Economist Intelligence Unit

The Economist

Governance, risk and compliance in financial services

A briefing paper from the Economist Intelligence Unit sponsored by Oracle

Preface

Governance, risk and compliance in financial services is an Economist Intelligence Unit briefing paper, sponsored by Oracle. The Economist Intelligence Unit executed the survey, conducted the analysis and wrote the report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

Research for the report was conducted in February 2008. The Economist Intelligence Unit surveyed 167 executives from the financial services industry worldwide using an online questionnaire. To supplement the survey results, the Economist Intelligence Unit also conducted in-depth interviews with senior executives on how they approach the challenges of governance, risk and compliance.

June 2008

Executive summary

Among the hard-won lessons of the global credit crisis is the importance of a consistent—and consistently enforced—set of governance, risk and compliance policies. Consistency is no guarantee against loss; as Warren Buffett has noted, bankers who act like lemmings are likely to experience a lemming-like fate.[1] But at the very least, an integrated governance, risk and compliance programme promotes a common language and understanding of risk and discourages the development of siloed oversight functions that operate in isolation from the business.

To learn more about this issue, the Economist Intelligence Unit conducted a study, sponsored by Oracle, including a comprehensive global online survey and one-on-one interviews with a series of senior governance, risk and compliance executives. The principal findings are as follows:

■ **Independent yet overlapping control functions hinder a comprehensive understanding of risk.** In financial services institutions, governance, risk and compliance activities are typically spread across multiple overlapping and related functions such as audit, compliance, finance, IT, operations and legal. Each operates somewhat independently, leading to inconsistent and inefficient processes. But the bigger problem is that each silo reports to senior management independently, impeding a comprehensive understanding of risk.

■ **Institutions that invest in governance, risk and compliance are more likely to integrate pricing and risk.** Risk-adjusted pricing is fine in theory; in practice, the desire to win business often triumphs, even in volatile and risky markets. The more progress institutions had made in integrating governance, risk and compliance, the more likely they were to have increased product prices to offset higher risk during the credit crisis, according to the survey results.

■ **Equity investors recognise the importance of governance, risk and compliance.** Organisations with programmes to integrate governance, risk and compliance are less likely to have suffered significant stock price declines during the recent credit crisis, according to the survey.

■ **Organisations that fail to integrate governance, risk and compliance are often the ones that need it most.** Survey respondents were asked whether their institutions strike a balance between risk and opportunity or are overly biased towards one or the other. The firms that have not taken steps to integrate governance, risk and compliance tend also to be those focused on the pursuit of new business to the exclusion of risk control.

■ **These same organisations tend to exhibit other dysfunctional behaviour.** Respondents from firms that have not taken steps to integrate governance, risk and compliance are more likely to agree with statements like "My organisation's policies and objectives exist only as a formality—they do not reflect how the organisation is run in practice," and to say that the firm's risk and compliance policies are not well understood throughout the organisation.

[1] "In their lending, many bankers played follow-the-leader with lemming-like zeal; now they are experiencing a lemming-like fate." *Berkshire Hathaway annual letter to shareholders*, 1990. (http://www.berkshirehathaway.com/letters/1990.html)

Introduction

A foolish consistency, said Ralph Waldo Emerson, an American essayist and poet, is the hobgoblin of little minds. But there is nothing foolish about working to implement consistent policies across an organisation. Indeed, at a highly leveraged financial institution—where a small loss may wipe out a large chunk of capital—a consistent and integrated set of risk policies may mean the difference between prosperity and insolvency.

This, in a nutshell, is the rationale behind the growing interest in governance, risk and compliance—a phrase that refers to the entire set of processes, policies and activities around risk management, broadly defined (see "Governance, risk and compliance defined" on page 5). The integration of governance, risk and compliance activities is particularly important in the financial services industry. There are several reasons:

- Financial services institutions play a key role in the health of the global economy. They are counterparties to vast numbers of transactions, and their ability to maintain sufficient capital to offset risk is of interest to the general public, not just the more narrow community of shareholders, management and employees.

- Like all corporate stewards, financial services executives face the challenge of generating steadily rising earnings. But financial services firms must do it in an environment more fraught with risk: volatile financial markets, operationally complex systems and commodity-type products with narrow margins.

- The global credit crisis has driven investors to make sharper distinctions between well-managed firms that balance opportunity and risk and those that pursue opportunity at the expense of risk. Shareholders have suffered both from declining share prices and the dilutive effect of capital infusions into institutions such as UBS, Citigroup, Merrill Lynch, Lehman Brothers and Wachovia.

All of this argues for special attention to governance, risk and compliance activities within

Who took the survey?

In February 2008 the Economist Intelligence Unit conducted an online survey of 167 executives worldwide to determine how they approach the challenges of governance, risk and compliance. Of the respondents to the survey, 51% were senior executives (board-level or C-level), and 49% were directors, business unit heads and other managers. Worldwide, 30% of respondents were based in North America, 23% in Western Europe, 30% in the Asia-Pacific region, and 17% from Latin America, Eastern Europe, the Middle East and Africa. More than one-half of the respondents (52%) worked at organisations with global assets of more than US$50bn. All respondents were in the financial services industry. In addition to the survey, qualitative interviews were conducted with senior executives familiar with governance, risk and compliance.

financial services institutions. The problem with these activities now is not that any single activity is flawed; it is that different activities have grown up independently, and information gathering is not harmonised or standardised across governance, risk management, compliance and internal control systems.

"Information is reported upwards in a fragmented way," says Dan McKinney, a partner at Ernst & Young's Risk Advisory Services. "Boards and risk committees are concerned they're getting individual reports from each silo," he says. "They're wanting a more comprehensive view of risk."

Few executives would disagree with this objective in theory. And yet many of the managers involved in governance, risk and compliance fail to interact with each other. Each remains in his or her own functional silo, with its own terminology, technology and processes. The advantage is efficiency within each silo; the disadvantage is duplication and inefficiency across the organisation, as well as the failure of senior management to gain the comprehensive view of risk that can emerge when information is prepared and shared using a consistent methodology.

"Boards and risk committees are concerned they're getting individual reports from each silo. They're wanting a more comprehensive view of risk."

Dan McKinney, partner, risk advisory services, Ernst & Young

Governance, risk and compliance defined

Governance, risk and compliance (GRC) has become a well-known phrase in the financial services industry, with over 400,000 references on Google (many from the sites of consulting and IT firms). The term refers to multiple overlapping activities dealing with risk and compliance, including:

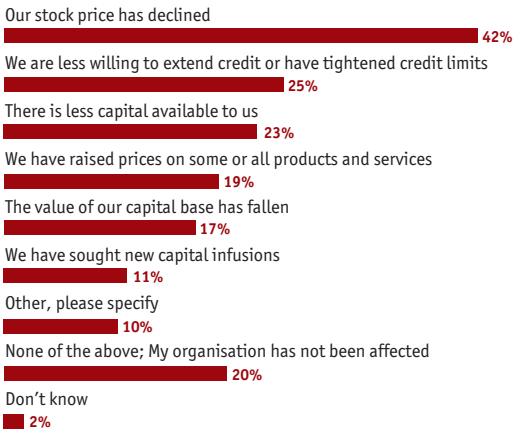
- Risk governance;
- Financial, operational and IT risk management;
- Audit and control activities;
- Compliance efforts; and
- All of the policies, processes, documentation and IT infrastructure associated with the above.

Proponents of an integrated governance, risk and compliance strategy suggest that all of these elements should be linked in order to bring together information relevant to risk management (broadly defined). This will eventually enable a more comprehensive and transparent view of risk across an organisation than exists today, including the ability to report on effectiveness of governance and risk policies and track and enforce compliance within lines of business. ■

Balancing risk and opportunity

Turmoil is often a catalyst for change. "Any time there's a major dislocation, as there is now, there's a large opportunity to learn," comments Kevin Blakely, president of the US-based Risk Management Association, which has 3,000 members in the financial services industry. "It helps financial services firms to come out a bit smarter."

How has your organisation been affected by the credit crisis and associated market turmoil? (Select all that apply)



"There are many lessons to be taken away from the crisis," says Teo Swee Lian, deputy managing director at the Monetary Authority of Singapore (the central bank). "These include the over-reliance of financial institutions on external ratings, [the need for] better oversight of banks' off-balance-sheet exposures, the regulatory treatment of these exposures and the need to strengthen stress testing in financial institutions."

One positive outcome of the recent bout of asset price volatility is that it has exposed weaknesses in the risk governance of financial institutions. A proper governance policy defines the organisation's risk profile, lays out a process for evaluating and prioritising risks, and ensures that the process is followed.

How the oversight is structured—for instance, whether it resides in the audit committee or the board of directors—appears to be less important than expertise, resources and engagement. According to a 2008 study by RiskMetrics, for instance, Goldman Sachs was relatively untouched by the credit crisis despite the fact that its governance infrastructure is similar to that of other banks.[2] What is significant, suggests the study, is the intellectual firepower on Goldman's audit committee (where risk oversight resides) and that Goldman "ascribes as much status, prestige and pay to people engaged in control functions as to those running businesses"—to the extent that employees are forced to rotate between risk control and business operations.

In other words, Goldman has actively tried to prevent the common rift between those focused on risk and those focused on the business. When a schism opens between these two groups—and when the people running businesses have more "status, prestige and pay" than those charged with controlling risk—the stage is often set for a breakdown in the checks and balances that allow institutions to pursue new business without taking on undue risk. It is this kind of breakdown that an integrated system of governance, risk and compliance activities is intended to avoid.

[2] RiskMetrics Group, *Credit Crisis and Corporate Governance Implications: Guidance for Proxy Season and Insight into Best Practices,* April 2008.

The case for integration is bolstered by a report[3] by financial regulators from France, Germany, Switzerland, the UK and the US, which assesses risk management practices in the light of the credit crisis. The report shows that "siloed" firms in some cases "left different business areas to make decisions in isolation and in ignorance of other areas' insights". One result was that, although some business line managers recognised that underwriting standards for some products were loosening, other business line managers did not. Instead, they continued to add to the warehouse of assets whose credit quality was probably deteriorating.

The report also found that "senior managers at firms that experienced more significant unexpected losses tolerated a more segregated approach to internal communications about risk management". Moreover, firms that avoided significant losses tended to be those where risk management not only had independence and authority within the organisation but also where there was "considerable direct interaction with senior business managers".

"Any time there's a major dislocation, as there is now, there's a large opportunity to learn."

Kevin Blakeley, president, Risk Management Association

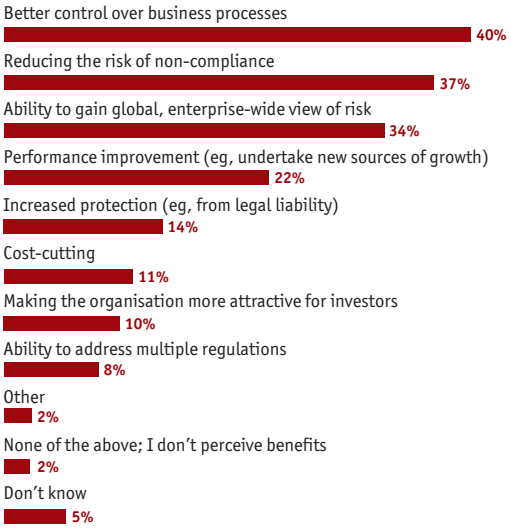
[3] Senior Supervisors Group, *Observations on Risk Management Practices during the Recent Market Turbulence*, March 2008.

Motives for integration

Executives see the biggest benefits of integrating governance, risk and compliance first in terms of gaining better control over business processes and, second, in reducing the risk of non-compliance. Dan Chelly, head of operational risk at Groupe Caisse d'Epargne, a French bank, says that as organisations such as his expand operations further into foreign markets, they have to deal not only with new regulations but also "specifically the weight of liability in some countries". An integrated approach to risk becomes all the more important. It is critical, for example, to be able to handle national governance regulations properly and avoid damaging instances such as class actions. Mr Chelly believes that the main factors for international risk strategies are to set up the same basic language and risk culture—"the core principles". It is also important to share the same risk management tool, and to listen to local managers as they try to adapt core principles to their area.

The ability to gain a global, enterprise-wide view of risk is seen as significant by more than one-third of survey respondents. As many as 22% rate performance improvement—for example, putting the firm in a better position to undertake new sources of growth—as a key benefit. Lower down the list are

What do you regard as the biggest benefits of integrating GRC at your organisation? (Select up to two)



the benefits of increased protection and cost-cutting. Only one in ten respondents believes that integrating governance, risk and compliance makes the organisation more attractive for investors.

Progress in integration

The survey shows that 27% of the 167 respondents at financial services firms are either in the final stages of integrating governance, risk and compliance or are already completely integrated. A total of 66% of firms are either "somewhat integrated" or are at the starting phase of integration—setting up steering committees and working out how they can leverage a more unified effort.

However, these figures are more revealing when they are viewed in the light of the organisation's risk profile—how much risk it chooses to take on—and its sophistication around risk management activities. For instance, firms that are "not at all integrated" or "starting to integrate" are:

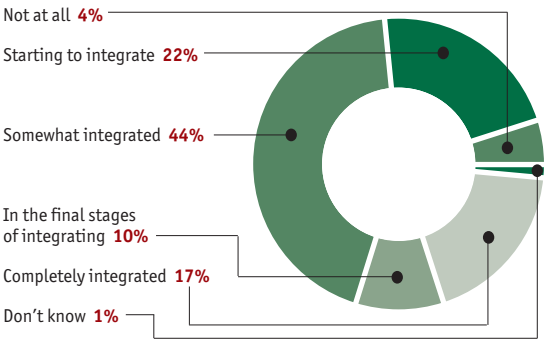
- Twice as likely to be focused on the pursuit of new business rather than control of risk;
- 50% more likely to say that their organisation's "policies and objectives exist only as a formality—they do not reflect how the organisation is run in practice";
- Four times as likely to say that their organisation's risk management policies are "less advanced than those of our peers"; and
- Over five times as likely to say that their organisation's policies on risk management are

poorly or very poorly understood throughout the organisation.

There is a difference in risk awareness as well. According to the survey, all banks judge financial risks as most important. But those that have integrated governance, risk and compliance appear to be more aware of operational and compliance risk than their peers. In other words, they take a more balanced and holistic approach to risk management.

Of course, many of the organisations that are just starting on the road to integration are well managed and cognisant of risk. However, for a disproportionate number, the failure to move ahead is part of a pattern of giving insufficient attention to risk management. It would seem that many of the organisations failing to integrate governance, risk and compliance are those that need it most.

Has your organisation integrated its governance, risk and compliance processes? (% respondents)



Ways to foster integration

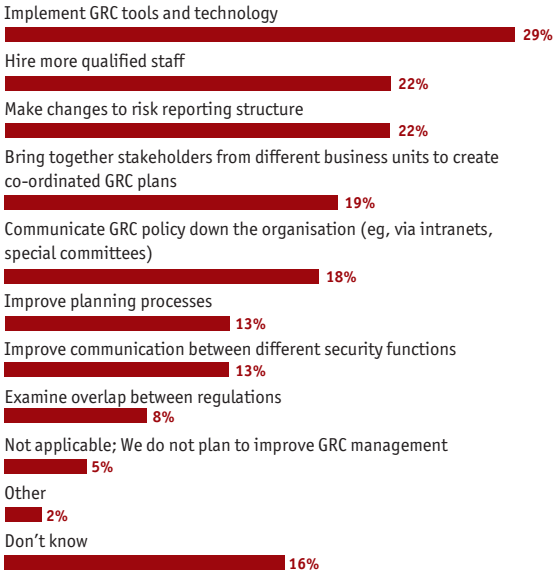
Organisations are planning multiple ways to improve the management of governance, risk and compliance over the next three years. Executives in the survey have as their first priority implementing tools and technology. Hiring more qualified staff and making changes to risk reporting structures come an equal second after implementing tools and technology, and many plan to bring together stakeholders from different business units to create co-ordinated governance, risk and compliance plans. Mr Blakely believes that organisations should go a step further and give incentives for risk. "We're not incentivising people properly," he says.

Some firms intend to communicate governance, risk and compliance policy down the organisation by a variety of means such as intranets and special committees. A few plan to bolster governance, risk and compliance either by improving planning processes or communication between different security functions, or again by examining overlap between regulations.

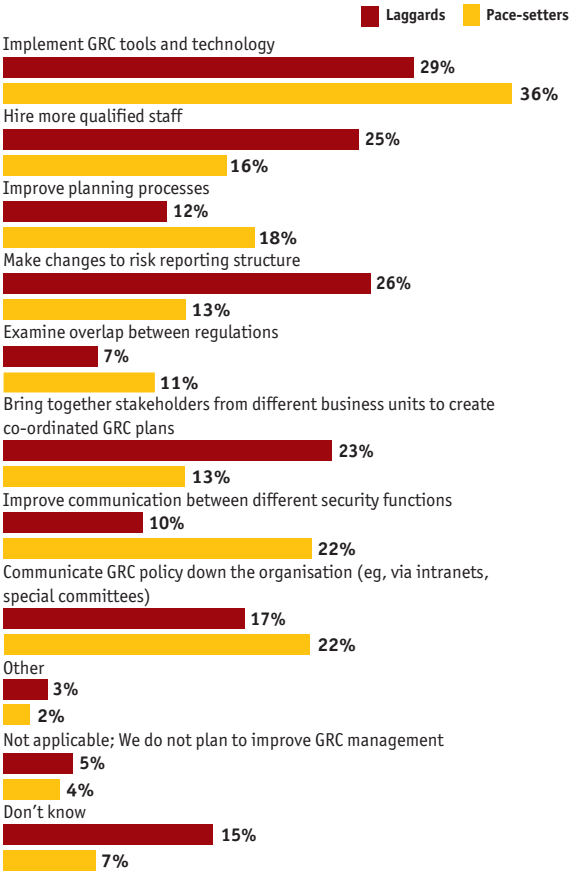
How to communicate governance, risk and compliance itself is also crucial. Jorge Soeiro Marques, chief risk officer of Lusitania Companhia de Seguros, a Portuguese insurance firm that is currently implementing a governance, risk and compliance programme, comments: "We need to transmit to the whole organisation the changes in how we manage investment, claims and con-

tracts with clients, and how we face competitors. It's not easy to communicate this to front-office staff. They need to understand the meaning of risk, and know that each decision they take is important."

How does your organisation plan to improve GRC management in the next three years? (Select up to two)



How do the "laggards" vs the "pace-setters" at your organisation plan to improve GRC management in the next three years?



The goal of data consistency

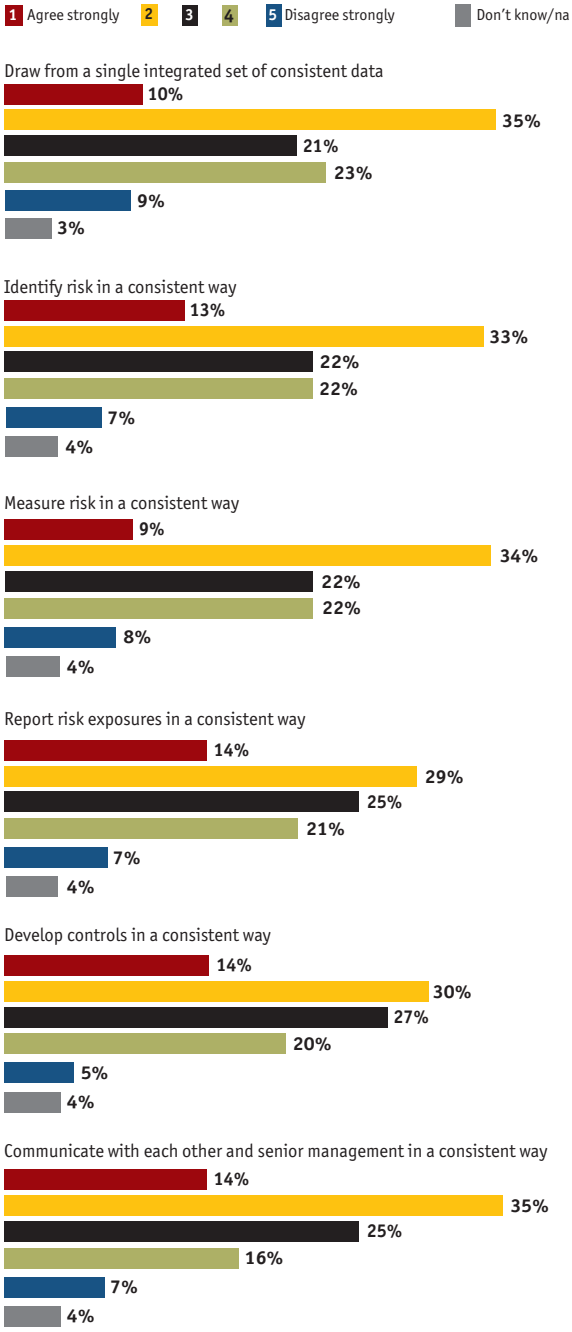
Financial services firms are thus moving towards a more consistent approach to data gathering and presentation. Across their organisation, 45% of executives either agree or agree strongly that compliance and risk managers draw from a single integrated set of consistent data, and a similar proportion believe that they not only identify and measure risk consistently, but also report risk exposures. Firms less advanced in integrating governance, risk and compliance are more likely to have inconsistent data residing in different parts of the organisation.

Fewer than one-half of financial institutions believe their risk and compliance managers develop

controls in a consistent way, and the same goes for the way they communicate with each other and senior management. By contrast, many still have a long way to go in terms of alignment: 29% say that their firm does not identify risk in a consistent way. Firms whose policies and objectives on risk and compliance are less understood throughout the organisation also identify risk less consistently.

Of the organisations that have not embarked on integrating governance, risk and compliance, not a single respondent could claim a consistent data set. Virtually all agree that multiple concepts of risk are floating around the organisation, and that risk and compliance managers communicate with management in inconsistent ways. These respondents tended to put much greater emphasis on "politics" too when describing the barriers to governance, risk and compliance.

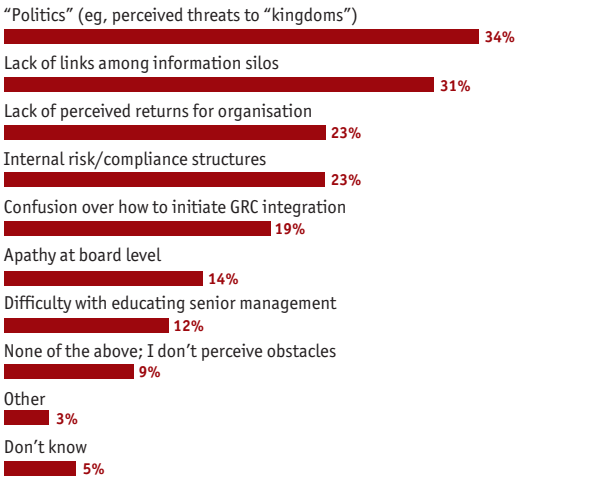
To what extent do you agree or disagree with the following statements? Across my organisation, compliance and risk managers...
(Rate on a scale where 1 = Agree strongly and 5 = Disagree strongly)



Obstacles to integration

It is not apathy at board level or problems with information silos that are the main obstacles to implementing an integrated governance, risk and compliance programme. Usually it comes down to "politics", including perceived threats to "kingdoms". This very human factor is mentioned by 34% of survey respondents as the main hindrance, compared with 31% who say a lack of links among information silos is to blame. Proportionally fewer firms with a strong bias towards risk management versus business opportunity list politics as the main hindrance, however.

What do you think are the main obstacles to implementing an integrated GRC programme in your organisation? (Select up to two)



"Risk reporting gets overwhelming for the board. By focusing on the wrong problem, hundreds of millions of dollars can be lost elsewhere."

Kevin Blakeley, president, Risk Management Association

Doubts about return on investment from the governance, risk and compliance programme get in the way for 23% of respondents, with the same percentage citing existing internal risk/compliance structures. Confusion reigns over how to initiate integration of governance, risk and compliance in just under one-fifth of firms, whereas apathy at board level and difficulty educating senior management each apply to a smaller percentage.

"Risk convergence presents the financial services industry with a major challenge, one that our survey clearly indicates is inevitable. But it also represents a tremendous opportunity," says Mr McKinney. "Those that embark on this journey will be rewarded with a flexible, efficient and sustainable risk management framework that effectively meets not only today's requirements, but those of the future."

There is pressure to use information better, to get the functions working together and to simplify information to make it more useful—that is, be able to present the top ten risks facing the firm. "Risk reporting gets overwhelming for the board," states Mr Blakely. "By focusing on the wrong problem, hundreds of millions of dollars can be lost elsewhere." For instance, in the case of the rogue trader at Société Générale in 2007, fast growth in the equity derivatives business apparently masked a breakdown in control processes.

Furthermore, Mr McKinney believes that as finan-

cial services firms ramp up to deal with Basel II and numerous regulations, as well as disaster recovery and business continuity planning, the end-result is "risk management fatigue". "They're forced to run so many programmes," he says. "Ultimately, businesses feel they're suffocating: filling in numerous forms, testing and so on. They have had to increase budgets and personnel to address the risk and regulatory issues. Now they are seeing the rising costs and are asking, 'How can we integrate risk assessment so we don't repeat processes?' 'How can we consolidate three to five assessment platforms into one?'"

Conclusion

Although their risk systems have helped the vast majority of financial services firms to survive the credit crisis, few would argue against the benefits of integrating governance, risk and compliance. This is especially relevant in the current climate as most firms will see an increase in the level of oversight, requiring additional resources. In addition, many firms will consider moving to a more open governance, risk and compliance environment, away from the "black box" or manual solutions found today.

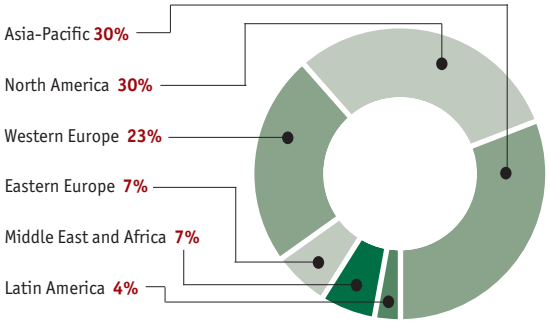
Most experts agree that to gain a firmer understanding of risk across the enterprise, stakeholders should be drawn together from different departments through workshops. This would allow them to define the risk they face, discuss their current approaches to governance, risk and compliance and how to achieve related goals, as well as find out what is required to reach them. Work can then start on setting up a database to analyse risk commonalities and trends within the different business units. Insights on risk exposure will emerge that would not have done so when the information was kept in separate silos.

Not only will a clearer, more comprehensive and realistic view of risk emerge as a result for financial services firms, but much wasted effort will also be removed. That said, no one claims that getting there is an easy feat to pull off. A whole range of hurdles lie ahead—internal power struggles, disconnected information entrenched in silos and worries about return on investment, to name but a few. It is far more likely, however, that better judgements will be made if based on accurate, well-ordered data that boards and risk committees know tell the full story. Besides, all financial services firms have one thing in common, as Mr Blakely says: "They have to be very careful: they're dealing with people's money. If they screw up, it attracts a lot of attention."

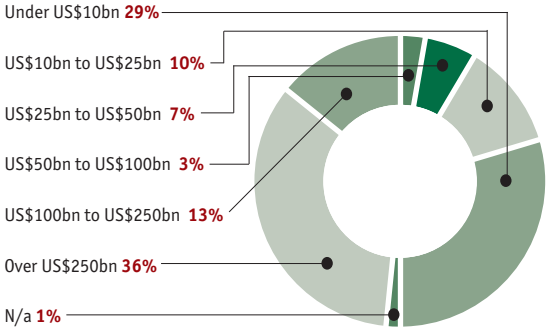
Appendix: Survey results

In February 2008 the Economist Intelligence Unit conducted an online survey of 167 executives worldwide. Please note that not all answers add up to 100% because of rounding or because respondents were able to provide multiple answers to some questions.

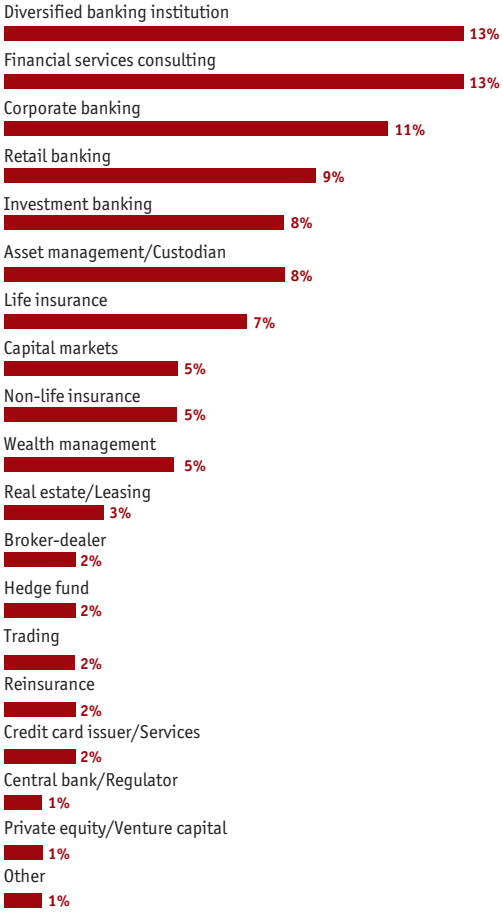
In which region are you personally located?



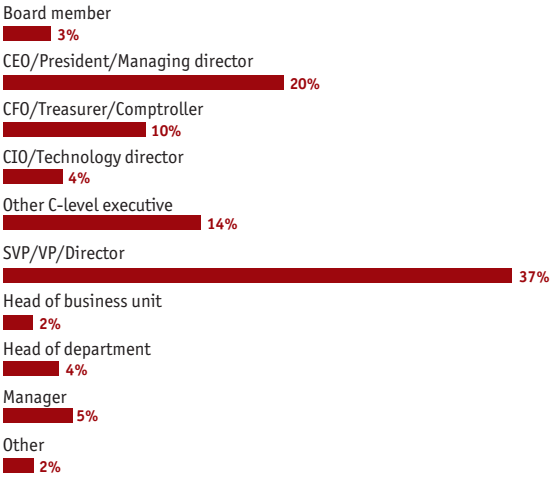
What are your organisation's global assets in US dollars?



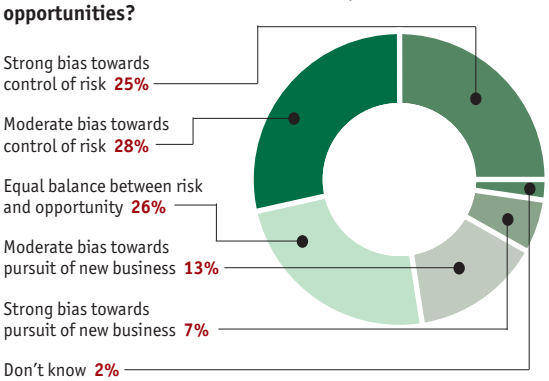
In which subsector of financial services does your organisation operate?



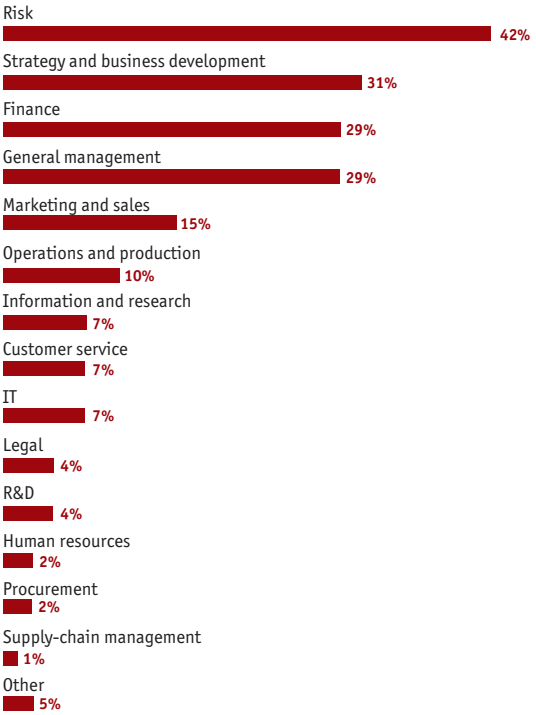
Which of the following best describes your title?



Risk and opportunity are two sides of the same coin. Relative to its peers, is your organisation—taken as a whole—more focused on the control of risk or on the pursuit of new business opportunities?

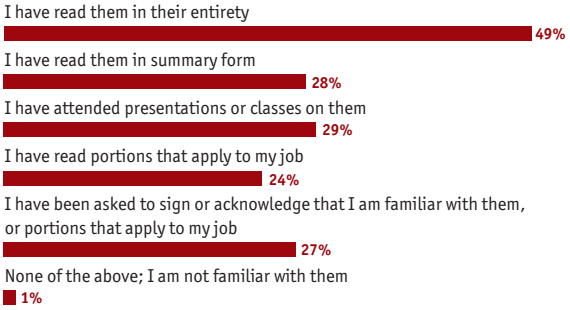


What are your main functional roles? (Please choose no more than three functions)

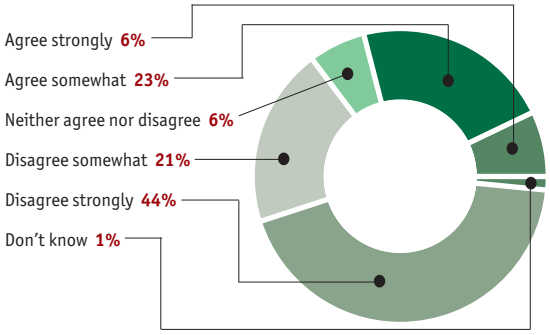


Why do you believe that your organisation has this stance towards risk and opportunity? (Select all that apply)

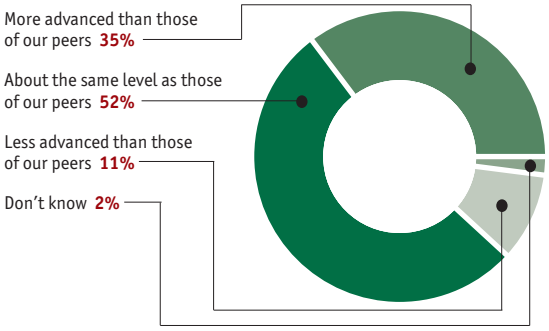
To what extent are you familiar with your organisation's corporate governance policies? (Select all that apply)



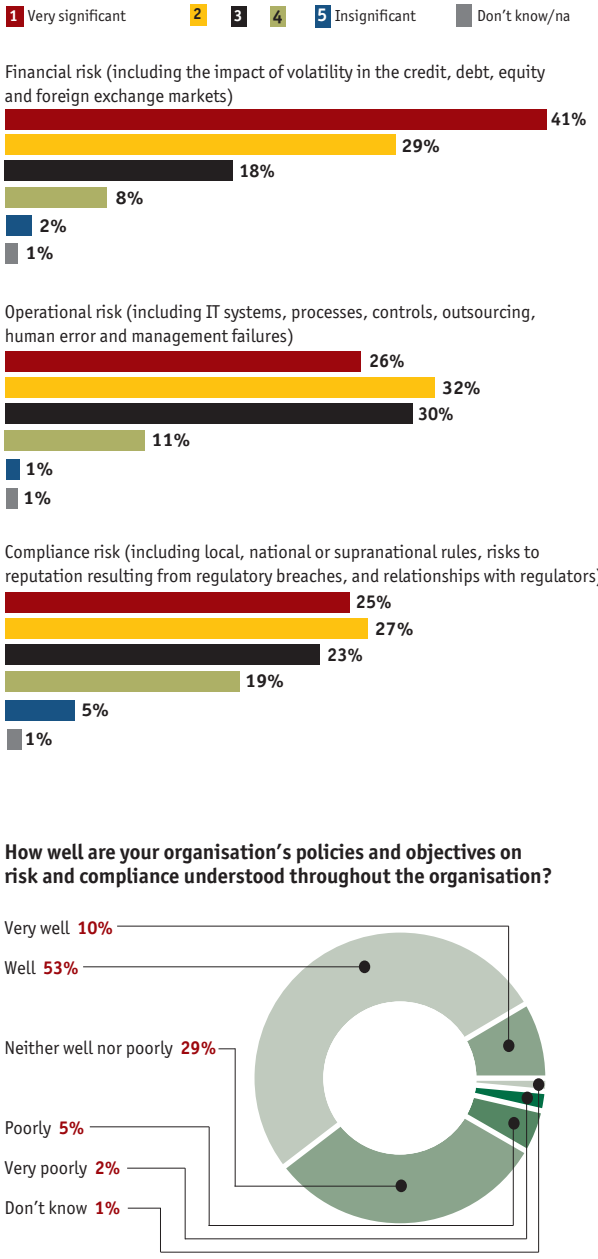
To what extent do you agree with the following statement: My organisation's policies and objectives exist only as a formality—they do not reflect how the organisation is run in practice.



Relative to its peers, how do you think your organisation's risk management capabilities compare?

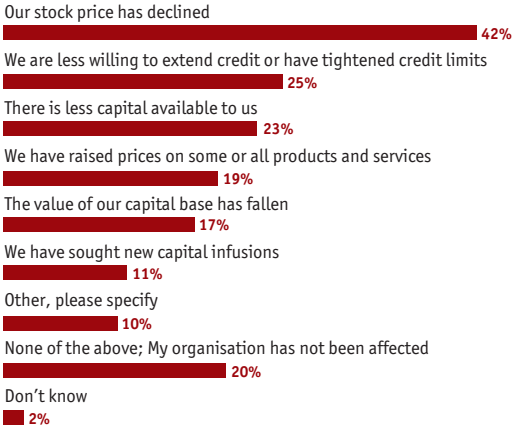


How significant do you consider the following risks to be for your organisation over the next three years? (Rate on a scale of 1 to 5 where 1 = Very significant and 5 = Insignificant)



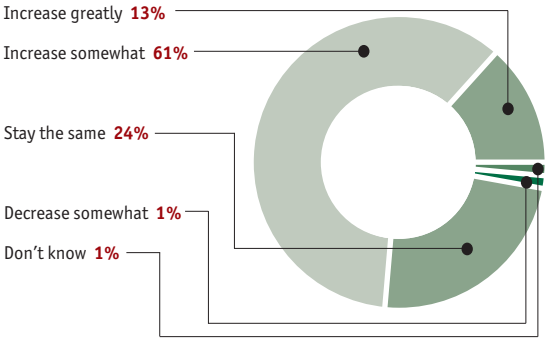
How well are your organisation's policies and objectives on risk and compliance understood throughout the organisation?

How has your organisation been affected by the credit crisis and associated market turmoil? (Select all that apply)

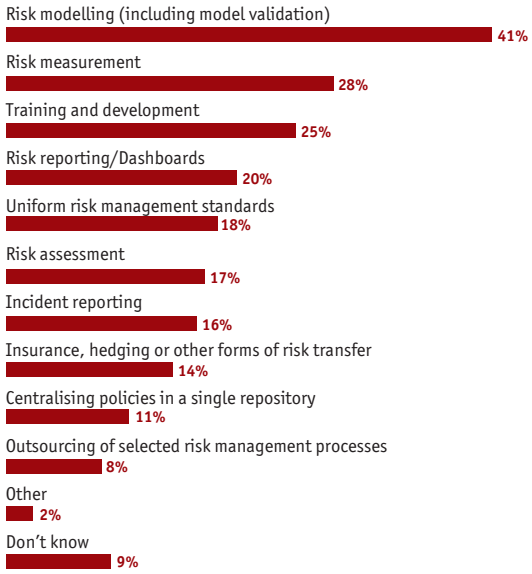


How have your organisation's risk management objectives and activities changed as a result of the credit crisis and associated market turmoil? (Select all that apply)

Compared with the past 12 months, I expect the number of hours my organisation spends on compliance and risk management to:

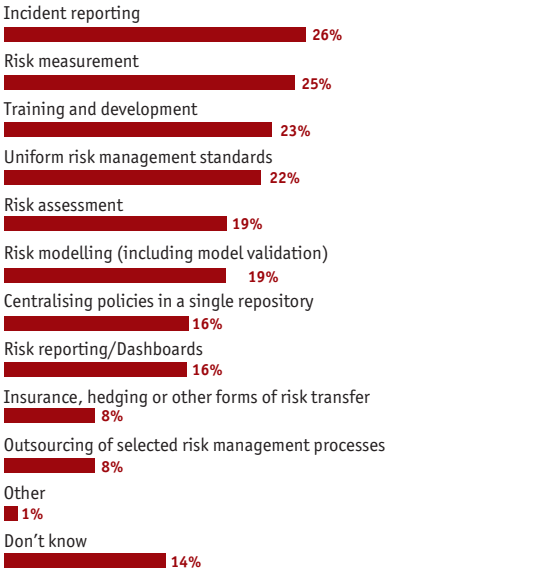


Where do you think your organisation is weakest in managing financial risk? (Select up to three)

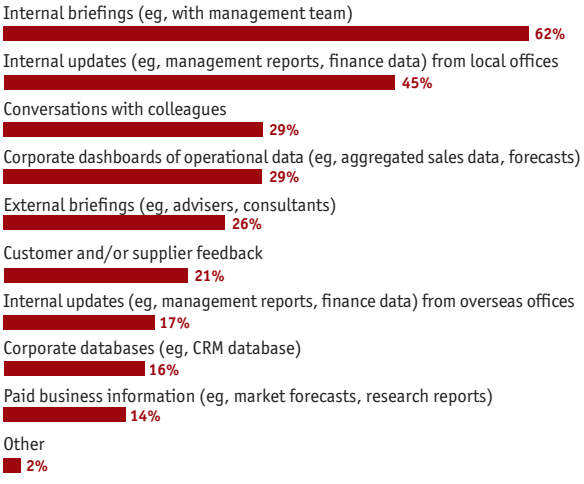


Where do you think your organisation is weakest in managing operational risk (including IT risk)? (Select up to three)

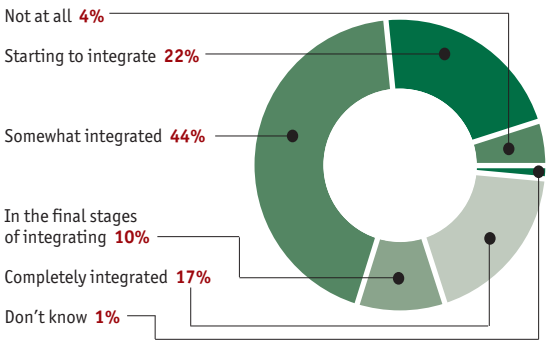
Where do you think your organisation is weakest in managing compliance risk? (Select up to three)



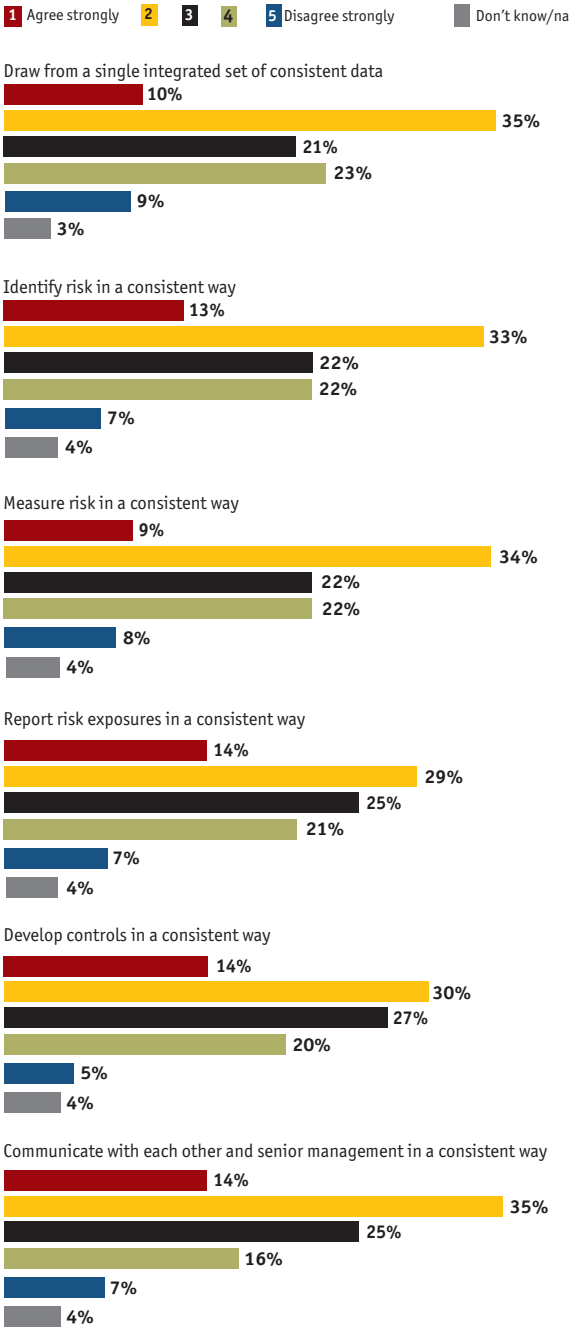
In your organisation, which of the following sources of information do you use most often when making key decisions regarding risk? (Select up to three)



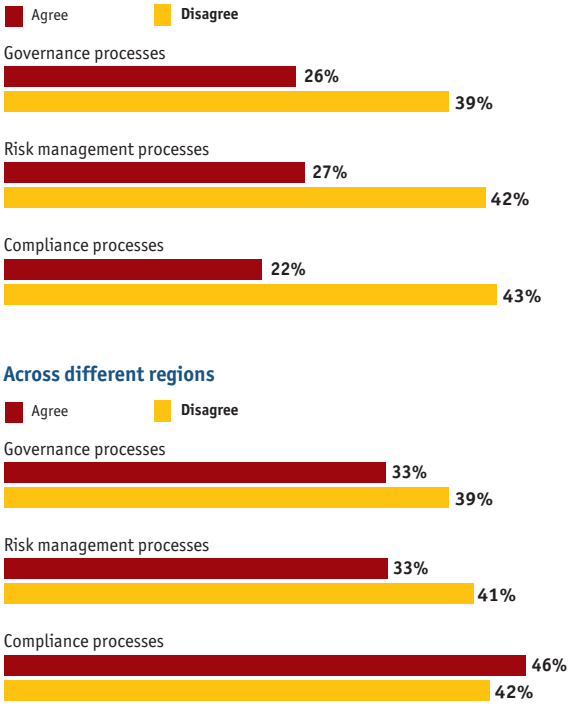
Has your organisation integrated its governance, risk and compliance processes?



To what extent do you agree or disagree with the following statements? Across my organisation, compliance and risk managers...
(Rate on a scale where 1 = Agree strongly and 5 = Disagree strongly)

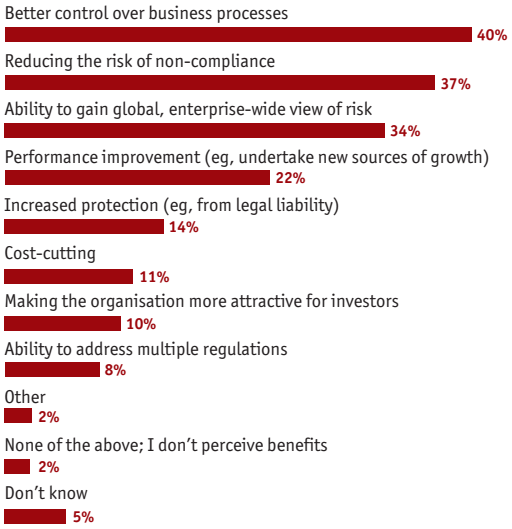


To what extent is duplication of compliance and risk management processes across your organisation a problem?



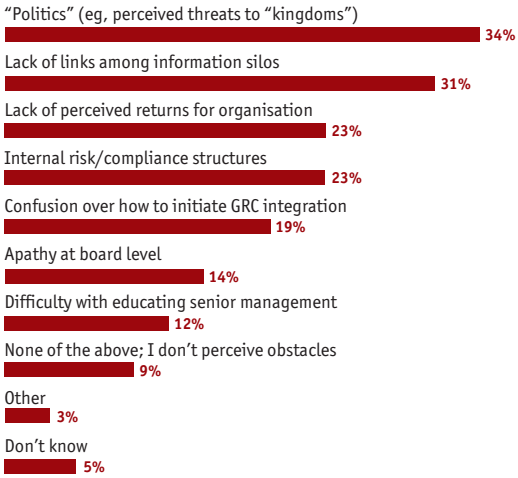
Note: Respondents who said "don't know" or "neither agree nor disagree" excluded.

What do you regard as the biggest benefits of integrating GRC at your organisation? (Select up to two)

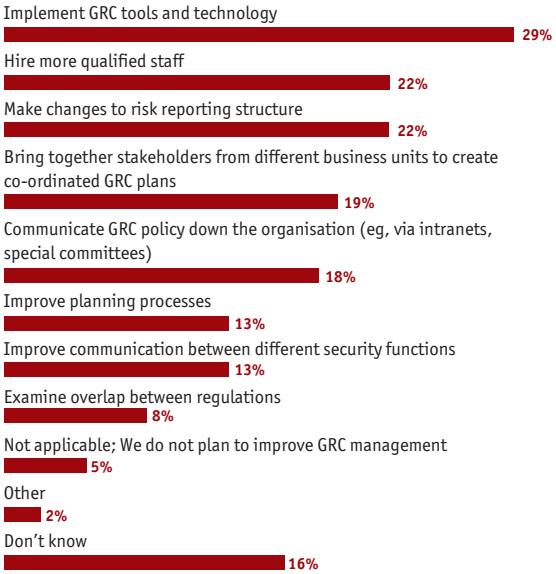


Which department or individual—if any—is driving the move to integrate GRC in your organisation?

What do you think are the main obstacles to implementing an integrated GRC programme in your organisation? (Select up to two)



How does your organisation plan to improve GRC management in the next three years? (Select up to two)



LONDON
26 Red Lion Square
London
WC1R 4HQ
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

NEW YORK
111 West 57th Street
New York
NY 10019
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
60/F, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com