Risk and regulation

Making smarter risk decisions

Reinventing risk*

*connectedthinking

PRICEWATERHOUSECOOPERS

Contents

‘In examining the risks (in U.S. foreign policy) I also felt it important to examine the consequences of failing to act… Our purpose should not be to eliminate risk, which is impossible, but to manage it, which we must do if we are to prosper.’

Madeleine K. Albright, former U.S. Secretary of State

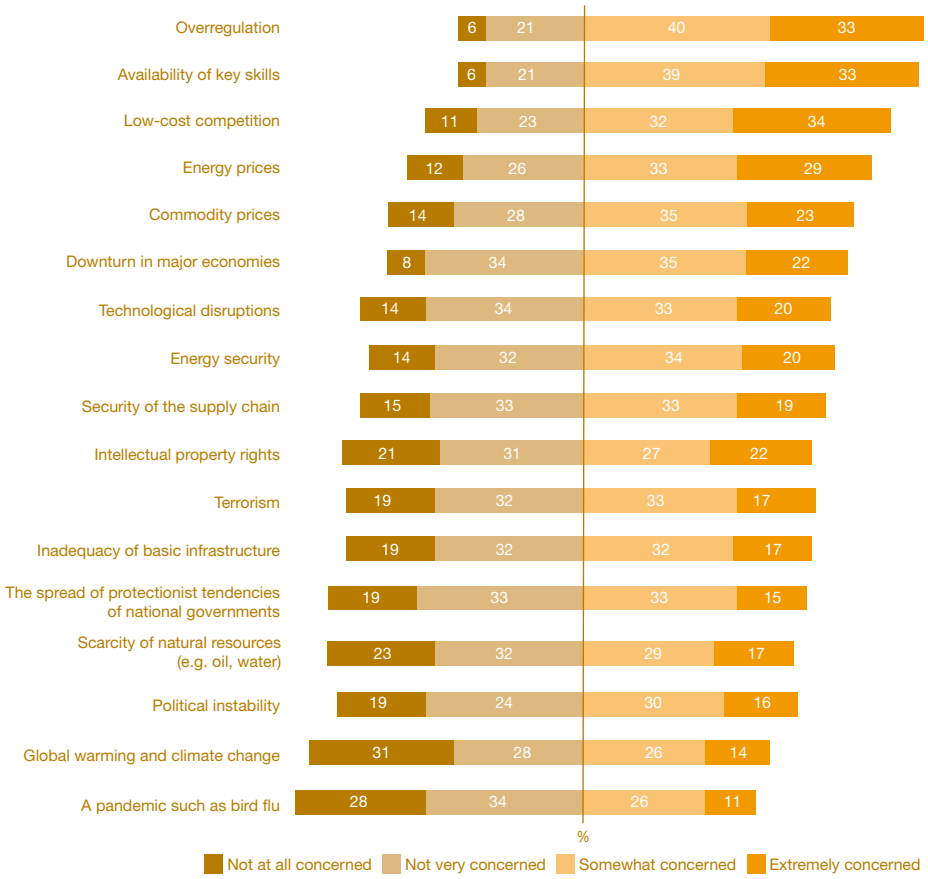
Reinventing risk

Enron, Worldcom, Parmalat, Adelphia. Each one a different case with a larger or smaller number of “bad actors”, but each one fundamentally the same story – the result of risk taking by people who failed to assess or acknowledge both the opportunity and the possible consequences of their individual and/or collective actions. In the end it is the human element that leads to success or otherwise – it is about enabling people to consistently evaluate the circumstances and make the best decisions possible for the business and all its stakeholders.

Arguably, the controls and transparency provisions of the 2002 Sarbanes-Oxley Act in the United States addressed this issue, holding managers personally accountable for the accuracy and truthfulness of their protocols and forcing more focus on evaluating both the potential rewards and pitfalls of risk taking. Yet the effect has been to give the impression that risk is something that can be largely eliminated through ever deeper layers of controls and sign-offs. Now the pendulum appears to be swinging back. While there is still a spotlight on some organisations that seemingly take too much risk at the expense of their license to operate, it is recognised that more and more organisations are failing to thrive. We believe it is because their approach to risk and regulation makes it difficult for them to identify and seize the genuine opportunities that they need to exploit in order to thrive in the market.

In many organisations, each new risk or regulation is addressed by creating a new oversight or designing a specific new process – on the presumption that each additional control will bring them nearer to zero risk. In reality, the rate of change continues to accelerate – new risks, regulations and sometimes crises are identified, and in the majority of cases the measures put in place to manage them may actually increase vulnerability by adding complexity or clouding accountability. When something goes wrong and external forces implement additional regulation, these same organisations often apply a costly band aid of control. However, as in the logic of investment returns – the past is no guarantee of the future, so the resulting risk management systems are designed to eradicate what went wrong yesterday, not to manage what might go wrong tomorrow. This is exacerbated when explicit risk culture and risk appetite are not defined or understood, and misaligned risk systems and processes are seen as a universal basis for decision making.

Serious concerns about business and macro threats indicate CEO optimism is not unbridled



Q: How concerned is your company about each of the following potential business threats? (Base 1,084)

Source: PricewaterhouseCoopers Global CEO Survey

Is this the right approach, or is there a better way?

Business leaders acknowledge that managing risk and regulation has diverted resources away from other priority risk management activities that might support greater revenue generation or business growth. In PricewaterhouseCoopers' most recent survey of global CEOs, executives saw over-regulation as the greatest threat to business growth.

This further suggests that many organisations believe they have and must continue to eliminate risk through compliance. But in truth, risk has not been eradicated by regulation – it has been driven underground. The thing we should be worried about is not the burden of compliance, but the suppression of risk taking and problems that can be caused if management does not have a proper understanding of appropriate risk appetite and tolerance-enabling appropriate risk taking decisions. In our view, some companies have allowed the focus on complying with risk and regulation requirements to obscure an open discussion about risk taking thresholds. Other companies have made progress embedding explicit risk management into business decision making, but must still do more to create efficiencies and drive risk-based resource decisions to improve business performance.

This is particularly evident in the Financial Services sector. According to another PricewaterhouseCoopers survey of more than 400 senior executives in financial services organisations worldwide (conducted with the Economic Intelligence Unit), in the past three years the boards of many financial institutions have focused on risk management largely as a result of industry regulation. The involvement of risk management in strategic business activities has, in contrast, been patchy.

The survey suggests that new business risks are coming into focus as a result of increased stakeholder demand for cost effective sourcing, higher levels of customer satisfaction, and desire for risk and regulation cost savings and efficiencies. Leadership wants to increase the value that risk management functions add to the business overall.

Winds of change

Main drivers of change in risk management priorities over the next three years; % change from drivers of change over the past three years

Increased focus on risk management on the part of senior management and board	-14%
Regulatory pressure	-11%
Losses at our own institution	-6%
Governance scandals affecting other financial institution or major corporates	-5%
Changes in reporting standards	-4%
Threat of terrorist activity	-2%
Focus on social responsibility programmes	-1%
Increased levels of IT security risk	-1%
Increased levels of geopolitical risk	0%
Demands for corporate transparency and accountability	+3%
Increased focus on risks pertaining to people and behaviour	+3%
Increased offshoring activities leading to greater emphasis on business continuity	+4%
Levels of customer satisfaction and/or churn	+4%
Macroeconomic volatility	+4%
Financial market volatility	+4%
Increased stakeholder focus on risk management practices	+4%
Securing competitive advantage over competitors	+4%
Focus on cost reduction and efficiency	+5%
Aim of increasing value of risk management to the business	+9%

Source: PricewaterhouseCoopers EIU Survey, January 2007

It appears that while risk and regulation measures are desperately sought in the bad times, they are often ignored and underinvested in the good times reinforcing the belief that the "risk" policeman is only of value when something has gone wrong. And as the drivers for risk management shift, there is growing concern that if the regulatory heat fades, leadership may reduce its focus and investment in risk management – just when its potential to create value for the organisation has never been higher.

Our experience is that organisations outside financial services are facing similar challenges. Globalisation, sourcing, supply chain, stakeholder requirements and macroeconomic considerations all influence the way organisations should view risk and regulation.

Today's businesses must reinvent prudent risk taking within a desired framework of compliance to strike an appropriate balance between risk, return and growth to create lasting value. To be successful the two are inseparable.

What if an organisation could truly define and then embed its optimal culture of risk taking and compliance across the enterprise and significantly reduce the need for control functions in a detecting or oversight role. How much more internal and external value could be realised in such an environment?

But, how does the organisation bring this vision to life? At PwC we believe and organisation will need to consider:

- Aligning Performance & Conformance – artculating an explicit risk appetite to ensure potential gain and desired compliance are viewed in conjunction to govern action;

- Optimising Performance Through Effective Risk Taking – linking risk appetite to business strategy and operations; leveraging risk choices to support commercial benefit; and

- Embedding Risk Appetite in Organisational Cutlure – driving the behaviours and measures required to support consistent recognition and application of the desired risk appetite across all business units, functions and people.

Aligning Performance & Conformance

The focus of management should not be purely on either performance or conformance. There needs to be a balance. With this in mind, risk-adjusted performance measurement decisions are crucial to an organisation's ability to create sustainable value.

How does this differ from what most organisations have today?

- Risk appetite is explicitly set and communicated;
- Risks are systematically identified and managed on a consistent basis by accountable executives;
- Risks are explicitly considered when evaluating new projects / investments both on a standalone and portfolio basis;
- Business unit performance is measured on a risk-adjusted basis in order to obtain a clear understanding of where and how much value is created/ destroyed across the enterprise;
- Organisations learn from failures;
- There is a no-blame culture because employees are empowered to make the decisions required by their role in the context of risk appetite – doing the right thing even when it leads to suboptimal outcome is not punished;
- Strategic planning integrates risk management to ensure proper compensation of the assumed risks and optimisation of resources;
- The board and senior managers confidently make informed decisions regarding risk/reward tradeoffs related to existing portfolio of business and new opportunities; and
- Key risk indicators impacting business performance targets are properly controlled.

‘Without an integrated, consistent and repeatable set of control metrics, we could never achieve our true goal of aligning our risk appetite with our risk tolerance’

Chief Executive Officer, Financial Services Company, United States

Aligning performance and risk management for value creation case study: Entity performance management improvement

One of the world’s largest financial institutions wanted to increase its market capitalisation by more effectively linking growth, risk and return. While it already had strategic planning processes and sound risk management, it felt it could do more to drive performance. Accordingly, the institution set out to explicitly describe how it would manage its business activities to create consistent and predictably growing returns at an acceptable level of volatility. The strategy addressed:

- An Entity Performance Management Framework;
- Objectives of Managing Risk;
- A Governance Structure; and
- Governance Processes.

This allowed the institution to define and communicate it objectives and risk appetite to:

- Build comprehensive risk assessment into all business processes;
- Minimise earnings volatility;
- Support efficient use of capital and the performance evaluation processes;
- Report a comprehensive risk profile;
- Facilitate calculated risk taking;
- Channel resources to the areas of highest growth and highest potential returns;
- Control expected and unexpected losses; and
- Increase its market capitalisation over a number of years.

As also evidenced by this case study, it is only in looking at performance and conformance together through the broader risk lens that organisations can fully understand priorities and trade-offs.

Optimising Performance Through Effective Risk Taking

Reinventing risk management & compliance systems

The challenges to integrating risk management processes with strategic decision making and day to day operations are significant and numerous. Layered onto this are the demands imposed by those newer regulatory requirements such as IFRS, Sarbanes-Oxley and Basel II, and the fact that large multinational corporations are struggling to merge technology platforms so that they can obtain integrated management information. The need to meet deadlines imposed by these regulations has undermined the effort to integrate and automate reporting systems.

While IT integration is often a good starting point for organisations, it is only part of the journey when seeking to fully integrate an organisation's risk with their management functions. The real point is that risk management and compliance functions are typically housed in distinct silos. Environmental compliance or workplace safety data conventionally reports into a corporate officer responsible for environmental health and safety. But employee information, which may cover some of the same ground, conventionally flows through Human Resources. To tackle these issues for one international bank, PricewaterhouseCoopers created a completely integrated risk platform that allowed for the aggregation and filtering of data from both operational systems and risk management activities within the bank. Now, the bank leverages existing technology to support a more holistic view of enterprise risks and has replaced duplicative, error prone manual processes with comprehensive, timely, trusted monitoring and management reporting – and they are able to correlate risks that might have otherwise gone unnoticed until they gave rise to an incident.

It is not the mere integration of the reporting systems that gives rise to tangible business benefits – it is, in addition, the organisational and functional integration that leads to superior decision making and increased business value.

Redesigning risk management & compliance processes

Effectively integrating risk and compliance mechanisms is only the first step in re-evaluating the role of the risk and compliance infrastructure. Often, the intense resource and financial energy devoted to individual functions prevents examination of fundamental questions about risk and reward:

- Do we have a business model commensurate with our appetite for risk and risk tolerance?
- How can we organise our risk and compliance functions to enable us to assess business opportunities quickly and effectively to obtain gain competitive advantage?
- How would we need to be organised to reduce our reliance on and significantly reduce the need for our risk and compliance functions?
- How would our view of operation change if we looked at "compliance" as the outcome of the design and operation of our risk systems including our culture and reward systems?
- How can we create and utilise integrated risk and compliance dashboards that encourage managers to take appropriate risks with new business initiatives such as outsourcing, entering new markets, or investing in new technologies?

‘…Increasingly, large, complex organisations are taking an enterprise-wide compliance risk management approach to augment and better coordinate what had been fragmented and duplicative compliance activities. Such an approach puts local compliance activities within individual business lines into an integrated, global program, makes possible an understanding of compliance requirements and performance across an organisation and promotes consistency in responsibility, expectations, documentation, assessment and reporting.’

Mark W. Olson, Governor, US Federal Reserve

Integrating risk & compliance case study: Rolling out a strategic risk control and compliance dashboard

One of the world’s largest companies wanted to improve its control environment, consistency and efficiency. The Company instituted a control optimisation effort to:

- Increase coordination between control functions;
- Delineate responsibility and accountability;
- Reduce duplication; and
- Focus on elements with the highest impact on the control environment.

The company collected standardised risk, compliance and functional updates on current/emerging control risks. The team then designed, piloted and implemented a Risk Control and Compliance (RCC) Dashboard at the largest business unit to prove the concept and encourage participation and collaboration among the remaining RCC entities. The RCC Dashboard incorporated measures and input from each of the key risk and control functions at the company, including: Internal Audit, Compliance (internal and regulatory), Risk and control self-assessments, Legal, Operational Risk, Information Security, Business Continuity, Finance, Operations and Technology.

After the pilot was successfully implemented, the company rolled the dashboard out to a small, but diverse group of RCC entities in the organisation and established a core set of processes and tools to allow the client to continue the full roll-out of the RCC Dashboard to the remaining entities.

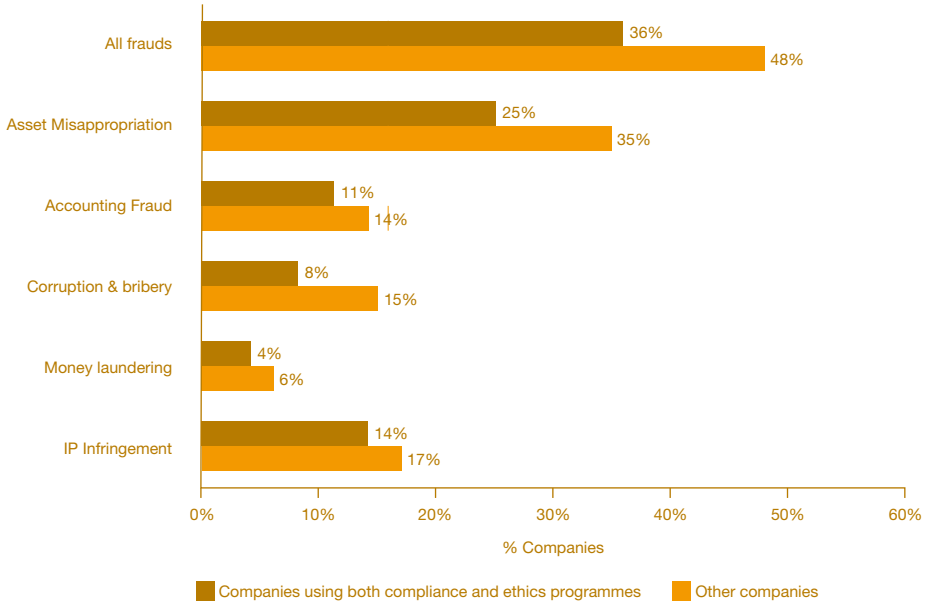
The RCC Dashboard has:

- Encouraged collaboration, and prevented duplication in reporting risk and controls across the Risk and Compliance Committees;
- Standardised control metrics; and
- Facilitated Risk, Control and Compliance meetings and provided a means of discussing control related issues and results surrounding each major business and geographical region.

Embedding Risk Appetite in Organisational Cutlure

Even when systems-related and organisational obstacles can be overcome, optimal risk decision making can only be achieved when the organisational culture understands, embraces and consistently applies the risk appetite to decisions and actions. While information flow is just one example of how culture underpins actions and results, it highlights how establishing a culture where the right people will do the right thing at the right time, regardless of the circumstances, is critical to an organisation's ability to seize the right risks and avoid the wrong ones. Developing this culture requires leadership to not only define risk appetite and ethical business standards, but to encourage employees to do the right thing through clear communication of objectives and risk appetite; incentive and reward systems that are aligned to employees "doing the right thing"; and role specific ethics, compliance and risk training programmes. It also requires that management be prepared to take a hard line with employees who don't "do the right thing", but not with those employees who truly "do the right thing" and achieve sub-optimal results. This further challenges management to ensure there is constant two-way conversation so employees understand "the right thing" regardless of dynamic shifts in the landscape that impact strategy and resulting execution. No matter how sophisticated the risk appetite, processes, systems or controls – if the underlying culture does not understand and commit to "doing the right thing", an organisation will not consistently make the right decisions to optimise business success and stay in compliance.

Companies with both ethical guidelines and compliance programmes report suffering fewer economic crimes



Source: PricewaterhouseCoopers 2007 Global Economic Crime Survey

A good example of this can be found when the issue is the prevention of fraud. PricewaterhouseCoopers' 2007 Global Economic Crime Survey demonstrates that only where compliance programs are combined with ethical guidelines, incentives and training do levels of fraud decrease.

Within the context of culture and reputation, compliance (ie, "doing the right thing") continues to play an active part in governing the relationship between the corporation and its stakeholders – board, management, employees, customers and suppliers, not just the regulators. And

‘No business deal can ever justify putting our company’s reputation risk’

CEO, Global Automotive Company

when “doing the right thing” is clearly articulated and integrated into the risk appetite and driven into culture, people can have an explicit dialogue about appropriate risks for the organisation. This will then encourage individual accountability for risk taking and mitigation throughout the organisation and make risk and regulation integral to the decision making process, rather than just a separate functional responsibility.

While it has been tempting to believe that at some point we would return to “business as usual,” the full flowering of globalisation in which we now find ourselves has made it perfectly clear that fundamental and not merely cyclical transformations in risk have taken place and are still under way. Continuous change forces us to adopt a new way of thinking about how to create and preserve value.

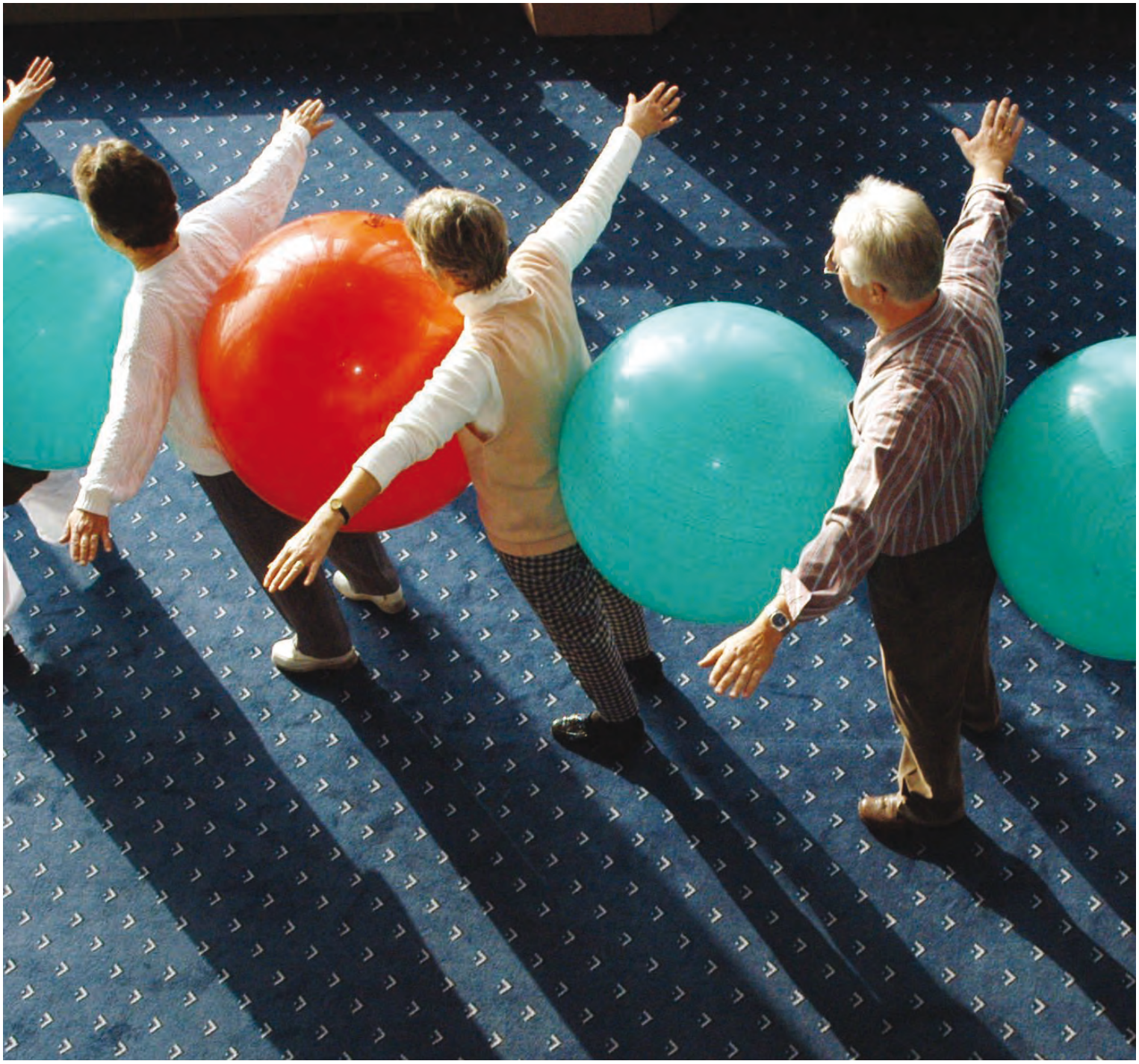
Organisations should ask themselves “what would my organisation need to look like” – what behaviours, processes and technology would need to be in place so that “control functions” are simply part of a fully integrated and effective risk management – upside and downside – where effective risk taking aligned to overall business strategy is a core skill and competency across the organisation. Risk exists and regulation (and therefore compliance) is just one of many risks that must be managed effectively to preserve and grow the business. With each new risk or regulation comes new opportunity for those who see the value, understand the trade-offs and can harness the benefits. Organisations that reinvent their view of risk through aligning risk taking with performance objectives, developing and fostering the complementary and necessary risk taking culture, integrating and optimising risk and compliance functions, will be positioned to identify, holistically assess and embrace those risks that will bring success and differentiate the organisation in the market.

Organisations that do not alter their way of thinking about risk can continue to use compliance as a security system and secretly harbour hope that one day pure compliance will be a differentiator.

But at PwC, we think that’s a pretty risky proposition.

Coordination and culture

Effective risk management requires the function to have a foot in all camps, straddling business units and groups, local territories and headquarters. It is imperative that these various groups are well coordinated. But clear processes provide one solution to this problem of coordination. For an organisation to truly optimise business success and differentiate itself in the market, the organisation must foster the complementary and necessary risk taking culture.



How PricewaterhouseCoopers can help

PricewaterhouseCoopers works to solve complex business issues – locally and globally. Our teams draw upon skills in finance, regulation, risk, tax, people, operations and technology to devise, deliver and embed lasting change. We advise and we implement.

In particular we can help you to:

- Assess and benchmark your organisation's risk maturity against core principles and industry practice;
- Engage stakeholders in the dialogue to adopt the right risk appetite;
- Design and embed appropriate risk taking into your organisation, through strategy, governance, performance management, operations and culture;
- Build business cases to drive integrated Governance, Risk and Compliance and integrated performance management;
- Improve risk & compliance effectiveness and integrate the response to risk & regulation across the organisation;
- Embed benchmarking and appropriate monitoring metrics;
- Integrate technology to support the application of these principles; and
- Manage through a crisis with confidence you are taking the right measures to remediate the problem and avoid relapse.

We take the time to listen to your situation and offer a range of smart choices to consider – choices based on independent and challenging insights, supported by facts and industry benchmarks. We help organisations reinvent risk and make risk choices to succeed. For more information please visit www.pwc.com.

Contacts

Australia
Sandra Birkensleigh +61 2 826 62808 sandra.birkensleigh@au.pwc.com

Belgium
Eddy Schuermans +32 2 710 7102 eddy.schuermans@be.pwc.com

Canada
Neal Oswald +1 416 815 5054 neal.oswald@ca.pwc.com

Germany
Christof Menzies +49 (69) 9585 1122 christof.menzies@de.pwc.com

HK/China
Rick Heathcote +852 2289 1155 rick.heathcote@hk.pwc.com

Netherlands
Hans Borghouts +31 (0) 20 568 6463 hans.borghouts@nl.pwc.com

Singapore
Keith Stephenson + 65 6236 3358 keith.stephenson@sg.pwc.com

South America
Federico Servideo + 55 11 3674 3989 federico.servideo@br.pwc.com

Switzerland
Juerg Wyser +41 (58) 792 2720 juerg.wyser@ch.pwc.com

United Kingdom
Steve Beet +44 161 247 4193 steve.w.beet@uk.pwc.com

United States
Miles Everson +1 646 471 8620 miles.everson@us.pwc.com

pwc.com