Economist Intelligence Unit

The Economist

Ascending the maturity curve

Effective management of enterprise risk and compliance

A report from the Economist Intelligence Unit
Sponsored by SAP

Contents

Preface

Ascending the maturity curve: Effective management of enterprise risk and compliance is an Economist Intelligence Unit briefing paper sponsored by SAP. The Economist Intelligence Unit bears sole responsibility for this research. Our findings drew on desk research, a global survey and in-depth interviews with executives familiar with risk and compliance within their organisations. The findings and views expressed in this report do not necessarily reflect those of the sponsor. Rob Mitchell was the author of this report and and Mike Kenny was responsible for its design.

March 2011

Executive Summary

Most organisations have come a long way in managing financial risks, and it is a rare large company that does not have a C-level executive focusing on the overall approach to risk and compliance. That does not mean that risk and compliance are under control; in fact, there are usually varying levels of effectiveness throughout the organisation. Despite recognising the benefits of an integrated approach, few organisations manage risk and compliance activities consistently and efficiently.

One reason is the apparent cost and complexity of an enterprise-wide risk and compliance implementation. In most organisations, risk responsibilities span a wide range of activities, from health and safety and IT security to financial reporting and credit risk exposure. This dispersal of risk responsibilities inevitably leads to a disconnected approach, with different departments setting their own policies and operating their own processes. Integrating these activities to permit an enterprise-wide view can seem like a Herculean task.

Ever-evolving compliance obligations muddy the waters further, particularly for heavily regulated industries, such as financial services, energy and utilities, and pharmaceuticals. As each new set of regulations emerges, a typical response is for the company to create a new initiative to handle it. According to Scott Mitchell, chief executive of the Open Compliance and Ethics Group, a US-based risk and compliance organisation with local communities in 11 countries, it is not uncommon for companies to have between three and 15 different compliance silos.

Amid these challenges, calls from a wide range of internal and external stakeholders for more effective enterprise risk and compliance management are becoming louder. Boards are under pressure to demonstrate effective oversight of risk management, while regulators are increasing their scrutiny of business practices. Rating agencies and investors are also looking more carefully at risk and compliance, and there is a growing consensus that effective management of this area is not just hygiene for business, but a barometer of good management overall.

In December 2010 the Economist Intelligence Unit conducted a worldwide survey of 385 senior executives from finance, risk, compliance and legal functions to assess the current state of risk and compliance management. The survey focused on perception versus reality: how executives view their risk mitigation capabilities versus what they are actually doing. This report presents the highlights of those survey findings, along with related additional insights drawn from interviews with industry experts and commentators. Key findings from this research are as follows.

- **Companies may be underestimating the extent of risk and compliance failures in their organisation**. Just over one-third of respondents say that their organisation has suffered from one or more significant risk or compliance failures in the past three years. But this proportion is most likely owing to the fact that most respondents come from the finance function, where awareness of failures is relatively low. Among the four functions surveyed—finance, legal, risk and compliance—respondents from outside finance estimate significantly higher levels of risk and compliance failures. This suggests not only that the finance function is underestimating the level of failures, but that knowledge about risk failures is not being widely disseminated in order to improve practices and tighten policies.
- **Risk and compliance management processes may appear to work well —until something goes wrong**. Unsurprisingly, respondents who say that they have experienced failures are far less likely to consider that their risk and compliance are consistent with best practice in their industry. Respondents who have experienced failures are also more likely to admit that they do not have a consistent set of principles and policies governing business practices. In other words, companies may make the assumption that their approach is working well, until a major risk event reveals shortcomings that need to be addressed.
- **Companies may not be learning the broader lessons from risk failures**. Almost three-quarters of respondents say that their organisation deals with risk failures by tightening up policies and procedures to reduce the chances of a similar mishap. But not all companies adopt this approach. The majority of risk failures take place at the business unit level, which can lead to a tendency to address issues in isolation. More than one-quarter of respondents say that they fix the problem within the unit, outside the oversight of the wider organisation and of superiors. This suggests that a significant proportion of companies are not doing enough to share risk information and learn the broader lessons from risk failures.
- **High-performing companies are more likely to have a consistent risk appetite across the organisation**. The survey reveals that most companies have a broad range of risk tolerances within the organisation. Sales and marketing functions have the greatest tolerance for risk, while finance and legal have the lowest. But what is more striking is the extent to which high-performing companies (those in the top 20% of their industry in terms of revenue growth) tend to be more consistent in their risk tolerance. Among that group, 48% say that their risk tolerance is consistent across functions, while just 29% of those in the lower-performing group (those in the bottom 60% of their industry) offer the same assessment.

Introduction

Enterprise risk and compliance management is a concept that eludes simple definition. Although the disciplines that comprise it are well understood, their interaction within an organisation is less straightforward. For some companies, it is a set of technology tools that support risk and compliance management, while for others it is a complete philosophy that enables their business strategy to be achieved within a set of enterprise-wide values, rules and parameters.

Confusion over the scope of enterprise risk and compliance management and the investments that are required has tended to hamper its effectiveness. A survey from Ernst & Young[1] found that two-thirds of international companies wanted to invest more. But almost half said they found it difficult to implement, mainly because they were unsure about which model to adopt.

One source of confusion is the changing nature of the concept. The GRC (governance, risk and compliance) acronym originated in the period following the Sarbanes-Oxley Act in the US and similar legislation in other markets, such as J-Sox in Japan and Bill 198 in Canada. Although these regulations differed in detail, the goal was the same: they required companies to step up their corporate governance and establish more rigorous internal controls.

While the implementation of these regulations remains an often challenging business priority, leading companies have moved beyond the notion of risk and compliance management as a set of tools whose primary objective is to enable compliance with governance legislation. In their more developed form, the tools should not only facilitate the compliance process, but also fit together into a broader framework that is consistent across the enterprise.

About the survey

In December 2010 the Economist Intelligence Unit conducted a worldwide survey of 385 senior executives from finance, risk, compliance and legal functions. All respondents were executives in one of the following industries: financial services; healthcare; energy and utilities; logistics and manufacturing; or the public sector. Outside the public sector, 63% of respondents work for companies with annual revenue of over US$500m or the equivalent, and 25% work for firms with over US$5bn in annual revenue. The average annual company revenue was around US$4bn. One-third of the respondents are employed in Western Europe, 28% in the Asia-Pacific region and 27% in North America.

1. "The multi-billion dollar black hole," Ernst & Young, 2010 (http://www.ey.com/GL/en/Services/Advisory/Risk/The-multi-billion-dollar-black-hole)

The call for an integrated enterprise approach

"GRC gives you the ability to take the components and bring them together to gain a better overview of where the organisation is."

Tim Brooke, managing director, Protiviti.

The pressure for integration is coming from the top. Boards are being asked by shareholders and other external stakeholders to demonstrate that they are providing effective risk oversight at a time of considerable turbulence. "Boards have recognised that, in the past, they may not have been getting the whole picture," says Tim Brooke, managing director of Protiviti, a multinational business consulting and internal audit firm. "You've got lots of different groups providing packs of information to the Board, but it's difficult for them to sort the wood from the trees. GRC gives you the ability to take the components and bring them together to gain a better overview of where the organisation is."

At the operational level, there is a cost and efficiency argument for integration. "Without having a single integrated programme, you almost certainly are experiencing inefficiencies and extra costs to manage the risks and remain in compliance," adds Paul Sobel, an internal audit executive and member of the Board and Executive Committee at the UK-based Institute of Internal Auditors (IIA). "You also expose yourself as an organisation to having things slip through the cracks, because there's so much noise out there around risk and compliance that it's difficult to know whether you caught it all."

In some industries, most notably financial services, regulatory scrutiny is forcing companies to provide stronger evidence that they have effective risk management and internal controls in place. The insurance industry in Europe, for example, is currently grappling with the implementation of Solvency II, a new set of capital adequacy rules and risk management standards. Under Pillar II of the legislation, insurers must be able to demonstrate that they have sound internal controls and a robust risk framework in place.

"There's a requirement to provide evidence of how risks are being considered as we take decisions within the business," says Robert Beattie, director of internal audit at UK-based financial services group Friends Provident. "This means that risk and compliance need to be more engaged with the business than they would have been in the past around proposals, strategic decisions and options. We'll need to model the risks involved and that should lead to better decision-making."

The strategic imperative

Effective risk and compliance management is not just a necessary evil that facilitates compliance and reduces the cost of risk management. Increasingly, companies see it as a way of enhancing corporate performance and enabling strategy to be discussed and implemented from a position of greater confidence. Although the argument is not new, an increasing variability of financial results has made it

"[GRC integration] is all about ensuring that performance will be sustainable, which means that financial results will be achieved, but in the proper manner, without cutting corners."

Yves Muckensturm, director of internal audit at EDF Energy.

newly relevant. "Integration of GRC is all about alignment and bringing added value to the business," says Yves Muckensturm, director of internal audit at EDF Energy, part of the French EDF Group, one of the largest energy firms in Europe. "It's all about ensuring that performance will be sustainable, which means that financial results will be achieved, but in the proper manner, without cutting corners."

"Sound risk and compliance is a key factor in being able to implement strategy," says Martyn Scrivens, director of group audit for Lloyd's, the multinational banking group. "If we decide that we want to be in a particular business, then we need to consider the risks involved in investing the required amount of human, intellectual and financial capital. We need to know how much of that risk we are prepared to accept, and ensure that we have the right frameworks, controls and compliance mechanisms in place so that we stay within those parameters. If you don't do that, you're navigating without a compass."

Better co-ordination between risk and controls also benefits lines of business because managers gain greater awareness of the connection between the two concepts. "By consolidating risk and controls, we benefit the business, because managers can automatically see the linkages between the risk and controls," says Paul Kaczmar, head of operational audit at Electrocomponents, an electronic parts distributor operating in 80 countries. "It also enables them to challenge if they're looking at risks and controls and they don't match or aren't appropriate."

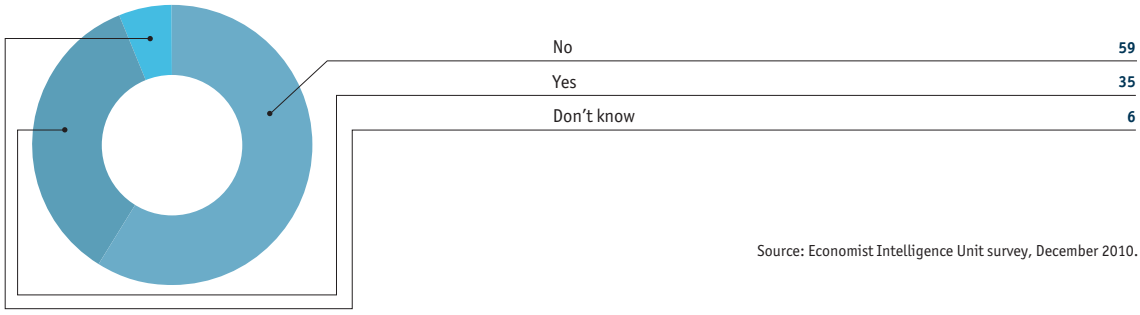
By demonstrating publicly that they have an effective risk management and compliance programme in place, companies should also find that they are more attractive to investors, customers and employees. "Organisations that have effective GRC are likely to have a competitive edge," says Chris Baker, technical manager of the Chartered Institute of Internal Auditors. "Sound GRC is therefore likely to attract investors and shareholders who will see these organisations as being managed well, balancing risk and reward, and complying with the law. It will also attract customers who want to do business with reliable, trusted and respected organisations."

Nasty surprises provide an impetus

These drivers of change may be important, but there is nothing that will do more to encourage a more proactive focus on risk and compliance than a shock. Just as a homeowner who has been burgled will be more likely to seek insurance, so companies that have been affected by a major risk event will be more likely to focus on their risk and compliance processes.

Just over one-third of survey respondents say that their organisation or business unit has suffered from one or more significant risk or compliance failures over the past three years. Unsurprisingly, in view of the global financial collapse of 2008-09, respondents that have suffered such an incident are disproportionately likely to represent the financial services industry.

To the best of your knowledge, has your organisation or business unit suffered from one or more significant risk or compliance failures during the past three years?
(% respondents)

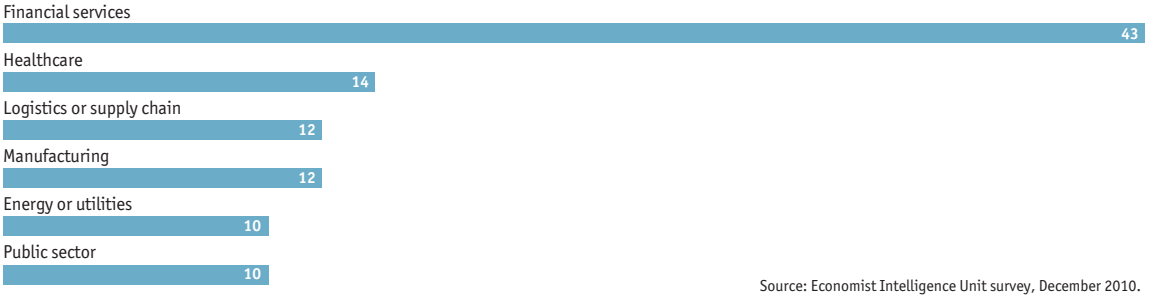


Source: Economist Intelligence Unit survey, December 2010.

At first glance, the fact that only one-third of respondents have experienced a risk or compliance failure might seem like a comforting finding. But respondents are most likely underestimating the scale and frequency of such events. Executives from the legal, risk and compliance functions are considerably more likely to be aware of failures than colleagues in the finance function. This also suggests that information about risk failures is not being disseminated throughout the organisation.

Respondents reporting a significant risk or compliance failure during the past three years...
(% respondents)

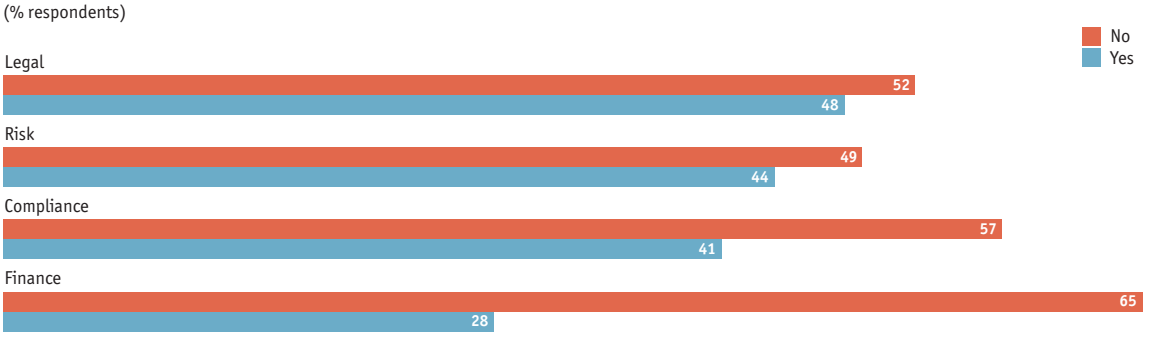
...by industry



Source: Economist Intelligence Unit survey, December 2010.

...by function

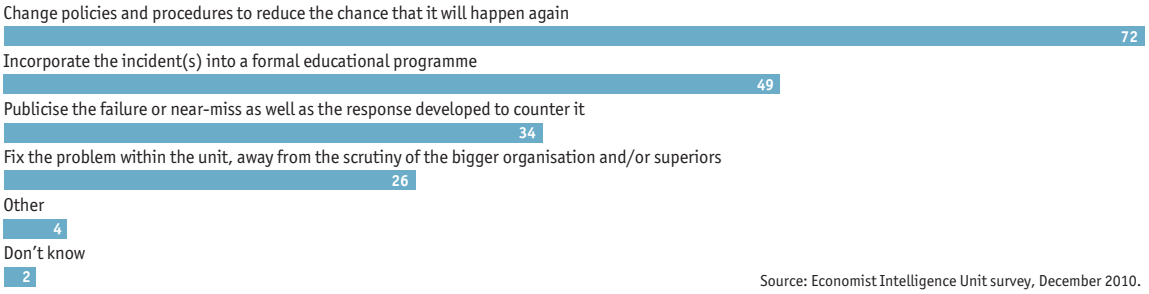
(% respondents)



Source: Economist Intelligence Unit survey, December 2010.

Other survey findings reinforce the idea that many companies are secretive about risk and compliance failures within the organisation. More than one-quarter of respondents say that that they fix the problem within the business unit, away from the scrutiny of the organisation and their superiors. This approach does little to enable the company as a whole to learn from mistakes and put in place measures to prevent the same problems from happening again.

How does your organisation deal with failures or near-misses in the area of risk or compliance?
(% respondents)



Source: Economist Intelligence Unit survey, December 2010.

Mr Muckensturm of EDF Energy highlights the importance of tracking risk events effectively in order to facilitate management assessment of whether changes to policies or controls are required. "By analysing our company risk register and updating it on a quarterly basis, we may decide in conjunction with management that we need to improve our controls in a given area," says Mr Muckensturm. "It's important to have a feedback loop that makes it possible to escalate concerns about a certain type of risk, so that a decision might be taken to change our processes or the way we monitor our business activities."

The road to implementation

The rationale for investment may be compelling, but the complexity of the task, and the variety of approaches that can be taken, can deter companies from taking the plunge. Moreover, many companies that have already invested in enterprise risk and compliance management may not feel that they are getting the value that they expect. In a 2010 survey by Ernst & Young, two-thirds of respondents said that there was a "strong need" for their GRC programmes to be enhanced.[2]

"There's a perception that a GRC structure is an overhead, so that can drive reluctance to invest in it," says Protiviti's Mr Brooke. "It's also a complicated undertaking that requires investment at multiple levels. You've got to get your risk management, legal and compliance, and internal audit infrastructures all working well together, and that can be tough."

There is no doubt that developing risk and compliance management systems can be costly, but advocates of the approach suggest that this can be offset by the savings made over the longer term. "At the very minimum, you would expect that the investment in headcount and technology would be at least cost neutral once you have taken the efficiency savings into account," says Steve Culp, managing director for the finance and performance management line at Accenture, a multinational management consultant and technology outsourcing company.

Correctly implemented, risk and compliance management processes should lead to significant cost savings. These can derive from a number of sources, including a reduction in duplication of effort, the streamlining of processes and greater use of automated controls. "Effective GRC should lead to efficiencies in the back office, and lower deviations in cash flow from forecast to actual," says Glenn Labhart, a former chief risk officer (CRO) for Dynergy, a Texas-based energy firm, and now an independent risk consultant. "Compliance violations should become less frequent and, when they do happen, you should be able to handle those issues more quickly."

Stages of adoption

The maturity cycle of enterprise risk and compliance management adoption is often described as having four stages: reaction; acceptance; collaboration; and orchestration.[3]

- In the "reacting" stage, companies are responding to a specific stimulus without thinking about the broader picture. They are often in panic mode.

2. Ibid.

3. This GRC maturity cycle framework was popularised by AMR Research, now a part of Gartner, in 2006.

- The "anticipating" stage refers to the point when the company starts to see linkages between multiple programmes and seeks out efficiencies and automation.
- The "collaborating" stage occurs when priorities are established and technology is re-used for multiple purposes.
- In the "orchestrating" stage, there are clear enterprise objectives, and complete co-ordination and visibility across risk exposure.

The transition from the "reacting" to the "orchestrating" stage requires companies to consider changes to processes, technology, reporting lines and organisational structures. And because these factors differ across companies, each model should be designed to suit the company's context and specifics.

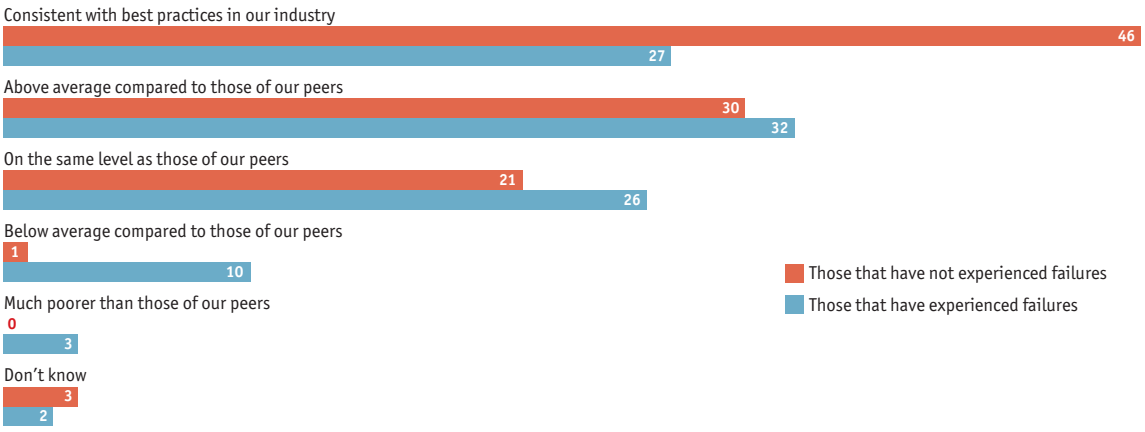
"A one-size-fits-all approach will not work," says Rainer Lenz, vice-president of internal audit at Actavis Group, a multinational pharmaceuticals company. "GRC needs to give room for maneuver so that business managers can apply judgment within well-defined boundaries."

Typically, the migration to effective and mature risk and compliance management will not require a complete overhaul. More often, it is about integrating existing processes and disseminating best practice where appropriate. A first step is often to carry out an audit of current processes and information to establish where risk and compliance activities reside within the organisation.

"You don't necessarily have to start with a plain sheet of paper, because there's probably a lot of very good and useful activities that are already occurring in the organisation," says Mr Sobel of the IIA. "It can be helpful in trying to break down silos to let people know that you value what they're already doing, and that you're just trying to find a way to better integrate it so that they can get more done with less effort."

The surveyed companies tend to rate themselves as advanced in their adoption of an integrated approach. But other findings suggest complacency. Only 27% of respondents whose companies have

In general, how do the risk and compliance practices of your organisation, as well as your business unit, rate relative to the rest of your industry?
(% respondents)



Source: Economist Intelligence Unit survey, December 2010.

experienced failures consider their risk and compliance as consistent with best practice within their industry, compared with 46% of those that have not experienced failures.

Respondents who have experienced failures are also more likely to admit that they do not have a consistent set of principles and policies governing their business practices. In other words, companies may make the assumption that their approach is working well until a major risk event reveals shortcomings that need to be addressed.

Overcoming organisational challenges

As with any enterprise-wide initiative, support must come from the top. "A critical factor for success is board sponsorship and direction," says Mr Culp. "One of the tangible elements that boards can effectively bring into GRC programmes is a level of materiality and focus."

Pressure from external stakeholders

By demonstrating that it has effective risk and compliance management processes in place, a company can benefit from more open and trusting relationships with key external stakeholders. "If there's a good GRC process in place, then external auditors can have a greater degree of confidence about how the numbers evolve," says Tim Brooke, managing director of Protiviti, a business consulting and internal audit firm. "Insurance companies will also look at the quality of your risk management and, if you can demonstrate the rigour of your approach, that can have a direct and positive impact on your premiums."

For heavily regulated industries, companies that can demonstrate a robust approach to risk and compliance management may be able to benefit from quicker, more accurate responses to requests from regulators that may ultimately lead to less intrusive regulatory intervention. "Regulators are a lot more interested and insistent on seeing evidence of risk management and compliance in practice," says Martyn Scrivens, director of group audit for Lloyds Banking Group. "The form and intensiveness of that scrutiny will depend on how good your risk management and control processes are."

By building a better relationship with regulators, companies can reduce the management resources that are devoted to risk management and compliance, and re-allocate those resources to more strategic activities. "If the leadership in the organisation is focused on dealing with regulators and having to pull together compliance-oriented information, then the return on investment for that time and effort is incredibly low," says Steve Culp, managing director for the finance and performance management line at Accenture. "Whereas, if they spend less time on these activities, then they can focus on their competitive position, their sales and their customers."

In the financial services industry, the largest and most interconnected institutions have been subject to the most rigorous scrutiny. Some observers believe that these companies may now be able to turn the investments they have made in response to this scrutiny to their advantage. "Leading banks have been subject to serious demands from regulators and, having got through that process, they are looking to use the data they have gathered to help them run their business better," says Simon Bailey, Director of Payments at Logica, a UK-based logistics firm.

Investors are also becoming more interested in risk and compliance management because, properly implemented, it can lead to more stable financial performance. "GRC is something that is requested by a growing number of external stakeholders because it reduces the volatility of financial results and increases the sustainability of both technical and financial performance," says Mr Muckensturm, director of internal audit at EDF Energy.

There is growing evidence that markets reward companies with effective risk and compliance programmes in place. In April 2010 the Corporate Library published a report in which it asserted that investors who excluded companies seen as high risk from a governance perspective would have enjoyed significantly better returns between 2003 and 2010[4]. And an Ernst & Young survey found that 82% will pay a premium for companies that demonstrate successful risk management.

4. The Corporate Library's Governance Ratings and Equity Returns, April 2010, available at http://www.thecorporatelibrary.com

5. Investors on risk, Ernst & Young, 2006

"Those organisations that really focus on aligning their risk programmes to their business priorities and try to drive them in a more integrated way tend to have higher success rates."

Steve Culp, managing director, Accenture.

But, while boards can provide the mandate for the organisation to implement the project, they do not always have a clear idea of the outcome they are trying to reach. "Boards recognise that they need more information to perform better oversight, but that doesn't mean they know exactly what they need," says Mr Sobel. "They often find it difficult to direct management to say 'This is the type of information we want, here's the level of detail and here's how frequently we want it.' Part of a successful programme is figuring out who should need what information and when. And then making sure that they get it."

A successful programme requires input from a range of different functions, including risk, legal, compliance and internal audit. And while it may be tempting to create a separate function to oversee risk and compliance, there are serious downsides to this, including increased cost and the potential for new silos to be created. Instead, experts recommend the formation of a steering committee, with representatives from appropriate functions, to discuss and recommend ways of improving risk and compliance processes.

As an independent function within the organisation, internal audit can play an important role in guiding the process. "You need some good unbiased facilitators to try and move this process forward," says Mr Sobel. "That's where internal audit, which is typically considered a 'no skin in the game' function, can do an effective job. It's important to get the silos to the table so that, together, you can figure out how to improve risk and compliance."

This kind of independent facilitation can be extremely valuable in fostering a more collaborative approach. While it may be conceptually difficult to disagree with the breakdown of organisational silos, it is not uncommon for those affected to resist change because they fear that it may erode the scope of their responsibilities.

"When you have the competing agendas of growth versus compliance at the coalface of the business, then quite often you find that the messaging, intent and impact of GRC programmes can meet with resistance," says Mr Culp. "Those organisations that really focus on aligning their risk programmes to their business priorities and try to drive them in a more integrated way tend to have higher success rates."

The key role of technology

Technology helps organisations to link disparate sources of assurance and automate the controls environment. "You need to invest in systems and structures because that's the only way you can pull together the sort of management information that you need to determine whether or not you're actually staying within the limits that the board has set," says Mr Scrivens.

In many organisations, a fragmented approach to documentation and compliance processes means that critical information resides in spreadsheets, and that processes are relying on inconsistent underlying data. By replacing this approach with a central repository for data and information, companies ensure that there is "a single source of truth" that is constantly updated. "You can get overwhelmed with data. Technology can be a key way of managing it, and making sure that you get the right data to the right people at the right times to support decision-making," says Mr Sobel.

Technology also facilitates the automation of controls and compliance processes. Without automation, the costs of risk and controls can spiral as checks must be done manually and rely on random sampling of

transactions to uncover transgressions. Automated controls can provide real-time detection to prevent violations and better support and streamline the audit process. This is not only more effective, it is also cheaper, because there is no need for time-consuming manual intervention. Automation also facilitates the creation of reports and analysis to provide management with a complete picture of compliance with both internal and external policies.

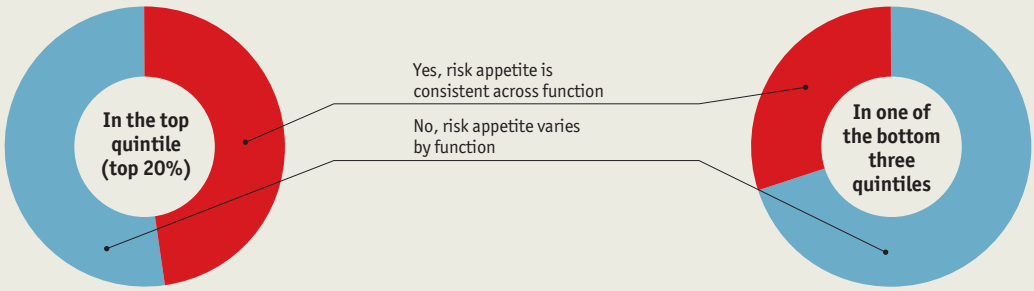
While technology is necessary—at least for organisations above a very small size —it is not sufficient. Mr Muckensturm highlights the importance of putting business processes first. "We want to drive the tools. We don't want the tools to drive us," he says. "If you rely too heavily on a system, the danger is that the technical view of the system will prevail."

Where there is disagreement on risk, financial performance may suffer

Among survey respondents, just 45% say that the various functions within the organisation agree on risk tolerance. Risk appetite is highest in sales and marketing (especially in financial services), and lowest in finance and legal. This finding highlights the importance of putting in place a robust controls framework that accounts for differences in individual or functional views on the appropriate amount of risk. It also suggests that, in organisations without agreement on risk tolerance, the risk and controls environment may not be providing a consistent set of limits within which business managers can operate.

The survey also suggests a link between inconsistent attitudes towards risk and overall financial performance. Higher-performing companies have a more consistent risk appetite across the company. In lower-performing companies, there are wider differences in risk tolerance within the organisation. The chart below contrasts these two groups, showing how respondents judge their own organisation's performance versus how consistent they judge the organisation's risk tolerance to be.

Do all functions agree on the organisation's risk tolerance, or are certain functions more aggressive or conservative than others?
(% respondents)



Source: Economist Intelligence Unit survey, December 2010.

Conclusion

Almost a decade after the GRC concept entered widespread use, risk and compliance management remains as relevant as ever. Compared with the early days, the rationale for investing in a programme has broadened considerably. In addition to the traditional goal of meeting compliance obligations, companies see the investment as a means of aligning their risk and controls with broader strategic goals, building better relationships with stakeholders and enhancing overall performance.

Yet despite these benefits, many companies remain at a relatively early stage of adoption. An absence of serious risk failures—or lack of knowledge of them—can breed complacency and a misguided conclusion that, just because nothing has yet gone wrong, the tools continue to be effective. At a time when regulatory scrutiny is greater than ever, and when markets remain highly volatile and turbulent, this is a dangerous assumption to make.

In particular, the findings from the survey and interviews suggest the following action points for those charged with implementing risk and compliance management.

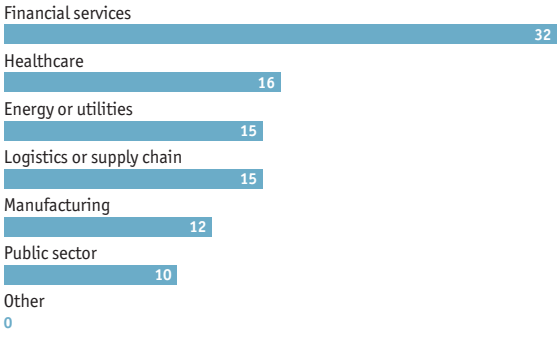
- **Help the business owners "own" the risk and compliance issues that arise from their businesses.** The idea is not to tell them what to do, but rather to enable them to manage and mitigate the risks within their own processes.
- **Join business owners at the idea stage of business initiatives, with the aim of helping them to achieve sustainable financial performance.** Help them to be explicit about how much risk the business is accepting, and to set up controls to ensure that the agreed-upon level of risk is not exceeded.
- **Think carefully about the messaging used when bridging the competing agendas of growth versus compliance.** This is seen most dramatically in the gap in attitudes between the sales function and the legal, risk and compliance functions. The more closely aligned the attitudes across the functions, the higher the success rate.
- **Consider bringing silos together with a facilitator from senior management.** It is hard to disagree with the notion of breaking down silos. But in practice, change is hard because those affected fear a loss of power. A senior executive has the authority and credibility to tear down the walls.

- **Have a feedback loop in place**. The idea of treating risk failures as a warning and completing the feedback loop by modifying policies or controls if warranted may sound like common sense. But the finding that one-quarter of survey respondents fail to examine policies or controls after risk events suggests that it is often common sense unheeded.
- **Strive to bring hidden costs to the surface**. Organisations that fail to build an integrated risk and compliance framework incur costs on several levels. These costs often go unmeasured. They range from the trivial, such as time spent on manual and duplicative processes, to the serious, such as damaged reputations and weakened valuations.
- **Before embarking on an integration initiative, take steps to uncover and publicise the "good and useful activities" (in the words of the IIA's Mr Sobel) that are already occurring**. Let these individuals know that what they do is valuable and that integration will help them to get more done with less effort.
- **Look carefully at steps towards greater automation of the controls environment.** Automated controls can provide real-time detection to identify and prevent violations. This is not only more effective in controlling risk, it is also cheaper. It also facilitates the generation of reports and analysis that make it possible for management to review compliance with both internal and external policies.
- **Think about technology—and beyond technology, too**. Focus first on the process and governance structure. Then leverage technology to make it consistent across the organisation.

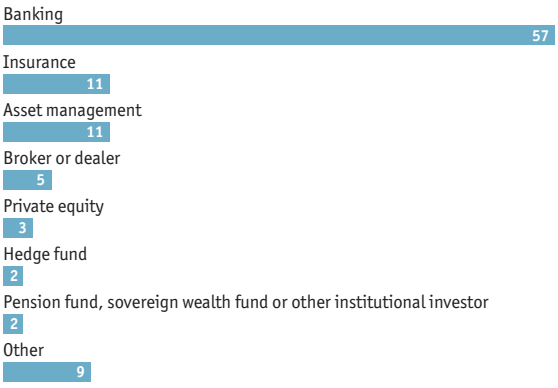
Appendix: Survey results

Percentages may not add to 100% owing to rounding or the ability of respondents to choose multiple responses.

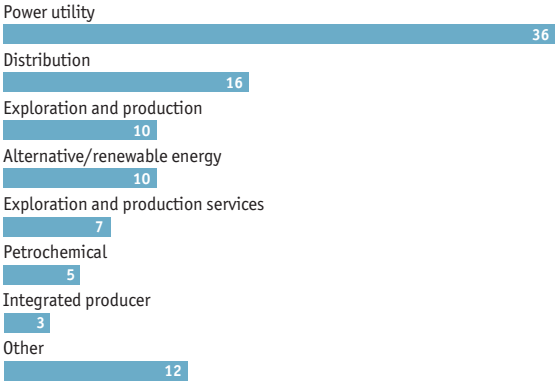
In which industry do you work?
(% respondents)



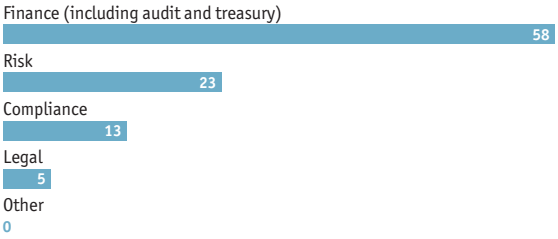
What is your sector within financial services?
(% respondents)



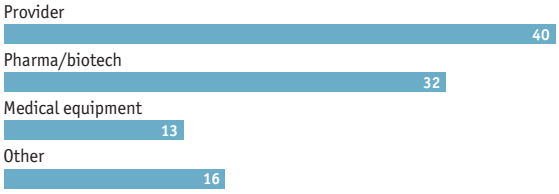
What is your sector within energy/utilities?
(% respondents)



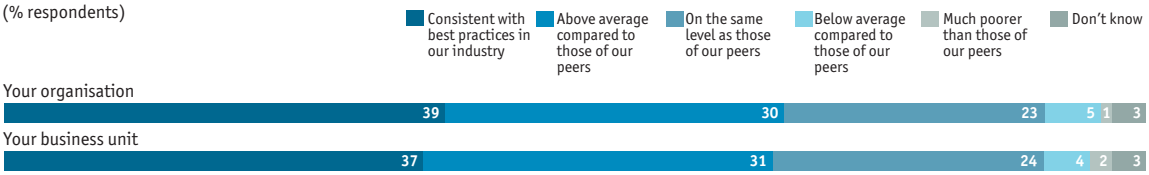
What is your main functional role?
(% respondents)



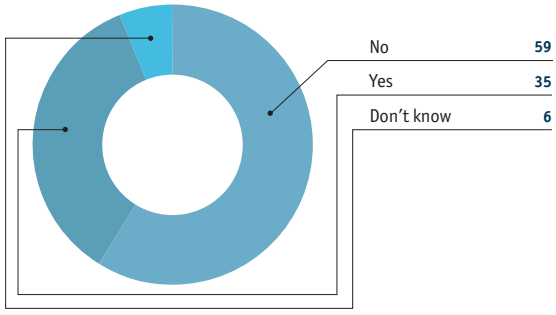
What is your sector within healthcare?
(% respondents)



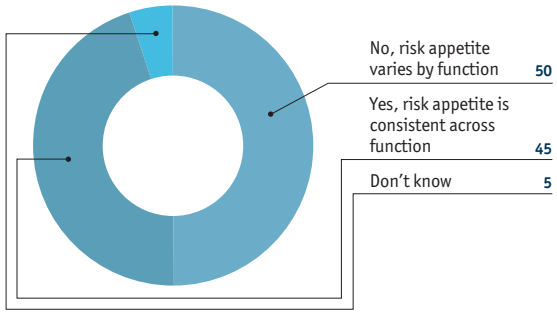
In general, how do the risk and compliance practices of your organisation, as well as your business unit, rate relative to the rest of your industry?
(% respondents)



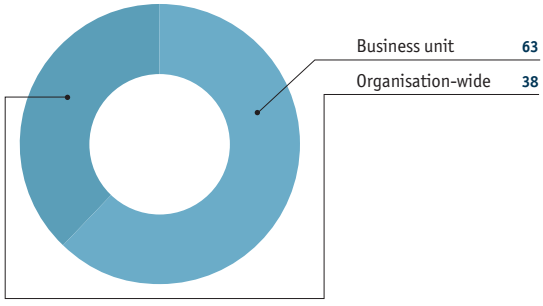
To the best of your knowledge, has your organisation or business unit suffered from one or more significant risk or compliance failures during the past three years?
(% respondents)



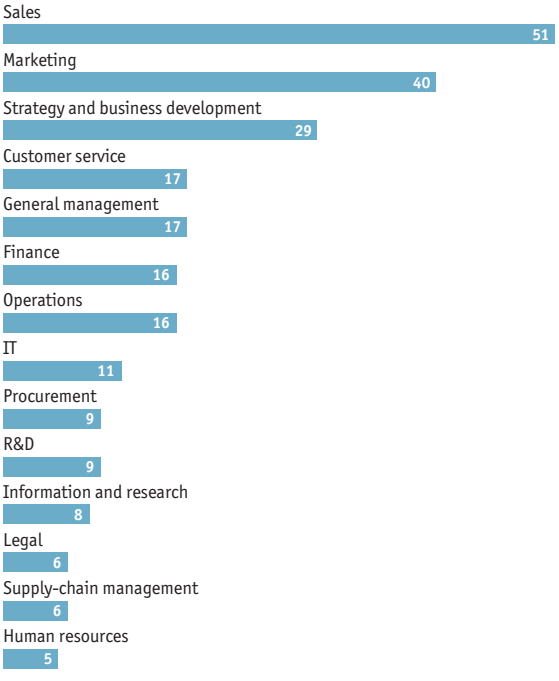
Do all functions agree on the organisation's risk tolerance, or are certain functions more aggressive or conservative than others?
(% respondents)



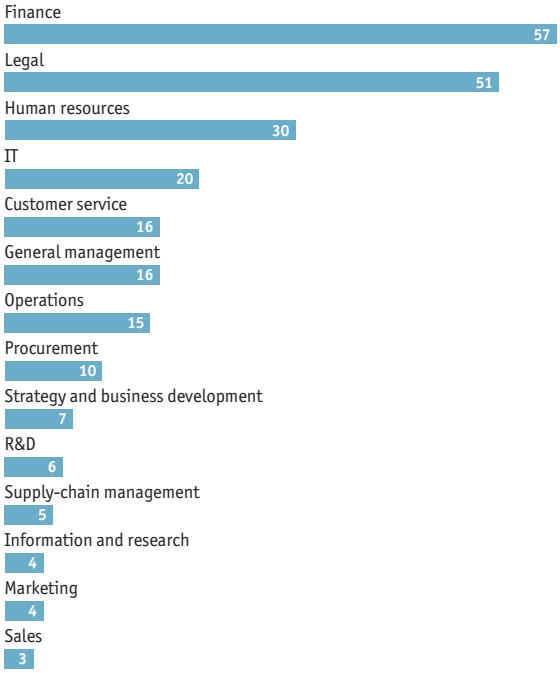
At what level did the significant risk or compliance failure occur?
(% respondents)



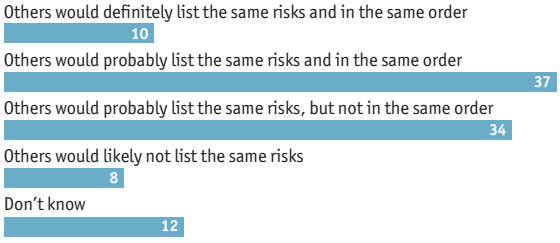
In your organisation, which functions have the biggest appetite for risk?
(% respondents)



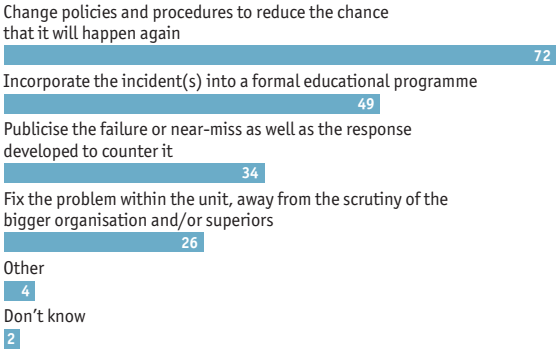
In your organisation, which functions have the smallest appetite for risk?
(% respondents)



How do you think others in your organisation would answer the previous question?
(% respondents)

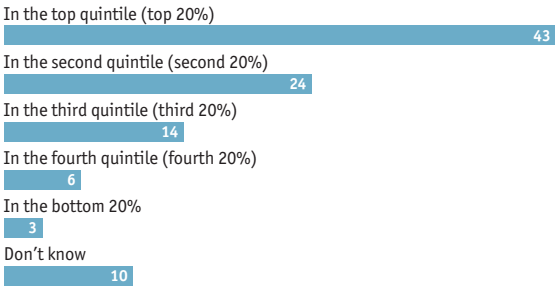


How does your organisation deal with failures or near-misses in the area of risk or compliance? Select all that apply.
(% respondents)

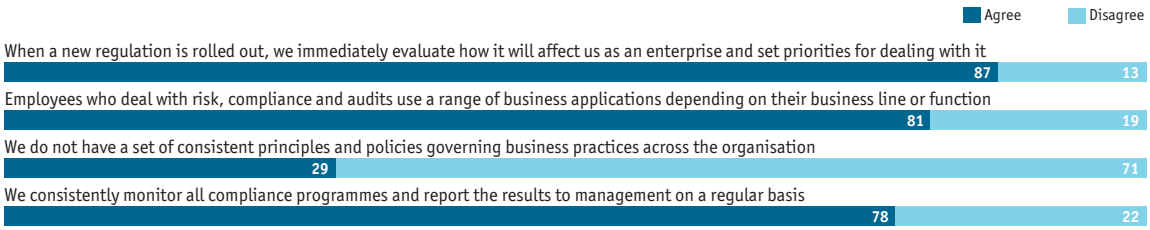


The executives in our business lines treat the chief risk officer (or other risk oversight executives) as:
(% respondents)

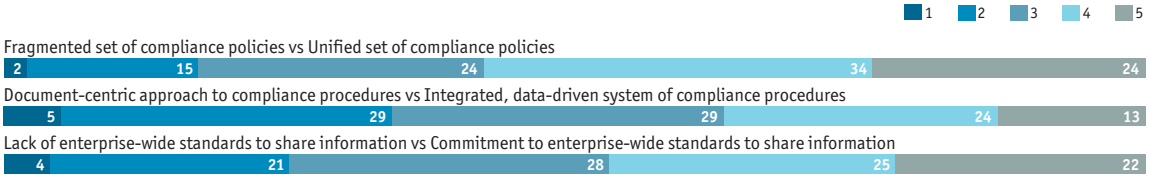
In terms of revenue growth, how does your organisation compare to its industry peers?
(% respondents)



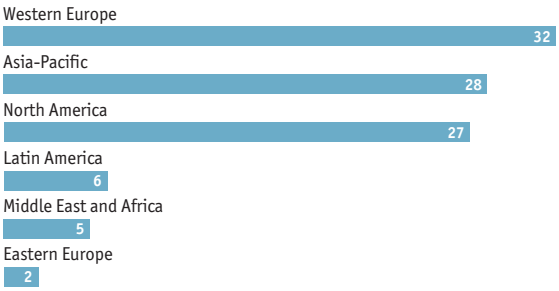
For each of the following statements, please indicate whether you agree or disagree:
(% respondents)



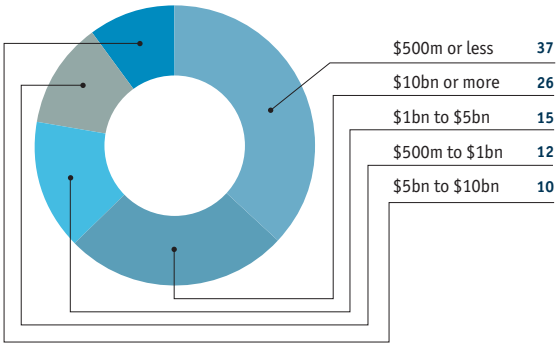
Where does your organisation fall on the spectrum below?
Use the slider to characterise your organisation's primary approach.
(% respondents)



In which region are you personally based?
(% respondents)



What are your company's annual global revenues in US dollars?
(% respondents)



Cover: Shutterstock

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
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

GENEVA
Boulevard des Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com