senior executives who responded to the survey were drawn from a cross-section of industries and all respondents have influence over or responsibility for strategic decisions on risk management. More than one half of respondents are C-level or board-level executives.

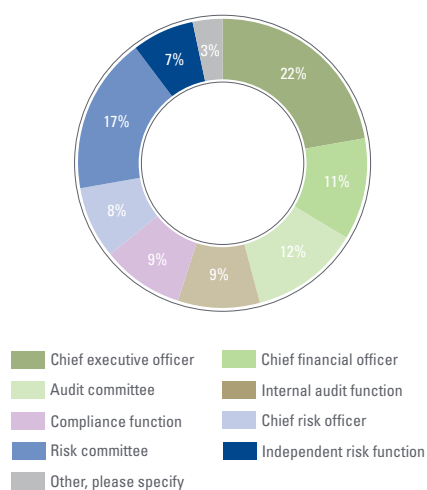
# Appendix

## Survey results

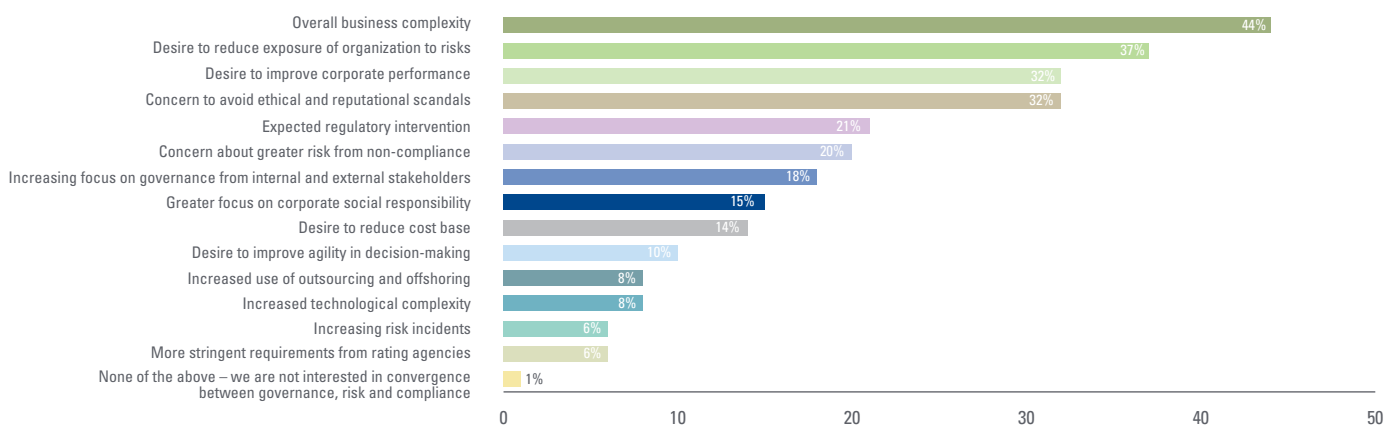
1. Which of the following roles, risk functions and committees do you have in place, formally, in your company? Select all that apply.



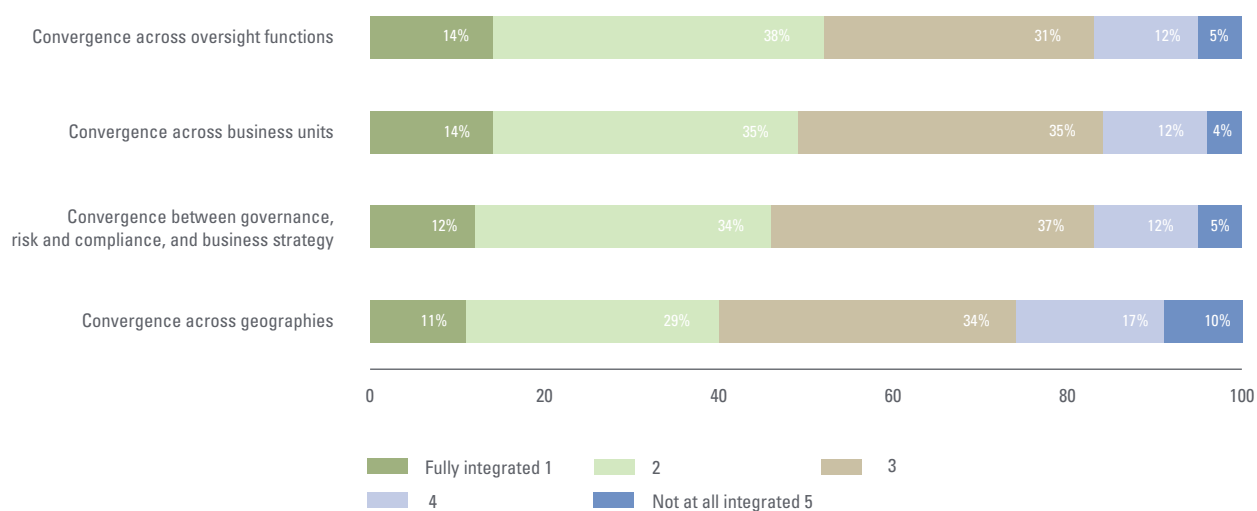
2. Which of the following risk functions or committees has the lead role in implementing or overseeing the organisation's governance, risk, and compliance efforts?



3. Which of the following factors are influencing your organisation's interest in the convergence of governance, risk and compliance? Select up to three.

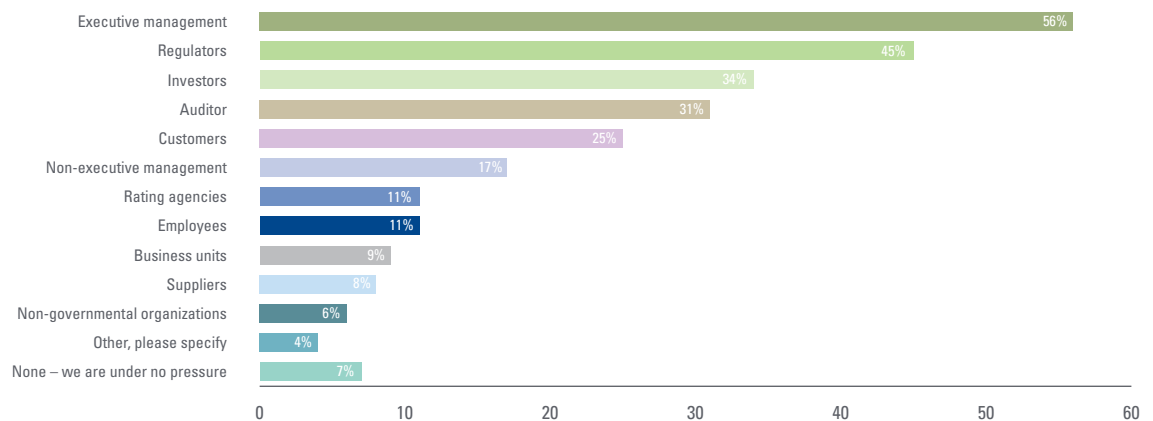


4. How would you rate the degree of convergence between governance, risk and compliance across the following entities in your organization? Please rate 1 to 5 where 1 is fully integrated and 5 is not at all integrated.

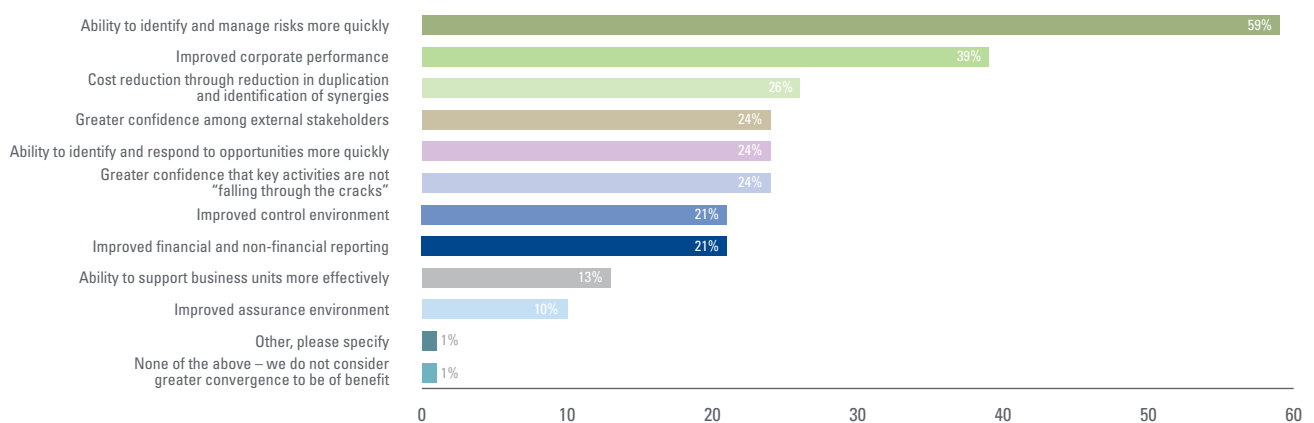




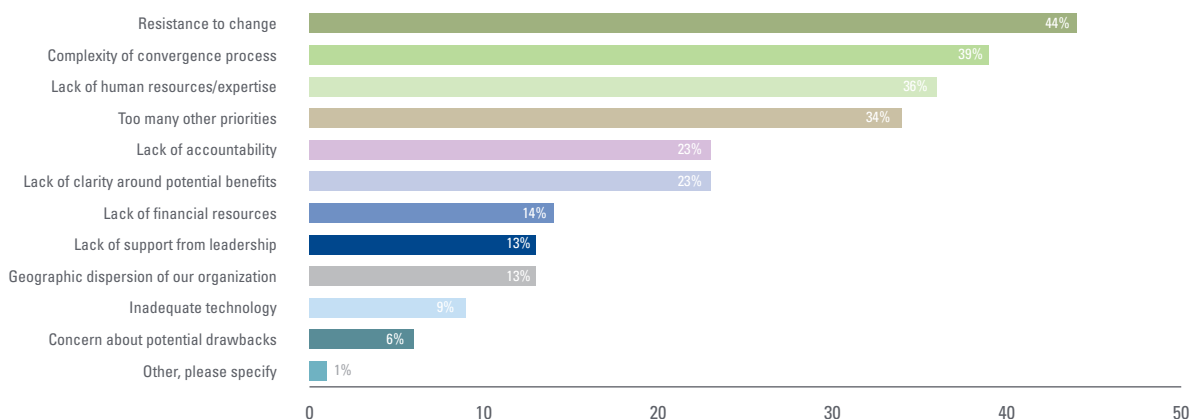
5. Which of the following stakeholders are exerting pressure on your organization to improve its convergence of governance, risk and compliance functions? Please select all that apply.



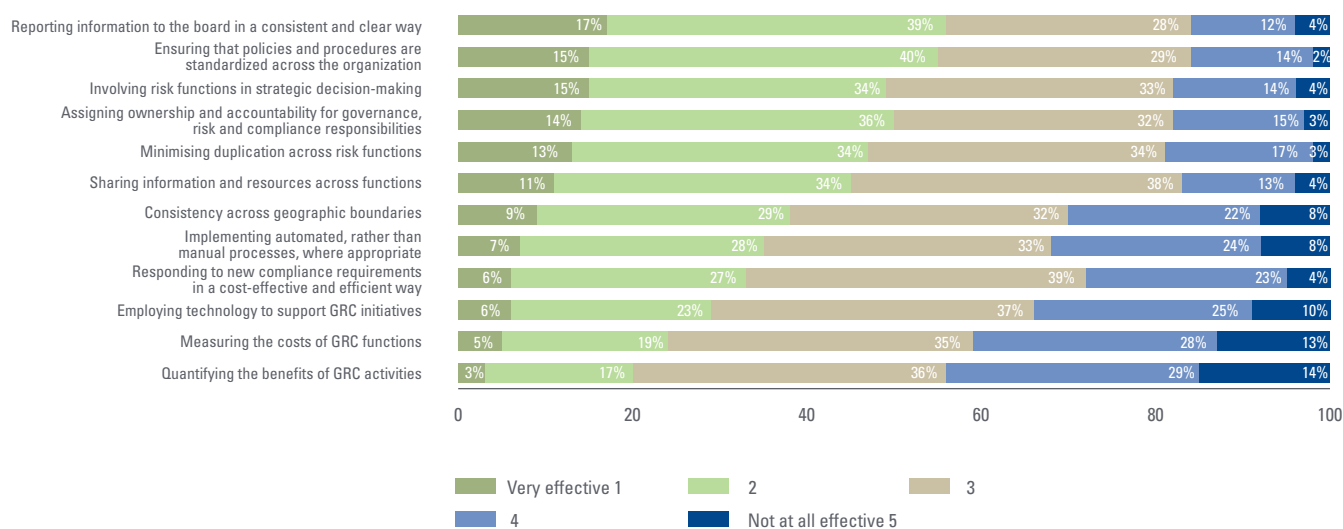
6. What do you consider to be the main benefits of better convergence between governance, risk and compliance functions? Select up to three.



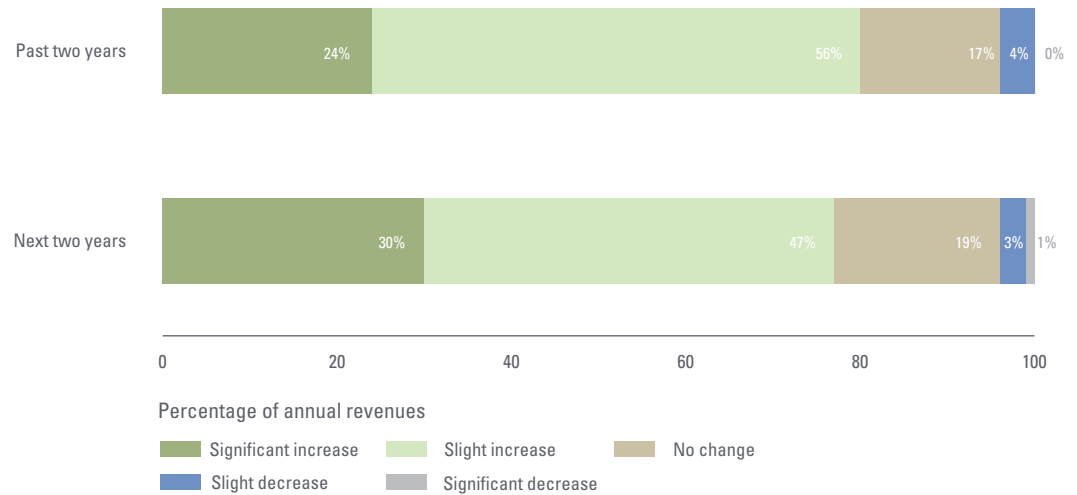
7. Which of the following do you consider to be the most significant barriers to greater convergence of governance, risk and compliance? Select up to three.



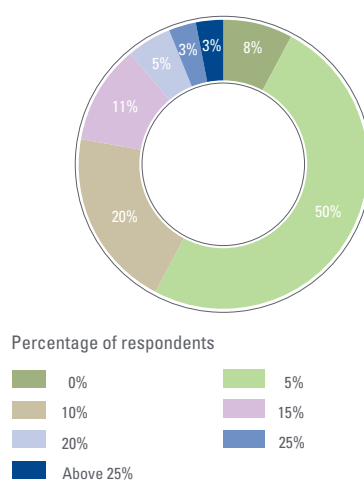
8. How would you rate the effectiveness of your organization at managing the following aspects of governance, risk and compliance? Please rate 1 to 5 where 1 is very effective and 5 is not at all effective.



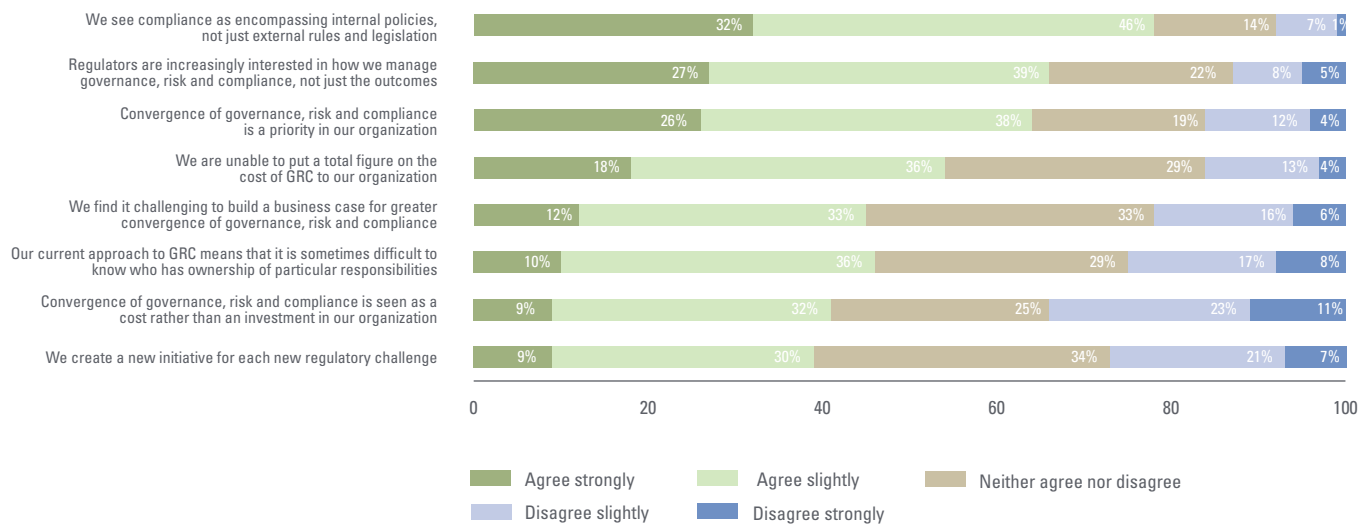
9. What change has there been to the cost of your governance, risk and compliance efforts over the past two years, and what change do you expect over the next two years?



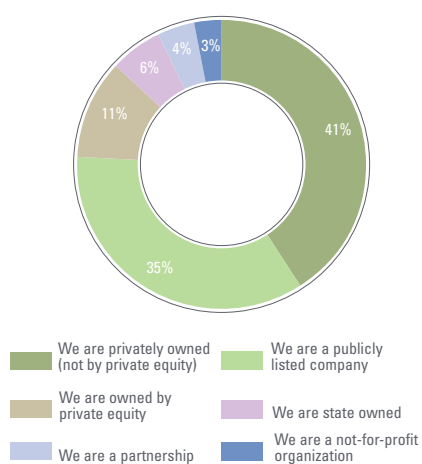
10. Please estimate the annual cost of your overall governance, risk and compliance activities as a percentage of your annual revenues.



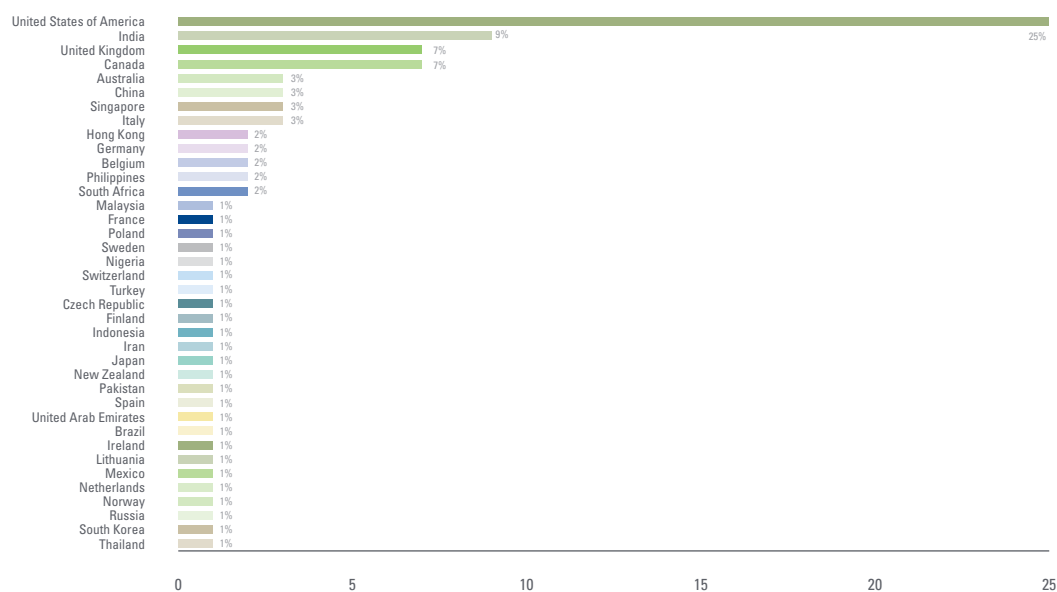
### 11. Please indicate whether you agree or disagree with the following statements.



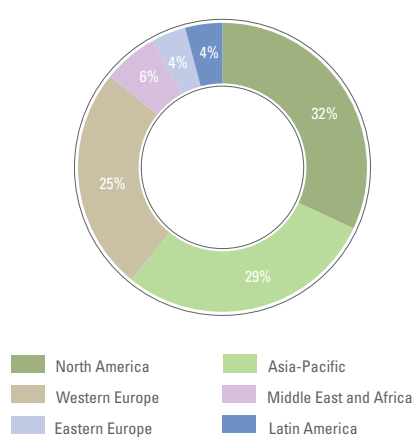
### 12. Which of the following best describes the ownership of your company?



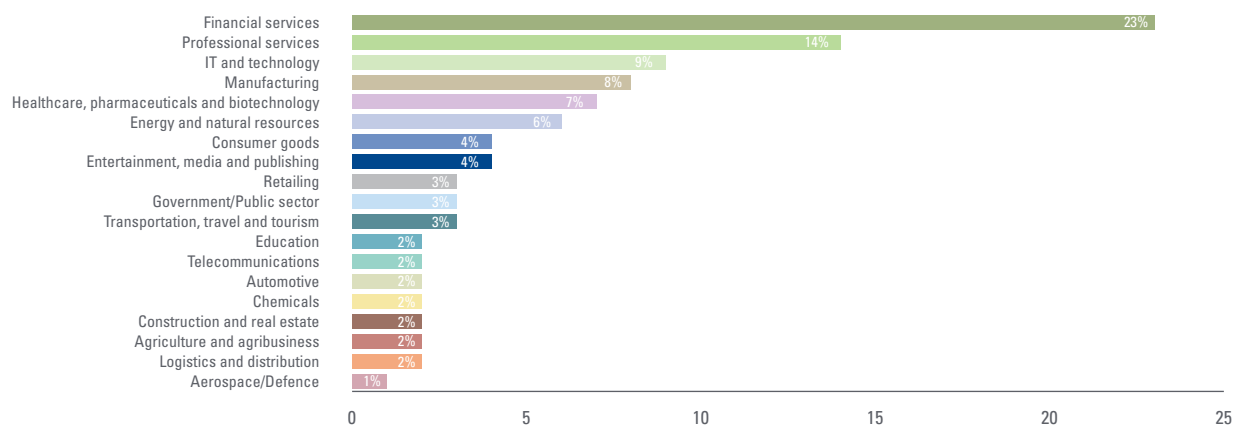
### 13. In which country are you personally located?



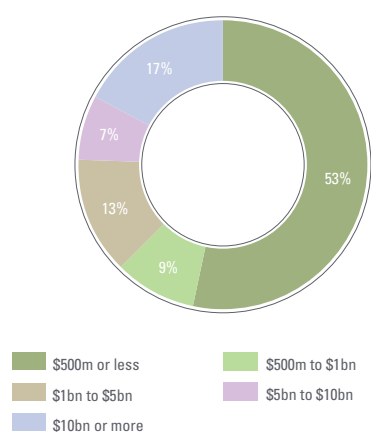
### 14. In which region are you personally based?



## 15. What is your primary industry?

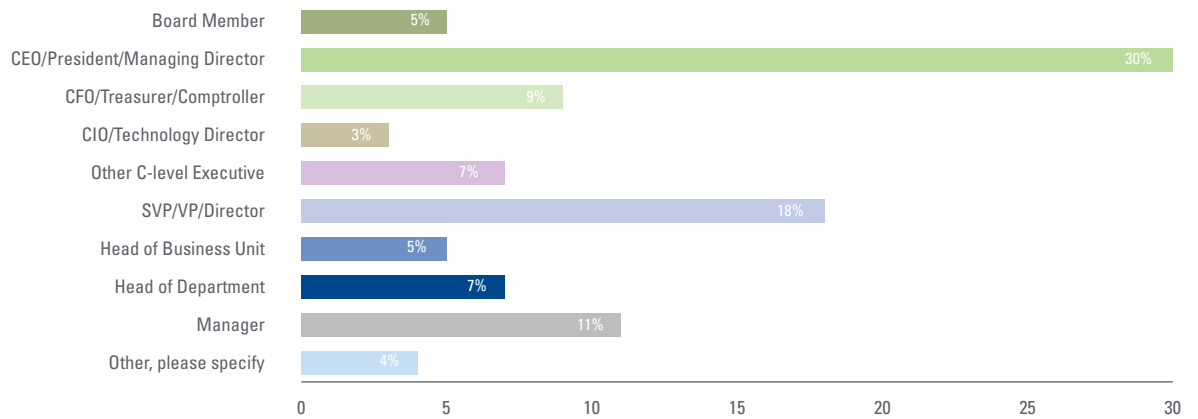


## 16. What are your company's annual global revenues in US dollars?





### 17. What is your title?







## Authors

### Oliver Engels

KPMG in the UK  
European Head of Governance,  
Risk & Compliance  
Tel. +49 69 9587 1777  
oengels@kpmg.com

### Simon Evans

KPMG in the UK  
Director, Risk & Compliance  
Tel. +44 207 311 8790  
simon.db.evans@kpmg.co.uk

## Additional key contacts:

### KPMG in Americas region

#### John Farrell

Tel. +1 212 872 3047  
johnmichaelfarrell@kpmg.com

#### Mike Nolan

Tel. +1 713 319 2802  
mjnolan@kpmg.com

#### Tony Torchia

Tel. +1 412 232 1629  
atorchia@kpmg.com

### KPMG in Asia Pacific region

#### Sally Freeman

Tel. +61 3 9288 5389  
sallyfreeman@kpmg.com.au

#### Michael Lai

Tel. +86 21 2212 2730  
michael.lai@kpmg.com.cn

#### Stephen Lee

Tel. +852 2826 7267  
stephen.lee@kpmg.com.hk

### KPMG in Europe, Middle East & Africa

#### Steven Briers

Tel. +27 11 647 5673  
steven.briers@kpmg.co.za

#### Peter Paul Brouwers

+31 402 502 325  
brouwers.peterpaul@kpmg.nl

#### Oliver Engels

Tel. +49 69 9587 1777  
oengels@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the survey respondents and do not necessarily represent the views and opinions of KPMG International or KPMG member firms.

© 2010 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. Printed in the United Kingdom.

KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative ("KPMG International"), a Swiss entity.

Designed and produced by KPMG LLP (UK)'s Design Services

Publication name: The convergence challenge

Publication number: RRD-171343

Publication date: February 2010

Printed on recycled material.