Fortifying the enterprise: Governance, risk and compliance strategies

A briefing paper from the Economist Intelligence Unit sponsored by Oracle
Preface

Fortifying the enterprise: Governance, risk and compliance strategies is an Economist Intelligence Unit white paper, sponsored by Oracle. The Economist Intelligence Unit’s editorial team wrote the report, and the findings and views expressed do not necessarily reflect the views of the sponsor. Terry Ernest-Jones was the author of the report and Dan Armstrong was the editor. Richard Zoehrer was responsible for layout and design.

November 2007
Introduction

Both private and public sector executives are under pressure today to increase their understanding of governance, risk and compliance (GRC) issues—and their ability to respond to them. They are expected to deliver against a range of key performance indicators (KPIs), including profitability, customer satisfaction, revenue growth, market share, market value and brand awareness. At the same time they face escalating demands for information from outside stakeholders, regulatory bodies, analysts and the media.

All the while, they are also operating in an environment more prone to risk. Compared with five years ago, a crisis in one part of the world—such as a hurricane, political upheaval or terrorism—is now far more likely to have an impact on the entire organisation. Supply chain partners can number 100,000 for a single company, with an interdependent network stretching from Houston to Hong Kong. Failure in one area is often felt immediately across the board.

Mergers and acquisitions (M&A) only add to complexity and risk as networks of multiple business partners are brought together. Furthermore, companies are collaborating more than ever on projects with overseas partners—often with firms that are competitors in other fields. The scope for theft of intellectual property, contravening data privacy laws and general abuse of network security abound.

Compliance with a web of new regulations adds another dimension of complexity and risk. Jorge Soeiro Marques, chief risk officer at Lusitania Companhia de Seguros, a Portuguese insurance firm, says his industry has had to deal with 300 new regulations in the past three years. Companies in other countries and across a range of industries—energy, banking, retail and manufacturing—face much the same situation.

None of this helps executives to sleep well at night. They are battling against a tide of information, down to a micro level of detail, and they and their frontline staff cannot easily keep

“The portfolio of risk is broadening. And it’s changing from quarter to quarter.”

Scott Mitchell, CEO, Open Compliance and Ethics Group
up with it. Nevertheless, regulators hold them responsible for acting on such information. To help keep tabs on complexity, keep regulators at bay, keep stakeholders informed and continue to deliver performance against KPIs, a well-planned and responsive GRC structure is crucial. If not properly established, executives will remain in reactive mode, continually distracted by the latest crisis and unable to take a proactive role in shaping risk management in order to increase the value of the organisation. They may find themselves liable too in the event of losses arising from a preventable breach.

“The portfolio of risk is broadening,” says Scott Mitchell, CEO of the Open Compliance and Ethics Group (OCEG), a non-profit think tank based in Arizona, aimed at helping organisations align their governance, risk and compliance activities. “And it’s changing from quarter to quarter.”

Using GRC as a resource

Forward-looking companies see the underlying value of implementing corporate GRC measures to keep better track of business processes. Others view these functions as a drain on company resources. Far from fulfilling a hazy ideal, a strategic focus on GRC integration can raise the company's status in the eyes of investors, improve internal operations and company data, and ultimately increase competitiveness in the market.

“We will be more competitive,” confirms Mr Marques of Lusitania Companhia de Seguros. “The insurance business deals with a lot of intermediate people. They’re very concerned with new regulations. If we can show them we’re ready to face new challenges, we’ll be ahead of competitors.” Although Lusitania has not formally quantified the competitive impact—more customers, increased revenue, lower operating costs—the company anticipates significant future benefits.

The change in emphasis towards using GRC to add value requires a shift away from traditional approaches, however. Instead of paying lip service, “If you embrace GRC wholeheartedly and take an integrated, enterprise approach, it’s going to cost less than a collection of fragmented processes.”

Lee Dittmar, global leader GRC, Deloitte

in response to external pressures, the internal organisation must adapt to apply best business principles to manage risk. When this is achieved, expenditure falls too.

“If you embrace GRC wholeheartedly and take an integrated, enterprise approach, it’s going to cost less than a collection of fragmented processes,” says Lee Dittmar, Deloitte’s global leader for governance, risk and compliance consulting. “You will be taking out unnecessary complexity, and should be able to re-deploy resources elsewhere.”

GRC has gained the attention of senior management in a wide range of government
organisations as well. For example, according to a local government authority in the UK, Wolverhampton City Council, which serves 250,000 citizens: “Risk management is an integral part of the Council’s corporate governance arrangements and has been built into the management processes as part of the Authority’s overall service delivery framework.”

A benchmarking survey published in early 2007 by ALARM, a UK association for risk management in the public sector, showed that risk management is “clearly embedded” in strategic plans for more than three-quarters of cases. Peter Andrews, ALARM’s chairman, adds: “It is significant that 70% of respondents confirmed that risk management is contributing to improved performance.” Overall, compared with a previous survey in 2003, there has been “a considerable increase in the contribution that risk management is making to the achievement of corporate objectives, delivery of innovative projects, targeting of resources and improvement in service delivery”.

A different picture appears in emerging economies, several of which are host to major collaborative partnerships. Chinese companies, in particular, have never had a culture of risk management and compliance. The focus has been on cost and delivery. However, things are changing in China too—as they must, with the integration of China into the global economy.

“Large state-owned enterprises have felt above the law in China,” says Douglas Clark, managing partner of law firm Lovells’ Shanghai office. “They certainly don’t now. Risk management is getting higher on the agenda in large companies in China.”

Elsewhere in Asia, adequate risk management has also been lacking in many companies. The ninth global fraud survey by Ernst & Young shows that levels of fraud in India have increased acutely in the past two years. Sixty-eight percent of the respondents from India said in the survey that their companies do not provide formal training to their employees so that they can understand and implement anti-fraud policies. According to Ernst & Young, the findings of the survey reveal that “India Inc. has a long way to go in terms of fraud risk management”.

Preparing for trouble in China
Chinese companies have until recently been able to ignore GRC issues. But there is now a much stronger interest among those exporting and selling overseas, or those listed on foreign stock exchanges, to avoid legal recrimination. Chinese companies that previously had 30-40% of their business abroad are now likely to find that it is 60-70%. (Perhaps the most dramatic shift has been for an indigenous firm, Lenovo, which became the third-largest PC maker in the world after taking over IBM’s personal computing division.)

“Five years ago, no one understood risk manage-

---

2 Ernst & Young, Fraud risk in emerging markets, June 2006.
Fortifying the enterprise: Governance, risk and compliance strategies

“Five years ago [in China], no one understood risk management in a mature way. Now awareness of the risk of non-compliance is growing.”

Robert Lewis, managing partner of Lovells’ Beijing office

“Five years ago [in China], no one understood risk management in a mature way. Now awareness of the risk of non-compliance is growing.”

Robert Lewis, managing partner of Lovells’ Beijing office

ment in a mature way,” says Robert Lewis, managing partner of Lovells’ Beijing office. “Now awareness of the risk of non-compliance is growing.”

There are signs too that the Chinese government is taking GRC more seriously, now that the economy is closely tied with international markets, and with the country moving from a planned to a market economy. The State-owned Assets Supervision and Administration Commission (SASAC) formed in 2003 is responsible for overseeing state-owned enterprises and protecting investors, and is pushing for stronger corporate governance.

Regulatory enforcement in China remains “spotty” at best, says Mr Lewis, as many regulators lack sufficient enforcement authority. Shareholders have no real legal redress. And the holding companies that often run multiple provincial state-owned enterprises have long histories of autonomy.

Chinese companies are struggling to emerge from an environment void of a culture of GRC. However, “legal compliance is massively underdeveloped,” says Mr Lewis. “On the face of it, [companies] feel comfortable if their guidelines are compliant—but there is zero infrastructure to implement them.”

For example, China Aviation Oil (Singapore) was involved in a trading scandal in 2005, after which its CEO was jailed and the company fell. This was not the result of an absence of a stated governance policy, but there was no infrastructure to monitor activities or to hold anyone accountable. “Corporations in China are like large bureaucracies. It’s difficult to change this,” says Mr Lewis. Often, he says, “the only teacher is a knock on the head”.

But behaviour is starting to change. For a start, SASAC is taking a lead in setting up assessment criteria. The dense bureaucracy is becoming more streamlined. Brighter and more sophisticated managers, many of whom have studied abroad, are appearing. Mr Clark of Lovells’ Shanghai office adds that the position of general counsel is becoming widely established in Chinese firms.

If there’s a downturn in China’s economy, however, there’s a feeling that “the veil will be lifted”, and the threat of shareholder actions will bring about a focus on GRC. Often a shock has to occur for the company to become more risk-aware. One Chinese manufacturer of engineering parts that started exporting to large international vehicle brands soon discovered that its defect rate put it at severe legal risk. Although fixed relatively quickly, the CFO describes it as “a very painful experience”.

© The Economist Intelligence Unit 2007
Multiple regulations, common requirements

Different industry sectors face different regulatory requirements. For instance, financial services firms must wrestle with a whole thicket of unique regulations ranging from Basel II/IA to the Markets in Financial Instruments Directive (MiFID) to Gramm Leach Bliley. But there is also much common ground among the requirements.

“There are domains of risk and compliance that are company- or sector-specific, but there’s also a core commonality: to keep operating within certain boundaries,” says Mr Dittmar of Deloitte. He contends, for instance, that there is as much as a “90% overlap” between Sarbanes-Oxley and the 21 CFR Part 11 regulations concerning IT controls. Given the steep increase in the number of regulations, searching out common features could be a matter of survival when it comes to implementing them.

Often it is a crisis that triggers a company’s scrutiny of its GRC processes and systems

Often it is a crisis that triggers a company’s scrutiny of its GRC processes and systems. One example is Tyco International, a manufacturing group with operational headquarters in the US. Following a finance scandal that resulted in jail sentences for the CEO and CFO, risk management was centralised and its role significantly strengthened. And there was no longer a question of the high priority of strengthening the company’s GRC arrangements.

Research by Deloitte has shown that large tumbles in a company’s equity price are caused not by a single catastrophic event, but a coincidence of multiple risks acting in concert. Therefore companies focused on maintaining shareholder value should avoid focusing simply on the next big crisis. Instead, they should develop a comprehensive and detailed understanding of the myriad risks across the enterprise.

Human resources: risk minefield

When asked about the most treacherous risk minefield of all—faced in every country and industry sector—many executives would pick “finance” or “IT” or “supply chain”. Instead, the most perilous area may be employment law and human resources (HR) policy—especially in multinational corporations spread across multiple cultures. “Statistically, a company’s largest risk is employment,” says Mr Mitchell of OCEG. “SOX [Sarbanes Oxley] is way down the list for retailers compared with issues as ‘wage and hour’ and [other] HR issues that are driving large class action lawsuits.” Mr Dittmar of Deloitte agrees: “Employment compliance is worse in complexity.”

New legislation is continually introduced to protect employees from employers, for instance via directives from the European Union. And class action suits are also beginning to be seen in Europe. A recent issue has involved the loss of overtime entitlements by staff promoted to management.

Collaboration begets risk

Meanwhile, most large organisations are exposing themselves to new risks when they are forced by competitive factors to collaborate across borders. A growing number of collaborations are appearing as
companies move to more open models of research and development (R&D), product development, product distribution and, most importantly, far-flung supply chain networks.

A range of security issues need to be reviewed during the earliest stages of collaboration, as the company network opens up and brings together diverse groups from inside and outside the company. Questions that must be addressed include: Who will own the intellectual property? How secure is the service? The network? The storage of shared information?

To share information securely with external firms on a converged network, IT security teams from both companies need to get together and work out who will have access to what information. The network access method and security must be fully tested before launching the collaboration capabilities.

In a recent survey\(^3\) carried out by the Economist Intelligence Unit and AT&T, more than one-third of executives saw the loss of intellectual property as the main risk in entering a collaborative relationship. The China partnerships of many foreign companies have suffered as weak local enforcement of intellectual property laws has led to the loss of trade secrets. Slightly less than one-third of executives surveyed (30%) are extremely wary of reliance on partner firms in areas that are core to their company’s success. A further concern—reputation risk arising from association with another company—looms for around one-quarter of executives. They worry, for instance, that a partner may violate local laws on data privacy or employment. Allotting partners different levels of access to the corporate virtual private network (VPN) through individual “profiles” is one useful measure, especially as some partners are often also competitors.

Since collaborative relationships are not always long-term, the parties need to understand what happens to information once the project ends. The supplier of information must review the arrangement to determine the potential for the partner to leverage the information for other means. Only then can the benefits of the arrangement be realised.

“Statistically, a company’s largest risk is employment. Sarbanes Oxley is way down the list for retailers compared with HR issues.”

Scott Mitchell, CEO, OCEG

IT risk

The performance of IT is also now central to the success of the business, and systems failure or breaches of information security are among the highest threats to any organisation. Breaches not only disrupt business but also bring unwelcome attention from the press and consumers.

Although they are usually well aware of the threat posed by viruses and hacking, executives may fail to grasp the full implications of IT risk to their business. The impact of, say, a new website application under-performing or customer records getting corrupted can be as damaging as a strike by employees. IT applications are today behind almost all critical processes

\(^3\) EconomistIntelligence Unit/AT&T, Globalisation and networking, June 2007.
Fortifying the enterprise: Governance, risk and compliance strategies

needed to run the business—from payroll and billing, to customer service and supplier management, not to mention regulatory compliance. And as the influence of IT performance on business outcomes grows, so does the risk to the organisation.

One example of the destruction that can be caused by overlooking the “middle ground” (areas unrelated to dramatic virus or network intrusion attack) is Comair, a US regional airline, which left almost 200,000 people stranded in 2004 after cancelling all flights on Christmas Day and Boxing Day. The reason was a software flaw: the system that assigned flight crews crashed after running up against a hard-coded limit on the number of permissible changes each month. The incident cost Comair US$20m, hurt Comair’s reputation and ultimately led to a government investigation.4

Conversely, there is greater awareness than ever before of the risks presented by IT. Take the case of Kevin Bott, CIO of Ryder, a Miami-based transportation, logistics and supply chain solutions company. Mr Bott is engaged in three main areas of the business: managing supply chain outsourcing, which demands high systems availability to keep goods moving; the leasing of tens of thousands of vehicles; and supervising internal back-office systems, some of which require highly sophisticated risk management, partly driven by Sarbanes-Oxley requirements. Under Mr Bott, mission-critical systems require 99.1% end-to-end uptime. Failover networks and servers are key parts of Ryder’s technical defence, combined with advanced monitoring tools.

Risk management is shared between IT and business, and meetings are set up to discuss risk before projects start. If creating solutions for customers, participants are also invited to discuss risk before embarking on the project. “Security is built into everything we do,” confirms Mr Bott. He believes that people, processes and tools all have to be up to standard for effective risk management.

Tae Park, CIO at Greatbatch, a developer of components for medical devices based in New York, points out that there is a danger that the easier IT gets to use, the harder and more complex it is to secure. With the proliferation of mobile devices, further security issues arise as more sensitive data are carried around in laptops, thumb drives and other remote devices. He says that today IT risk is directly related to regulatory risk: “We have to make sure we’re diligent about the risk of system failure. It’s not just about shipping [products] late. It could mean a regulatory breach.”

Commonalities across industries

There is also commonality across industries and geographies as to what works well and what doesn’t. Most experts agree that the best way forward lies in encouraging collaboration among those responsible for GRC, including corporate compliance, enterprise risk, audit, IT, line-of-business, and legal, as well as forming a common framework and technology infrastructure.

“Integration” is the key word. To get an understanding of risk across the enterprise, Mr Dittmar of Deloitte recommends, as a practical move, that organisations call together stakeholders from different areas for half-day workshops, for instance, to define the risk they face, discuss their current approaches to GRC and “where they want to go”—and the work needed to get there. To fulfil GRC aims, they must ask: Is it process change, education or technology that needs attention? A roadmap must be developed, buy-in obtained and enterprise-wide metrics applied. GRC implementation has to be a multi-year initiative with stated goals and metrics. A major benefit, according to Mr Dittmar, is that “the process will show up inconsistencies across the enterprise, and highlight

Integrating risk: Lusitania Companhia de Seguros

Spiralling regulations and the need to manage capital better have sparked a major GRC programme at Lusitania Companhia de Seguros, a Portuguese insurance company. Jorge Soeiro Marques, chief risk officer, says that before starting the project the firm undertook a series of internal studies and benchmarks against competitors to understand which factors could help to manage capital more efficiently.

“We wanted to face risks in an integrated way and to find out which risks interfere with the management of the company,” he says. “After we started to implement the project, we found a lot more efficient ways to manage our portfolio.”

The company turned to the Open Compliance and Ethics Group (OCEG) guidelines in forming GRC policies covering key supporting areas such as HR, infrastructure and technology. Over the past two years, the firm has been implementing Phase I of its GRC programme, setting up a governance and control model as well as a department for risk and internal audit. The board is implementing the new governance model. “We have carried out risk-mapping and have made some ‘quick wins’ in overcoming risk,” says Mr Marques. The company is applying the risk model to budget and strategy plans over the next three years. Most of the project has been implemented.

Phase II will largely cover internal enterprise risk management. Mr Marques says that the company had inadequate HR and skills resources two years ago, but now has what it requires with a risk team including actuaries and a market risk manager.

This phase will change the internal culture. “We have to change the ways we manage risks,” he explains. “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.” Mr Marques was heartened by an internal survey in which the majority of staff described the risk management programme as an “opportunity” when compared with other options such as “danger” or “adventure”.

Hard work lies ahead. “We need to transmit to the whole organisation the changes in how we manage investment, claims and contracts with clients, and how we face competitors,” he says. Goal charts have been set up with scores for different departments such as marketing and IT, and different risk “councils” established to cover areas including ethics and social responsibility, internal controls and agents.

Also, internal committees are charged with transmitting risk information to staff across the organisation. “Their role is to help the whole organisation understand what is needed for the future, and to better manage resources.” Several channels are used for communicating risk policy and regulations, including internal meetings, workshops, newsletters and the intranet.

“We couldn’t manage risk without good internal IT systems,” confirms Mr Marques. Central to this is a very sound database, combined with IT staff resources and risk management technology solutions. The GRC implementation programme will continue to the end of 2010—in time for the deadline for the implementation of yet another major regulation: Solvency II.
opportunities to better manage risk. They’ll show up across global operations.”

Furthermore, when projects relating to governance, risk and compliance are introduced, they will be done so within the overall agreed enterprise GRC plan. In the end, complexity—a major source of increased risk—is reduced by integration.

True integration can only work of course if supported by the right corporate structure—or only tinkering will ensue. The existing structure may need to change. “[Our] research has shown many benefits of integrating governance, risk management, internal control and compliance processes,” says Mr Mitchell of OCEG. “But integration doesn’t mean consolidation under a single individual...That’s a recipe for disaster.”

Instead he believes that responsibility should be shared across different functions, and embedded within mainstream business processes with the CFO managing financial strategy and compliance, the chief ethics and compliance officer (CECO) handling non-financial issues such as antitrust, environmental and competitive practices, and the chief audit executive “providing assurance that the full portfolio of financial and non-financial controls are designed and operating effectively”. He recommends that the general counsel not be the CECO, as the roles can be at odds: the job should go beyond the legal strategy and protection of the company. He regards this as the most “elegant” GRC structure that balances the competing priorities of proactively managing risks while providing objective assurance that the system is effective.

Mr Mitchell says that an emerging best practice is the use of a GRC “center of excellence” which owns the tools, methods and approaches that are used by GRC executives and other mainstream business process owners. “We will know that all of this is really succeeding when mainstream business executives are responsible for the risks related to their own processes. When bribery risk, for example, is owned by the VP of Global Sales rather than by some attorney in headquarters.”

Mr Mitchell’s philosophy is “centralise information and monitoring, but decentralise implementation and management”, and he draws a parallel with CRM (customer relationship management) where there are distinct roles for the call centre and the sales and marketing function—they have to collaborate, but that doesn’t mean they should be consolidated.

He says that the influence of the chief audit officer has grown over the past five years as “the objective party”, able to give an independent view internally of risk issues. Generally, he believes that the status of internal audit is increasing.

Several other factors have to be considered and applied in order to create a robust and effective GRC structure, however. There is a need for good communication between different security units in the company. Does physical security talk to IT security? They cannot operate effectively in isolation—the two may need a single head. Successful long-term GRC depends too on making business continuity an integral part of company strategy. Business continuity requirements need to be understood, and rehearsed, by all key staff from the board downwards.

Encouragingly, Mr Mitchell cites recent research showing that success rates among those that have integrated GRC have risen sharply from the previously low records—86% compared with former averages of 25-40%. Furthermore, results from a field study announced in early 2007 by AMR Research, a US-based research group, showed that a majority (54%) of firms planned to increase their budgets for risk management in their supply chains over the next 12 months. Of those firms, the average spending increase will be 17% year on year. However, implementing thorough GRC—including proper enterprise-wide metrics—is an ongoing process that may take years to achieve.

---

Fortifying the enterprise: Governance, risk and compliance strategies

IT’s defining role

GRC will only work when supported by properly tuned IT systems (themselves a major source of risk). It is through IT systems that data concerning risk will be brought to executives. “Fragmented” information—for example emanating from several different ERP (enterprise resource planning) systems—must be brought together and streamlined. In addition, systems need to be able to spot approaching risks—for instance, if several employees’ conditions have changed to the point where they may take class action against the employer.

But IT operational “silos” that occur in large organisations must first be linked. Then executives will be able to make informed decisions based on real-time views of enterprise-wide data. A further challenge is that many infrastructure technologies have been implemented with inadequate settings for controls, or with insufficient granularity to meet requirements.

GRC technologies are available that allow management to access relevant compliance and governance information, and examine how internal controls are working. They also carry out a range of functions such as enforcing separation of duties to reduce the potential for fraud—for example, an individual responsible for paying a vendor cannot also change the vendor master record. The technologies overcome traditional ad hoc and slow manual methods and reduce a great deal of back-and-forth between IT and business staff.

Having implemented GRC tools alongside its ERP system, Greatbatch found that it had a firmer handle on risk across the organisation. The company has also saved time and costs by carrying out testing and other functions manually. “We’re getting closer to continuous monitoring and can find things out faster,” says Mr Park. He adds that, more importantly, the audit staff of the company is starting to trust the viability of the GRC tools.

Operating in the medical industry, Greatbatch is heavily regulated. FDA, ISO and EU rules are among those that must be addressed. “The [GRC] tools help us to forecast better and show the interdependencies between the regulations—how they intersect,” he says. “In an age of proliferating regulations, they help to leverage the overlap between the mandates, saving duplication of effort.” He believes that with the prevalence of M&A, having these tools becomes a necessity.

Mr Park maintains that GRC is becoming an increasingly important factor in the job of the CIO, but emphasises that GRC tools are for use by the business rather than IT staff. GRC acts as a support in fact for business/IT alignment, raising the visibility of IT. Mr Park has found too that a step-by-step approach has been effective for deploying the tools at Greatbatch—as opposed to the “big bang” approach—building momentum from successes, but “some internal marketing is needed”. Above all, however, “management support has to be there”.

GRC technologies are available that allow management to access relevant compliance and governance information, and examine how internal controls are working.
Fortifying the enterprise: Governance, risk and compliance strategies

Conclusion

It would be naive to pretend that GRC implementation is well advanced in most organisations today. Most actions to improve risk and compliance are implemented in isolation rather than as part of a systematic approach. It is rare that an organisation has the appetite and leadership to take on a grand programme of GRC integration. Nevertheless, starting in the developed democracies of the OECD countries, boards of directors are at least acknowledging the need for an integrated approach to GRC. It is hard for them to resist the argument that an integrated approach brings about more consistent and cost-effective protection and allows companies to develop greater responsiveness in the face of escalating risks.

The process of changing attitudes towards risk and compliance can be slow and painstaking, but it is worth it. The key is sustained leadership from the top of the organisation. As one commentator put it: “It won’t happen by accident.”

GRC Do’s and Don’ts

Executives interviewed for this paper have been intimately involved with GRC implementation at their own companies and as advisers to other companies. Their recommendations on what to do and what to avoid in implementing a GRC programme are listed below.

**Do**

- Determine what overlap exists between apparently differing regulations and seek out economies of scale in addressing them.
- Focus on gearing IT systems to provide executives with GRC summaries across silos.
- Use integrated GRC to reduce complexity—not increase it.
- Communicate risk policy down to the most junior members of the organisation—through a range of methods: intranets, special committees, newsletters, e-learning and workshops.
- Underpin GRC with sound business continuity planning; it needs to be understood across the firm and rehearsed regularly.

**Don’t**

- Expect fast results—the process of fully integrating GRC into the company culture is likely to take years.
- Overlook HR and employment risk: these can pose more danger than higher-profile areas such as financial and operational risk.
-’t try to guess future crises, while overlooking smaller risks: the greatest damage can come from a series of small events happening simultaneously.
- Approach GRC as a burden on resources: when the company is known not to leave things to chance, market value rises. (Business risks can then be taken safely.)
- Attempt to consolidate GRC “under one roof”: allow responsibility to be shared across the relevant functions.
- Wait for a damaging incident before taking action (which could have prevented it in the first place!)
While every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in the report.