Inside this issue:

FEATURE
Successfully managing competition risk

EXPERT FORUM
Enterprise risk management

HOT TOPIC
Risk and compliance issues arising from third-party business relationships
Berkeley Research Group, LLC is a leading global expert services and consulting firm that provides independent expert testimony, litigation and regulatory support, authoritative studies, strategic advice, and document and data analytics to major law firms, Fortune 500 corporations, government agencies, and regulatory bodies around the world. BRG is headquartered in Emeryville, California, with 22 offices in the United States, Canada, and London, UK.

Follow us on LinkedIn, Facebook, and Twitter | @brgexpert

Berkeley Research Group, LLC is not a CPA firm and does not provide audit, attest, or public accounting services. Berkeley Research Group is an equal opportunity employer.
CONTENTS

04 FOREWORD

07 FEATURE
Successfully managing competition risk

13 FEATURE
Tackling innovation risks

89 EDITORIAL PARTNERS

19 EXPERT FORUM
Enterprise risk management
Association for Federal Enterprise Risk Management;
Airmic; PayPal

30 PERSPECTIVES
Enterprise risk management – the ultimate Rubik’s Cube
Women Corporate Directors

34 PERSPECTIVES
The upfront costs of compliance are looking more like a bargain every day
Berkeley Research Group

38 PERSPECTIVES
The role of the Chief Risk Officer
The Risk Management Association

41 PERSPECTIVES
Risk management and slow thinking
Santa Clara University

45 PERSPECTIVES
Integrated reporting
Australian Institute of Company Directors
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>PERSPECTIVES</td>
<td>How to minimise the risk of insider trading and leaking of material information</td>
<td>Berkeley Research Group</td>
</tr>
<tr>
<td>53</td>
<td>PERSPECTIVES</td>
<td>Risk management: practical lessons from preliminary due diligence in bank M&amp;A</td>
<td>NACD</td>
</tr>
<tr>
<td>60</td>
<td>PERSPECTIVES</td>
<td>Terrorism – is your firm prepared?</td>
<td>Pool Re</td>
</tr>
<tr>
<td>65</td>
<td>PERSPECTIVES</td>
<td>Planning and conducting cost-effective FCPA investigations</td>
<td>Baker &amp; McKenzie LLP</td>
</tr>
<tr>
<td>73</td>
<td>PERSPECTIVES</td>
<td>Progress, not perfection</td>
<td>Ethics &amp; Compliance Officer Association</td>
</tr>
<tr>
<td>77</td>
<td>HOT TOPIC</td>
<td>Risk and compliance issues arising from third-party business relationships</td>
<td>Airmic, Berkeley Research Group, KPMG</td>
</tr>
</tbody>
</table>
ANY TIME. ANYWHERE. ANY MATTER OF RISK.

Global Corporate Compliance
Welcome to the fourth issue of Risk & Compliance, an e-magazine dedicated to the latest developments in corporate risk management and regulatory compliance. Published quarterly by Financier Worldwide, Risk & Compliance draws on the experience and expertise of leading experts in the field to deliver insight on the myriad risks facing global companies, the insurance solutions available to mitigate them, and the in-house processes and controls companies must adopt to manage them.

In this issue we present features on managing competition risk and tackling innovation risks. We also look at enterprise risk management; upfront compliance costs; the role of the Chief Risk Officer; risk management thinking; integrated reporting; insider trading and information leaks; bank M&A due diligence; terrorism risk; planning FCPA investigations; and third-party relationship risks.

Thanks go to our esteemed editorial partners for their valued contribution: Baker & McKenzie; Berkeley Research Group, LLC; KPMG; Airmic; Association for Federal Enterprise Risk Management; Australian Institute of Company Directors; Ethics & Compliance Officer Association; National Association of Corporate Directors; The Risk Management Association; Santa Clara University; and WomenCorporateDirectors.

– Editor
Visit the new website

Sign-up to our free emailing list

Forward the link to colleagues and clients

Receive and enjoy future copies of Risk & Compliance
SUCCESSFULLY MANAGING COMPETITION RISK

BY RICHARD SUMMERFIELD

In an increasingly global market, companies face rising levels of competition. As such, it is natural that all organisations face some degree of competitive risk. In recent years, many big name brands have fallen victim to competitive threats left unchecked. Former industry heavyweights in their respective sectors, companies such as Kodak, Blackberry and Nokia have all been laid low when faced with aggressive competitors and unable to defend their market share. The failure of companies such as Nokia and Kodak demonstrates that, irrespective of the size of the firm, any company can easily lose market share and potentially their entire business.

When it comes to the demise of former industry superpowers, hubris can undoubtedly play a part in companies’ lack of response to emerging threats. However, one of the main reasons businesses fail to defend themselves effectively is often that they simply underestimate the size of the risk posed. Be
it from existing rivals or start-ups just entering the market, from a position of size and dominance in a particular field, it is easy to dismiss threats from smaller, seemingly inconsequential rivals.

When it comes to managing competition risk, for many businesses a sound defensive strategy can be incredibly important. Pushing back new entrants to the market and responding to competitors should be considered a top priority for anyone running a business, although in some respects it may be harder for larger firms to justify a major defensive effort against a significantly smaller threat. Often, companies are unable or unwilling to redirect vital spending from offensive programs without a compelling reason to do so.

Such failing companies may become over-reliant on products experiencing stagnating or falling sales. They may fail to adapt to new consumer tastes and trends, stick with a flawed or unrealistic pricing strategy or fail to embrace and integrate technology as effectively as their competitors. Many other variables can also impact the competitive position of a company, including training, marketing, location, policies, branding, recruitment and reward schemes.

In this context, the adoption of an appropriate and effective defensive strategy is clearly important. Countering the advances of new entrants to the market and responding to established competitors must be a top priority for any organisation wishing to remain competitive or dominant in their respective field. The first step to responding to a perceived threat is to carry out a thorough analysis of competition risk. Failure to respond to these threats can lead to disastrous consequences, particularly since the onset of the global financial crisis.

Although companies face a number of challenges and problems as a result of competition risk, they can also derive a multitude of positives from understanding and analysing competitive risks. In many ways competition risk can play a positive and pivotal role in helping to decide the fortunes of businesses.

Accordingly, the manner in which these risks are managed is important. Approaches to competition risk must not simply be about waiting for alarm bells to go off, indeed, management of competitive risk, is predominantly about preparation and behaving proactively. By taking positive action companies can utilise competitive risk to further enhance their own businesses and interests. Companies can identify risk warnings, develop recommendations for strategic adjustments to align with market shifts, and execute actionable plans in order to gain a competitive advantage over their rivals.

**Identify and analyse**

The identification and analysis of competition plays a vital role in managing competition risk. The first step of any defensive strategy should involve an evaluation of a company’s competitive threats.

By indentifying other businesses in the same industry and gathering information on their products
SUCCESSFULLY MANAGING COMPETITION RISK

FEATURE

and future plans, organisations can help to mitigate the impact these products may have on their own business. By studying the areas of rivals’ research and the scope of their investment, businesses can further evaluate whether these competitors pose a threat to their market position.

It is crucial that organisations evaluate their competitive threats accurately; by doing so they are ideally placed to plan and respond accordingly. A significant competitive threat can warrant a major response, be it in the form of a new product launch, which in turn makes it difficult for the new entrant to the market to arrange for distribution of
a product, an investment in promotions to block the competitor’s trial, or a new advertising campaign to raise doubts about the new entrant’s feasibility in the marketplace. A more extreme response may call for organisations to carry out multi-billion dollar acquisitions, either to strengthen their own position via bolt-on purchases or to buy out the new market entrant altogether.

Successful organisations should also analyse and manage their own core competences in order to stave off competition. In order to build a sustainable competitive advantage, organisations must first determine what it is that they excel at. In order to achieve this, companies must determine their core competencies. To develop a sustainable competitive advantage, and therefore mitigate the potential risks created by competition, firms must focus on their day-to-day activities which cannot be easily duplicated. By outsourcing non-core activities, companies can focus directly on what the business is really about.

**Defensive strategy**

A sound defensive strategy is crucial to manage competition risk. Knowing your market position is a solid starting point to any defensive strategy. In order to effectively navigate the competitive landscape companies must have a solid understanding of their place in the market. Is that organisation a market leader and the main brand in the category? Or is the company new to the market? By understanding their place in the industry, companies may be better placed to mitigate risk while still achieving innovation.

Once a company has established its position within its particular industry, it is important that it plays to its strengths. By accentuating the positives and hiding the perceived negatives, companies can better position themselves to benefit from their strengths. If a particular company has been always been seen as innovative, it should harness this innovation and utilise it as a core strategy when entering a new market or trying to gain additional market share.

“*If a particular company has been always been seen as innovative, it should harness this innovation and utilise it as a core strategy when entering a new market or trying to gain additional market share.*”

Agility is also incredibly important when it comes to developing a defensive strategy. At the height of their powers, companies such as Kodak and Nokia were unable or unwilling to adapt to new emerging
technologies and techniques. These companies demonstrated an inability to evolve as new players entered the market. Accordingly, it is crucial that organisations and business leaders future-proof their operations to the extent possible, in order to prepare for future growth. Companies must innovate with their products and services in order to adapt to emerging trends, by doing this they can help seal the longevity of their organisations, as well as helping to alleviate the threat posed by competition risk.

**Compliance**

One of the biggest issues companies face today with regards to the management of competition risk is compliance with global competition regulations. Many companies are beginning to awaken to the fact that they are now operating within an increasingly competitive global market. As such, the scrutiny firms are experiencing from global competition regulators is at an all time high. While this is particularly noticeable across the UK, there is also evidence of increased analysis of compliance across Europe and globally.

Increasingly, the onus is on companies to ensure that they have in place adequate measures by which they can achieve full compliance with competition laws. By meeting their compliance needs, businesses will be able to avoid the penalties associated with contravention of those laws. Significant fines, personal consequences for directors and extensive reputational damage are just a few of the issues companies have to deal with when it comes to competition compliance. In the UK particularly, companies face one of the toughest compliance regimes in the world. The office of fair trading and the European Commission are extremely active in enforcing competition laws.

However, by adhering to competition rules, companies are able to protect and promote long term, healthy competition within their respective industries. This competition, in turn, will help drive innovation.

Effective compliance regimes can be vital to the longevity of businesses; yet this compliance can only realistically be achieved if all ‘at risk’ employees have a clear and definitive understanding of the applicable compliance rules, as well as their own personal obligations within those rules. An effective program also requires that employees are fully aware of the importance of compliance to the business, as well as the procedures the company has put in place in order to help them better manage risk.

In order to better promote awareness of compliance, organisations should implement a number of training and monitoring systems, or ethics and compliance programs. These compliance structures must be supported and endorsed in a top down approach. Senior management and boards of directors have important roles to play in helping to establish a firm respect and understanding of the required compliance program.
Equally, company compliance schemes must be well funded, monitored and updated regularly if they are to be effective in promoting compliance. By educating employees and promoting an awareness of compliance issues, companies will have a better understanding of the hazards of competition laws and their inherent risks.

Furthermore, in an effort to increase compliance with competition rules, some organisations may find that they do not currently have a systematic competition compliance program in place at all. Clearly, for these companies, there will be a great deal of work required to ensure that they achieve compliance with the relevant legislation in a timely fashion.

To that end, companies must target high risk areas as quickly as possible, as creating and implementing a comprehensive competition compliance program will be both time consuming and costly. Organisations should design procedures and control systems in order to address gaps in existing programs. These measures will help support the effective and speedy implementation of policies.

These policies, however, should be proportionate and appropriate; being built into existing processes as far as possible, and should also mitigate the specific risks identified. A regulatory system that places considerable weight on leniency may lead some companies to implement detective, as well as precautionary, procedures and controls. The overarching aim should be to make competition compliance part of ‘business as usual’, rather than something that is seen as a standalone project.

**Conclusion**

Irrespective of a company’s size or its standing in a particular industry, it will always face considerable competition risk. In order to properly navigate and even profit from those risks it is important that businesses have an effective and appropriate risk management strategy.

Competitive risk management is the art, or even the science, of identifying early warnings well before they become public knowledge and building systems which help to turn these red flags into viable and realistic business opportunities – although it is imperative that companies also have the plans in place to alter course if needs be. Competition risk management is not about predicting the future; it is simply about being better prepared for it. *RC*
Innovation is a very powerful tool and a key driver of value, but all forward leaps come with some degree of risk. In light of this it is vital that organisations, irrespective of their size, champion innovation in order to move forward. Likewise, companies must be prepared and willing to accept failure in order to flourish.

However, in the current economic climate many businesses are fearful of the inherent risks of pursuing new ideas that may not ultimately succeed. Clearly, it is of paramount importance that companies strike the right balance between innovation and necessary risk.

There is a widely held belief that typically it is start ups that make the ideal staging ground for innovation, as they are generally free to pursue innovation uninhibited. The perception is that start up companies are more liberated, comprising of independent and self sufficient teams, able to develop products and ideas with minimal oversight.
If the assertion is correct and these smaller firms do indeed have significantly less to lose by pursuing innovation, the opposite is often thought for larger, more restrictive, structured organisations. However, when properly fused, the two disciplines of innovation and risk can help organisations of any size pursue profitable opportunities that more risk-averse companies might otherwise ignore. In this context, a suitable risk management program can help further a company’s innovation agenda.

In an increasingly competitive and global business environment, innovation has become a crucial issue for companies the world over. Yet, often an organisation’s management team is frustrated by the results. While the freedoms of speed and flexibility are coveted, they fear these notions will increase risk. As corporate imperatives, risk management and innovation are becoming increasingly important – creating a symbiotic relationship between the two is the next logical step. Risk management can be harnessed to boost innovation efforts by creating confidence that risks are well managed from the start. Moreover, far from proving to be a hindrance to innovation, refined, state of the art management tools and techniques can help to foster a more innovative atmosphere and encourage innovation across the board.

With each new innovation comes an inherent degree of risk. Vikram Taneja, Governance, Risk & Compliance Consultant for HCL Comnet Ltd, agrees. “Risk managers need to play a very critical role,” he says. “Innovation will always have risk associated with it. Therefore defining risk appetite as per the market environment for the organisation is one of the crucial roles played by risk managers. This is followed by assessment of risk and evaluations as per risk appetite and finally allowing those ideas to be implemented that would be associated with company’s risk management policies”.

Role of IT

Information technology (IT) also has a crucial role to play in helping to accelerate innovation. Arguably, IT is one of the most powerful enablers of innovation in the current climate. With the recent and striking rise of social media, crowdfunding and other trends, IT has assumed an even greater importance with respect to innovation. David Froud, founder of Core Concept Security Ltd, supports this assertion. “You cannot innovate until you know exactly how to do what you are currently doing properly,” he notes. “The IT department is perfectly placed to enable the business side to map its process, and then suggest ways to transform that process in line with the business goals. These goals are not necessarily related to dramatic changes, but can be as simple as increased efficiency, accuracy through automation, or even the removal of a non profitable process line. Technology is never a goal in and of itself; it is a business enabler if properly applied.” Crowdsourcing is another facet of IT which is helping to drive innovation. Many firms are beginning to turn to the
wider internet community, not only for funding but also for ideas to help drive innovation forward.

In many respects, principles for effective risk management within the sphere of IT are extremely relevant to managing innovation risk. The principles of risk management within IT include always linking with business objectives, aligning innovation risk with overall enterprise risk management (ERM), promoting fair and open communication of risk throughout the organisation and ultimately establishing the right tone from the top. Equally, it is crucial that boards and management help to define and enforce personal accountability among employees for carrying out innovation projects within acceptable and appropriate company defined tolerance levels.

**Trust in failure**

Despite the many obvious advantages IT can bring to the innovation process, it should not be seen as a panacea for all problems. Innovation in and of itself can lead to significant failures. There are many risks associated with innovation, not just the failure of a particular project. Costs can be driven up exponentially, valuable time eaten up, and the whole project may provide insufficient value for the investment made.

Yet despite these obvious drawbacks, in many regards failure of innovation initiatives can be seen as a positive or healthy development. Although global confidence is beginning to return as economies continue on the path to recovery, many companies are still not particularly inclined to embrace significant levels of risk for fear of these potential consequences. Despite the reticence of these organisations, however, it is arguably impossible to achieve revenue driving innovation without taking on some level of risk.

In order to sustain innovation, risks must be taken. Throughout history, from the internet and television, back to the steam engine and railway, companies, their subsidiaries and even entire industries have innovated and adopted risk. “Innovation in the information age is far more rapid than it has ever been,” says Mr Froud. “Competitive advantage is now measured in weeks and months as opposed to years, and any organisation hoping to stay in the lead must be able to innovate faster, make quicker

“It is crucial that boards and management help to define and enforce personal accountability among employees for carrying out innovation projects within acceptable and appropriate company defined tolerance levels.”
decisions and cut their losses when they make the inevitable mistake. You just have to look at the growth in ratings and reviews and big data fields to see that organisations are desperate for information that will enable them to make the best decisions they can.”

In order to encourage the use of initiative and increase innovation companies must embrace and even encourage failure. Although organisations should encourage well reasoned and thoughtful risk taking, employees should feel safe enough within their working culture to fail. Even in failure, companies can still discover unexpected information or develop skills which stand them in good stead in the future.

Many companies now recognise that they can allow innovation teams to make strategically intelligent mistakes within a clearly understood governance framework. This, in turn, enables a culture that not only tolerates risk but also embraces failure as an integral part of the innovation process.

Furthermore, despite the obvious challenges and pitfalls associated with increasing levels of risk, companies can ill afford to ignore innovation. With established players and start ups entering new markets, those organisations unwilling to pursue
innovation may soon find themselves pushed into irrelevance by their competitors.

With this in mind, one of the most important elements in managing innovation risk is creating a culture of trust. By trusting individuals to pursue new ideas on behalf of the organisation, companies can help to develop a culture in which teams and individuals are not afraid to fail. The ability to make mistakes within a structured and well-reasoned risk taking environment will enable people to feel safe with the choices that they make, free from the threat of punitive measures. This type of environment should empower employees to do their best work. It is of paramount importance that boards of directors and senior executives focus on managing risks and not stifling innovation.

The need to allow individuals to make mistakes must, however, be mitigated to a certain degree. Organisations should not, of course, grant employees total carte blanche. Unnecessary and avoidable risks should not be undertaken. Determining the feasibility of a particular risk can dramatically reduce the impact or undertaking of unnecessary risks in the future. If companies wish to grow, they have to grow accustomed to living with, and adapt to the challenges presented by, risk. Successful organisations provide individuals with the confidence and trust required to take necessary risks because they understand their importance to the future prosperity of the company. Successful organisations enable employees to take appropriate risks while eliminating those that are unnecessary. Cultural shifts within firms are necessary and must begin with the chief executive and board of directors. If they do not see that risk management enables innovation, no one else will.

**Rewards**

Another key way to accelerate innovation within the boundaries of a sympathetic risk management strategy is by rewarding employees for their insight and innovation. A corporate culture that only celebrates success can discourage innovation by making people nervous about taking risks. Organisations must also encourage and celebrate failures by their staff. Organisations should not be afraid to present staff with an almost equal reward for the biggest success and the biggest failure, presented side by side in a ‘safe’ environment.

While these rewards can take the form of monetary compensation, some organisations provide staff with spaces in which they can engage in recreational activities, games, naps and meditation facilities or specific time slots during which employees can feel free to be creative. Until very recently, Google Inc’s so called ‘20 percent projects’ encouraged employees to innovate. Companies must create a relationship between culture, performance management and reward in order to help foster innovation.

Mr Taneja agrees. “Organisations should reward and award innovative ideas or thoughts
appropriately. They can start with programs targeting innovations, such as best innovative idea contest, innovations of the year, etc. Each employee may be asked to do risk assessment of the idea versus the profit or gain the idea can bring.” Furthermore, he notes that technology can play an important role in helping to promote innovation. “Technology would be an enabler as well as a support function for ideas generation, assessment and the implementation process.”

Future developments
The future of innovation risk will be multifaceted. As organisations continue along the road to economic recovery, and hopefully prosperity, they will continue to look to reduce costs as much as possible. According to Mr Taneja “Innovative risk has to be assessed with respect to different factors associated with the company. Social, economic and political factors must be taken into consideration as well as the company’s plan for growth and its objectives going forward. Therefore, an understanding of risk and the creation of a risk management strategy – that is, top-down and bottom-up strategies – would be a challenge. Risk managers would need to understand those perspectives. This will widen the scope of risk management”.

The pace of technological advancement will also help set the tone for future developments within the field of innovation risk. “The rate of innovation will only continue to accelerate as the information age reaches the next level: the Internet of Things. With everything online, accessible instantly by anyone anywhere in the world, innovation will not be anything special – as it is now – it will be the norm,” says Mr Froud. “Larger organisations will adapt their R&D, marketing, and customer service departments into an overarching department in charge of new services and product offerings. The role of chief innovation officer will become far more mainstream and critical to the business.”

Ultimately, all innovation involves a trade-off between risk and return. In order to minimise risk and unintended consequences, companies must better understand how to make informed choices when it comes to their products and services. 

RC
EXPERT FORUM

ENTERPRISE RISK MANAGEMENT
PANEL EXPERTS

Dr Doug Webster
Co-Founder
Association for Federal Enterprise Risk Management
T: +1 703 441 2212
E: dougwebster@cambiocg.com

Dr Doug Webster is the founder of the Cambio Consulting Group, an organisation focused on business transformation through strategic planning, cost/performance/risk management, and organisational change management. He is the former Chief Financial Officer of the US Department of Labor and has two decades of management consulting experience. He is also co-founder and past president of the Association for Federal Enterprise Risk Management.

John Hurrell
Chief Executive
Airmic
T: +44 (0)20 7680 3088
E: john.hurrell@airmic.co.uk

John Hurrell was appointed as Chief Executive of Airmic in January 2008 following a career of almost 30 years in the Marsh and McLennan Group of Companies. Prior to joining Airmic, Mr Hurrell was the Chief Executive of Marsh’s Risk Consulting business throughout Europe and the Middle East. Having been educated in London, Mr Hurrell entered the insurance industry in 1968 and qualified as a Fellow of The Chartered Insurance Institute.

Erik Wilgenhof Plante
Senior Manager Compliance, South East Asia
PayPal
E: send2erik@gmail.com

Erik Wilgenhof Plante is a Senior Manager Compliance, South East Asia at PayPal. He is responsible for regulatory and operational compliance in South East Asian markets as well as India. Mr Plante’s specialties include compliance, anti-money laundering (AML), anti terrorist financing (ATF), know your client (KYC), due diligence, fraud, MIFID, corporates and markets, securities compliance, risk, sustainability, management, internet banking, insolvency law, FATCA and FATF. He is a regular speaker at international conferences and an experienced writer of policies and procedures.
RC: Could you briefly explain the importance of enterprise risk management (ERM) and the benefits it brings to an organisation?

Webster: All organisations exist to create value for stakeholders. That value is greatest when considerations of product and service benefits, costs and risk are optimally balanced in a way that maximises that value. Maximising value at the enterprise level requires balancing these considerations as part of a portfolio of products and services delivered by the enterprise. Enterprise Risk Management is the management of key risks across the enterprise in a manner that maximises the opportunity for achieving enterprise goals and objectives. This is accomplished by applying the principles of completeness, consistency, integration and strategic alignment in order to develop an enterprise-level portfolio view of risk that is not achievable when managed only within functional and programmatic silos.

Hurrell: ERM was originally established to help companies achieve compliance – for example, Turnbull or Sarbanes-Oxley. But many successful companies are now going further and have placed the ERM function at the heart of strategy to underpin corporate resilience and even to support competitive differentiation in their markets.

Wilgenhof: ERM allows the company to gain a holistic view on risk exposure and design proper controls to keep risk at an acceptable level. It also allows allocating ownership, which is very important as quite often lack of ownership makes implementation of controls impossible. Without ERM there is a risk of ‘blind spots’ even if there is risk assessment on a lower level. Risk management is often taken for granted and ends up as nothing more than a paper exercise. The main reason for that is that ERM tools are often seen as too blunt and too generic. In a sense, ERM works as a navigation tool, allowing senior management to map risks and put controls in place before they become too large to handle. You can’t use generic tools and expect a custom result though. It depends on the scale of the company and how it is organised. A small company may have fewer but relatively larger risks. A large multinational might have risks that exist in multiple jurisdictions. Too many companies still work as a cluster of small islands that are not interconnected. Different departments see each other as competitors for resources and funding. A generic ERM system will have difficulty detecting the risks between different parts of the company. Scalability is therefore crucial for an effective enterprise wide risk assessment.

RC: A key objective of ERM is gaining a comprehensive view of the varied risks an organisation may face. How should companies tackle this challenge?
Hurrell: Our ‘Roads to Resilience’ research with Cranfield has highlighted the exceptional risk radar capabilities of resilient companies. In these organisations, not only would they regard every employee as part of their intelligence network on risk issues but, in many cases, their supply chains, contractors and even customers would be part of the risk radar process. This not only requires a very effective communication network with all barriers removed but also a clear prioritisation process to turn this radar information into effective decision making.

Wilgenhof: You could fill several volumes on ERM implementation. It is not a self-contained administrative exercise but should be part of a continual cycle. Risk management is something everyone should be involved with, not just the risk department. The best way should be to involve all parts of the company, map out the risks and then prioritise them. This ‘heat map’ is the main tool to design controls, with input of the various subject matter experts. After implementation of the controls they should be constantly – not periodically – monitored and adjusted where necessary. Risk doesn’t have to be, and almost never can be, zero but should be within the company’s risk appetite bandwidth. It is almost impossible to get a full view of all risks. Known risks can be identified and controlled quite easy but there are unknown risks that often remain under water. Sometimes these unknown risks are kept under water because they may threaten results of departments or even individuals. The financial crisis was partly a result of risk kept from senior management and the regulators. These ‘known unknowns’ were ignored until they started to threaten the very survival of the financial system. Risk managers may be seen as doomsayers if they don’t quantify risks. This makes the task more difficult because unknown risks are by their very nature not quantifiable.

“Risk managers may be seen as doomsayers if they don’t quantify risks. This makes the task more difficult because unknown risks are by their very nature not quantifiable.”

Webster: ERM builds upon traditional risk management focused on functions or programs by implementing practices that support the following core principles of ERM. First is completeness – focusing on risks within specific functions or programs results in missing risks in the ‘white
space’. These are areas that impact the organization but are not assigned to any one particular individual for responsibility. ERM takes an enterprise-wide view of risk, not simply a role up of focused areas of risk management. Second is consistency – risks managed within silos typically apply inconsistent processes and reflect different risk appetites. While these differences may sometimes be appropriate, they often result from uncoordinated efforts that fail to benefit from lessons learned elsewhere. ERM brings a consistent, best practice approach to risk management across the enterprise. Third is integration – by facilitating a cross flow of information across functional silos and prioritising risks at an enterprise level, the enterprise is able to develop a portfolio view of enterprise risk and manage that risk to maximise enterprise value. Fourth is strategic alignment – effective strategic planning ensures organisational objectives align with enterprise goals and objectives. This top-down planning process requires a supportive risk management process that ensures alignment of objectives and risks with enterprise-level objectives. This top-down planning process requires a supportive risk management process that ensures alignment of objectives and risks with enterprise-level objectives.

**Wilgenhof:** There are various methods to determine risk. It would go a bit too far to describe every method but whatever method you use, input from employees is crucial. They are the subject matter experts and should be able to identify risk. Start with interviews and have people describe the various processes they use every day. This is also an excellent opportunity to show the importance of risk management and get buy in from the various stakeholders. Like compliance, risk management requires more than a knack for filling in forms. An understanding of how the business works and how the various parts interconnect should be the foundation of any risk assessment program. Senior management often has conflicting priorities but it is important to let them know what the residual risk – after implementation of controls – is so they don’t navigate blind. That’s the whole point of ERM. They should therefore always be kept in the loop.

**Hurrell:** Input from employees and senior management is absolutely essential. In our experience, risk managers will generally have a good understanding of operational risks but may not fully appreciate the strategic or reputational consequences of catastrophic operational failures. Boards and other senior managers, on the other hand, may have a very good understanding of strategic risks whilst not being close enough to operations to appreciate this type of exposure. This
was strongly highlighted in our Cass Business School research, ‘Roads to Ruin’.

**Webster:** There are a host of techniques to identify risks, including interviews with subject matter experts, Delphi technique, use of checklists and templates, risk workshops, etc. However, an important caution is to not immediately jump into identifying risks before first truly understanding organisation objectives. Too often organisations seemingly seek to identify risks without first agreeing on the objectives against which risks need to be managed. Regardless of the techniques used, it is essential that both senior management and employees are engaged in the process. Organisational goals and objectives should flow from the top down in order to ensure that the efforts of the organisation are aligned with the intended direction. However, the ability to achieve any set of objectives is always dependent on the capabilities and capacities of the organisation. While senior leadership can set direction, this direction needs to be consistent with the capacity of the organisation to deliver. Employees often have insights into gaps in capabilities and capacities that are not evident to senior management. Moreover, from an organisational change management perspective, employees are far more likely to support necessary changes when they know their voices have been included as part of the process.

**RC:** In any ERM strategy, risks must be prioritised for monitoring purposes. In what ways can firms prioritise risks for monitoring purposes, and how can they be ‘measured’?

**Webster:** Risk monitoring should be prioritised based on a combination of: the ranking of the risk, which is a function of impact and probability; the risk velocity, which is the speed with which an impending risk turns into an event; and the ability of the organisation to adjust or respond to risks moving towards adverse events. For example, there is no need to closely monitor the risk of an evolving demographic shift to the savings and borrowing habits of the population. This shift, which is currently underway in the US, presents significant risk to financial services organisations, yet it is predictable and very slowly evolving. On the other hand, the Fukushima Daiichi nuclear plant experienced a 2011 disaster from a tsunami, in which risks turned into adverse events in a very short time. Seismic monitoring allowed the evacuation of personnel to higher ground and saved countless lives. However, this same monitoring was ineffective for protecting backup power systems at the nuclear plant. Frequency of monitoring must thus be matched to risk velocity and the ability to respond to an adverse event.
Hurrell: Prioritisation will most frequently be based on materiality from a financial point of view. However, this approach often results in a failure to evaluate the reputational fallout from certain events. So we would recommend that organisations prioritise using both sets of criteria and in particular to focus upon – and to be realistic about – the reputational consequences of the failure of respective risks.

Wilgenhof: Prioritising risk depends on the company’s industry and risk appetite. If you are a financial institution that deals with large clients, your risk prioritisation is probably different from a company selling shoes or running a restaurant chain. Defining risk appetite should be done at board level and be part of an overall company mission statement. I would first try to map out all risks, no matter how small, after which those risks can be cross referenced with the mission statement. Some risks are not relevant and can be prioritised right away. Others will have to be kept in control. The largest known risks should have the highest priority. Most risks are measured in chance of occurrence, impact and monetary loss but sometimes there are large risks that cannot be quantified but should still be named. I don’t think any risk officer calculated the risk that an earthquake would cause a tsunami that would wipe out the cooling system of the Fukushima reactors. These ‘what-if’ scenarios should still be part of the plan somewhere, although they are often overlooked or ignored.

RC: How should firms weigh the perceived impact of a particular risk with the probability that it will actually occur?

Wilgenhof: As the financial crisis has shown, it is extremely difficult to assess future events. Another example of the failure of a statistical approach of risk is the Fukushima nuclear disaster. The chance that there would be a series of disasters resulting in the second largest nuclear disaster in history was very small but it happened nonetheless. Of course, there should be a prioritisation of risk factors as it is impossible to prepare for every risk. However, it is dangerous to leave risk management to mathematical formulas. Even if there is a small
chance that something occurs, it never hurts to be prepared. More often than not, the impact of a risk is larger than it should be because nobody bothered to prepare for it. An often overlooked factor is company culture. In Asian countries it is often not done to improvise. That makes it necessary to have scenarios for everything. Another often overlooked factor is reporting lines. Who should report to whom and who should be informed? Confusion often leads to unnecessary increase in risk.

**Hurrell:** We would recommend that firms focus on the financial impact, taking fully into account reputational consequences rather than to spend too much time analysing probabilities. It is possible to make all the right risk decisions having only three categories of probability for those risks which pass the materiality criteria. These are: risks that are highly likely to eventuate in the current financial period which have to be managed; risks that are so improbable after careful analysis that they can be safely ignored; and then everything else. It is the ‘everything else’ category where the majority of management time should be expended, and the focus should be around managing categories of consequence rather than identifying every possible trigger.

**Webster:** This is the subject of ongoing debate. However, two points must be made. First, the significance of a risk to an organisation is not simply the impact multiplied by the probability, in terms of dollars. This suggests that an impact of 100 percent of the value of the business having a 0.1 percent chance of occurring in any given month is equal in importance to the impact of 0.1 percent value of the business occurring every month with almost certitude. The latter becomes essentially a cost of doing business that is easily accommodated, while the former suggests a 50/50 chance of experiencing a catastrophic blow to the business within six years. These are clearly not equivalent risks. The second point is to always remember that impact and probability are rarely known for certain. These are in reality point estimates that reflect distributions. There are no easy answers to this question, but those seeking to manage risks should avoid assuming
more knowledge in evaluating and ranking risks than they actually have.

**RC: In your opinion, what primary considerations should firms make when implementing an ERM strategy? What aspects define an effective ERM program?**

**Hurrell:** Companies need to ask a number of questions about ERM. Does it add value at the front end of the business, particularly in relationships with key stakeholders? Does it help to inform strategic decisions? Does it engage management and staff throughout the organisation? Is it sustainable?

**Webster:** Too often enterprise level risk management is little more than an aggregation of risks within functional or program silos, sometimes with the addition of an enterprise level ranking and monitoring of risks. This is not, in my view, meaningful ERM. ERM drives a consistent and integrated approach to risk management across the enterprise that truly provides a strategically aligned, portfolio view of risk aimed at maximising organisational stakeholder value. This requires a chief risk officer or similar function that promulgates consistent risk management policy across the organisation, works with the board and executive team to develop a well-understood and communicated risk appetite, and facilitates the cross-functional dialogue necessary across business units and functions to balance resources and risks in a manner that optimises enterprise-level ROI in pursuit of stakeholder value.

**Wilgenhof:** The first consideration should be the scope of the risk assessment. How much money do you want to spend and what is your expected result? Consultants and vendors are more than willing to sell you their solutions but do you really need that? Companies should pre-define their risk appetite bandwidth and make sure that all residual risks fit in there. An effective ERM program minimises the chance that a known risk has critical impact on the company. Map the known risks and keep in mind that there may be risks due to interconnection.

**RC: When rolling out ERM, how important is it for the board to articulate this strategy to the firm, and link it to business objectives?**

**Webster:** There are no risks without objectives. Seeking to identify risks, much less manage those risks, without identifying ‘risks to what’ is an exercise in futility. However, even if the board understands this linkage, the board is not in a position to manage risks to business objectives. It is thus critical for the board to communicate the role of ERM in managing risks to objectives, as only the management of the firm is in a position to translate goals into actions. Meaningful implementation of ERM is typically as
much a cultural change as it is a change in process. For this reason, tone-at-the-top is critical for sending the necessary messaging to the firm of the importance of ERM. This must be a joint board-CEO initiative, and ripple down through the executive team to all levels of the organisation. Along the way, it is essential that performance incentives are aligned with achieving business objectives and generating firm value.

**Hurrell:** This process is absolutely critical – establishing a risk culture is essential and needs to be led by the board and probably the CEO. The risk function can help to maintain a focus on critical risk issues throughout the organisation and act as an essential conduit between the board and operations. But the board has to drive this strategy.

**Wilgenhof:** Without making the ERM strategy part of the business, it’s like having a fast car without windows and proper brakes. Larger risks should make for larger returns but without knowing the risks those returns may never come. Realise that every risk may also be an opportunity to improve processes, control cost and increase revenue. ERM should be part of the business which means that the ERM strategy should not just be there to show what the risks are but also how they can be avoided or controlled.

**RC:** Do you expect more businesses to embrace ERM as a risk management strategy going forward?

**Wilgenhof:** Regulators are increasingly expecting companies to control risk. There may be a legal obligation to the shareholders but liability doesn’t end there. Even small companies can have a big impact when things go wrong. Globalisation has
multiplied the risk factors that companies are exposed to and without a proper ERM program, you’re not just flying blind but may be accused of wilful blindness. All too often a company ventures out in a new market expecting that nothing will change. However, legislation with international reach like the FCPA and the UK Bribery Act, as well as public opinion on international labour and environmental impact, all form part of the risk landscape. A known risk is a controllable risk; an unknown risk can kill you.

**Hurrell:** I expect to see more companies embracing a risk management strategy, but possibly not using the term ‘ERM’. Perhaps a more effective use of the acronym would be ‘Entrepreneurial Risk Management’. The future of ERM is to drive beyond compliance, towards placing risk at the heart of strategy.

**Webster:** The adoption of ERM principles has been growing steadily for the past 15 years, and I see no reason for this trend to stop, or even slow. For example, there was no position in the entire US federal government titled ‘chief risk officer’ just a few years ago. Today, that title is becoming increasingly common. Several federal agencies have embarked on formal ERM implementation programs. While too many organisations are unfortunately simply jumping on the ERM bandwagon by employing traditional risk management techniques and calling it ERM, meaningful ERM is being adopted more and more by organisations in all sectors. **RC**
Enterprise Risk Management (ERM) is the ultimate solution. Once we get this right, we can sleep at night because we are completely prepared. Whether it is evaluating an acquisition, fund investment, new business, or the existing business, we have all the pieces necessary to navigate for continual success. After all, is not ERM the means to identify the sustainability and dependability of revenue and components that impact cash flow? OK, maybe not, because risk is for prevention, or then maybe to satisfy stakeholders, or the mantle needed to demonstrate compliance with prescribed rules and mandated policies. Of course, we can utilise COSO, ISO 31000, guidelines from the NYSE and SEC, etc.

As a trained risk practitioner and reader of thousands of ERM articles and numerous methodologies, an ultimate solution gets my mind spinning as there are so many footprints none can be seen. This brings us to the Cube – The Rubik’s
Cub. Referencing Wikipedia permutation approach, suffice it to communicate there are 43 quintillion possibilities for the Rubik’s Cube. This is fine for engineering or challenging your intellect, but we are in business. We want useful and effective ERM – so how to untangle?

The key to the puzzle is to utilise a methodology that is founded in common sense. We have all worked with professionals who ‘get it’. They have a grasp of what is important and how to apply information. Thus, the business mind is the lead. Regulatory, legal, reporting and other mandated requirements need to be included. We refer to these as the ‘prescribed requirements’. It is also important to recognise that many of these prescribed requirements contribute to sound business decisions and ERM.

So, below is the formula to solve the Rubik’s Cube of ERM.

**Step One.** Determine the components of the business that sustain it and contribute to its growth. Do the same for intangible aspects of the business that make it attractive, such as geographic expansion, branding, reduce competition, etc. These are the core for business ‘value’. Surface the key risk that can impair the value. This is a high level exercise to be led by executives and subject matter experts as it will guide the ERM methodology. This is referred to as the ‘core business standards’.

**Step Two.** Prescribed requirements should be collected and organised by topic. Each topic is incrementally broken down to the lowest level, which is typically the way prescribed
requirements are systematised by the governing body or professional association. Every incremental level should have a tag which identifies its origins, for example, SEC, insurance regulation, GAAP, etc. Of course, consistency of topic and labelling tag is critical. Creating a reference dictionary is advisable.

With this as a complete digest, the core business standards from Step One, which should carry the identifying tag of ‘business’, are integrated. Consolidate all and you will be amazed how the number of Rubik’s Cube permutations is reduced as there is significant redundancy. Upon conclusion of Step One and Two, there are roadmaps for high level as well as granular elements.

Step Three. Create and build out the architecture for an ERM. ERM should be built upon the core business standards as the rest is to support the business or meet requirements established by others. Choosing the architecture for the build is also daunting as there are many methodologies reflecting the differences in business types and complexity. We have found that by adapting the FDIC model risk governance framework, all the key elements and considerations are identified. Its value is the methodology which is easy to follow and it provides the key considerations and questions. It is a systematic and pragmatic approach. There is an FDIC article in ‘Supervisory Insights 2005’ that provides a useful guide. Of course, it is easy to conclude this is outdated, which is why it is so useful. It is thoughtful and precedes the intricacies that new methodologies expound. The architecture is only as good as its usefulness and by focusing on what senior and executive management need is the most effective ERM architecture.

This architecture can be expanded and contracted allowing for the filtering of information to the appropriate level. For example, there is high level consolidated information for the C-Suite and board and detailed reports for various business functions; for example, producing compliance reports, analysing the profitability of a product, etc. Also, with a bit of tweaking, this can serve as the basis for due diligence.

“This architecture is only as good as its usefulness and by focusing on what senior and executive management need is the most effective ERM architecture.”

ENTERPRISE RISK MANAGEMENT – THE ULTIMATE RUBIK’S CUBE
receipt and delivery of information focused on the purpose. This provides producers and recipients with knowledge, confidence and accountability. While each report will vary in depth, content and purpose, there are a number of elements that should be embedded in reports. Some basics are: purpose, list of recipients, list of contributors, name and signature of quality review officer, frequency of report, key influences, (such as data timeliness; theory biases) key observations approved by quality review officer, highlight any changes made to material underlying substance of the report. To have report consistency with information and presentation is essential.

Reports speak to history and it is important to identify emerging trends and risk predictors. Separate and distinct from all methodologies, a business should put together its ERM predictors. Some examples may be tacking sales against norms or a trained professional noticing something that may appear unusual. These early warning systems are both on a high level macro basis and granular level.

ERM is essentially connecting silos, so information flows meaningfully and selectively, providing decision makers at all levels with the tools needed to run the business. The RMA of New York has a tag ‘Managing Risk for Enterprise Success’, which should be the purpose of the risk function.

The Rubik’s Cube is an assembly of alternatives. ERM is an assembly of alternatives. Random actions will not successfully solve 43 quintillion possibilities. The solution to solving the ERM puzzle is to determine and stick to a methodology founded in core business standards. RC

Bonita Z. Dorland
Advisory Board and Member
Women Corporate Directors
T: +1 212 628 6067
E: bonny.dorland@gmail.com
It seems with each passing year we see record-setting regulatory fines. Of course, some are more memorable than others. Most of us still recall the widespread media attention, beginning in late 2008, that was focused on Siemens when it was charged with violating the Foreign Corrupt Practices Act (FCPA) and agreed to pay a record $1bn in fines and disgorgement to resolve the charges with the US Department of Justice, US Securities and Exchange Commission, European Commission and Office of the Prosecutor General in Munich. At that time, the $450m criminal fine levied by the US was many times greater than the previous record fine in FCPA enforcement, which was $44.1m paid by Baker Hughes, Inc. in April 2007. In addition to the $1.6bn in fines and disgorgement paid by Siemens, it also incurred over $850m in costs related to an independent investigation conducted by 100 attorneys and 130 forensic accountants. The investigative work took place in 34 countries.
included more than 1750 interviews and 800 informational meetings and involved the collection and preservation of over 100 million documents. As a result, Siemens’ direct, ‘out of pocket’ costs related to its FCPA violations totalled nearly $2.5bn. No doubt, it’s always difficult to unscramble an egg once it has been broken.

More recently, we learned that various regulators have entered into a number of significant settlements related to the alleged manipulation of the London Interbank Offered Rate (LIBOR). Last December, UBS Securities Japan Co. Ltd, a wholly-owned subsidiary of UBS AG (UBS), agreed to plead guilty to felony wire fraud and admit its role in manipulating LIBOR. As a result, UBS agreed to pay $1.5bn in penalties and disgorgement, which currently stands as the highest settlement related to a LIBOR manipulation case to date. According to a US Department of Justice press release, the $1.5bn settlement consisted of $500m in penalties to the US Department of Justice, $700m in penalties and disgorgement to the US Commodity Futures Trading Commission, $259.2m in penalties and disgorgement to the UK Financial Services Authority and $64.3m in penalties and disgorgement to the Swiss Financial Markets Authority.

After UBS, additional LIBOR-related settlements soon followed. In February, RBS Securities Japan Limited, a wholly-owned subsidiary of The Royal Bank of Scotland PLC (RBS), agreed to plead guilty to felony wire fraud and admit its role in manipulating the Japanese Yen LIBOR. RBS agreed to pay $612m in regulatory fines and disgorgement, consisting of $150m in criminal fines to the US Department of Justice, $325m in civil penalties to the US Commodity Futures Trading Commission and £87.5m, or $137m in penalties to the Financial Services Authority. Then in June, Barclays Bank PLC (Barclays) agreed to pay $450m to resolve violations arising from its submissions for LIBOR and the Euro Interbank Offered Rate (EURIBOR), consisting of $160m in penalties to the US Department of Justice, $200m in penalties to the US Commodity Futures Trading Commission and £59.5m in penalties to the Financial Services Authority. To recap, LIBOR-related settlements with UBS, RBS and Barclays have topped $2.5bn. As of the writing of this article, ICAP PLC is reportedly also in the midst of negotiating a LIBOR-related settlement with regulatory authorities in the US and UK.

During the past year, we also learned of a record $1.9bn in fines and disgorgement for anti-money laundering violations. Last December, HSBC Holdings PLC and HSBC Bank USA N.A. (together, referred to as HSBC) agreed to forfeit $1.256bn and enter into a deferred prosecution agreement with the US Justice Department for HSBC’s violations of the Bank Secrecy Act, the International Emergency Economic Powers Act and the Trading with the Enemy Act. In addition to forfeiting $1.256bn as part of its deferred prosecution agreement with the US Department of Justice, HSBC has also agreed to pay $500m in
civil penalties to the Office of the Comptroller of the Currency and $165m to the Federal Reserve for its AML program violations. At the time of the US Department of Justice press release announcing the settlement, the UK’s Financial Services Authority was also pursuing a separate action.

The LIBOR scandal was accompanied in the news by another financial and environment disaster. In January of this year, we learned that BP will pay a record $4bn to settle criminal charges brought by the US Department of Justice arising from the Deepwater Horizon drilling rig disaster. The April 2010 explosion on Deepwater Horizon killed 11 workers and produced the worst offshore drilling oil spill in US history. At the time of the announcement of the $4bn settlement, criminal fines and accident and spill-related expenditures were expected to total a staggering $42bn. All of which, of course, pales in comparison to the loss of human life as a result of the disaster.

Further, there are the lingering ill-effects of the financial crisis, which if anything, has certainly kept lawyers busy. A recent Bloomberg article indicated that the six biggest US banks, led by JPMorgan Chase & Co. and Bank of America Corp., have incurred $103bn in legal costs since the financial crisis. JPMorgan and Bank of America represented about 75 percent of the total costs, with JPMorgan incurring $21.3bn in legal fees and litigation since the start of 2008.

Despite the record-setting amount of fines and disgorgement paid in recent years, these amounts still only represent a fraction of earnings and resources that were available to a number of these large, well-capitalised firms. Of course, the reputational damage to these firms as a result of their illegal activities is significant and their actions will not easily be forgiven (or even forgotten) by stakeholders, local communities and the general public.

“The reputational damage to these firms as a result of their illegal activities is significant and their actions will not easily be forgiven (or even forgotten) by stakeholders, local communities and the general public.”

public. With perfect hindsight, each one of the firms noted above would likely have invested greater resources in its compliance and internal control functions in order to avoid, or at least significantly mitigate, problems before they bloomed into full-blown regulatory and public relations disasters. Unfortunately, for many companies it seems that it takes a scandal of epic proportions before a conclusion is reached that the costs associated with
the implementation of a robust compliance function with effective internal controls are not only justified, but also a wise allocation of resources given the risks.

For companies that are without deep pockets, the stakes are much higher. Some firms will inevitably find themselves on the brink of bankruptcy due to the substantial amount of damages claimed by regulatory entities that aggressively seek fines, restitution and remediation. More and more frequently, company management and counsel are forced to assess the company’s ability to pay claims that may reach hundreds of millions or billions of dollars and are put in the unenviable position of determining the amount of payments that could be made without jeopardising the viability of the organisation going forward. Those familiar with the process utilised by most regulators to make an assessment of an entity’s ability to pay a large fine or restitution, understand that it consists of a gruelling and prolonged series of financial disclosures, interviews and meetings that require full transparency into all financial aspects of the organisation (past, present and future). There are no quick, painless solutions when settlement discussions with regulators are fixated on ability to pay.

We tend to see the headlines announcing record setting fines so often that we may lose sight of some of the harsher realities. Only the largest companies with the deepest pockets can pay such fines, and for every large settlement that a regulator proudly announces a press release, there are many more companies behind the headlines that are struggling to figure out how they will pay damages claims asserted by the government that exceed their stated book value, market value, earnings and cash flow by several times over and still remain a viable entity. As we all know, all stakeholders (investors, business partners and customers) and local community members lose when a company is forced to close its doors. In the long run, the benefits gained and disasters avoided (or at the very least, mitigated) by a well-planned, robust compliance program with effective internal controls will always outweigh the upfront costs needed to implement such processes and controls. RC

Jim Conversano
Principal
Berkeley Research Group
T: +1 202 480 2716
E: jconversano@brg-expert.com
The days when risk meant credit risk and the chief risk officer was the bank president are long gone. Risk has evolved and grown along with the complexity of institutions. Large global banks as well as small institutions need to understand how risks are interrelated and how a failure in one part of the bank can impact the enterprise. It is the role of the chief risk officer to oversee a risk organisation that takes an integrated approach and an enterprise-wide perspective. Yes, regulators require this approach, but institutions require it, too, because it drives shareholder value.

In building an enterprise risk management framework, the CRO, along with the board and senior management, must develop a risk culture that is communicated and understood throughout the organisation. The CRO leads the effort to develop a risk appetite for the organisation (how much risk are we willing to take?) and make sure that the organisation stays within the bounds of the risk appetite, in good times and bad.

The Risk Management Association, in its Governance and Policies Workbook, defines the role of the CRO as that of a senior executive who reports to the risk committee of the board or to the bank CEO or both.
Responsibilities of the CRO

The CRO serves as a key member of the financial institution’s executive management team and is responsible for the design, communication, implementation and oversight of its enterprise-wide risk management policy, program and framework. Specifically, those responsibilities include: serving as chairperson for management’s risk committee; ensuring that an enterprise-wide risk management (ERM) framework is in place that follows industry best practices in the identification, assessment and mitigation of risk; assisting the board and senior management in communicating that framework within the organisation, including the goals and objectives of the ERM program; and assisting the board and senior management in integrating risk management practices into strategic planning, bank operations and in change management.

Further, the CRO is responsible for assisting the board and senior management in developing a process and structure for defining and communicating risk appetite in the pursuit of fulfilling the strategic objectives; assisting the board and senior management in the development of appropriate risk management policies; ensuring that management has developed suitable risk classifications; assisting management as needed in the development and updating of enterprise risk assessments; and assisting senior management in ensuring that suitable risk mitigation controls are in place for all key risks and that risk monitoring systems are developed and maintained.

In addition, CROs are responsible for developing a reporting framework that allows for the aggregation of enterprise-wide risk profiles and assessment information, and presentation to the board and risk management committee for review and action as needed; ensuring that management systems are in place to oversee compliance with all policies and applicable laws and regulations, as well as a process for responding to policy exceptions and violations; ensuring integration between the ERM framework and the internal audit program; conducting management training as needed on
risk management practices and procedures; and serving as subject matter expert to the board and senior management in the risk aspects of strategic planning, risk alignment, capital management, resource planning, new projects and services, risk reporting and regulatory compliance.

Optional additional responsibilities include acting as a representative to the board risk committee (if one exists); supervising other oversight roles, such as the chief compliance officer, chief information security officer, and so on; and overseeing assurance of Sarbanes-Oxley compliance and validation.

Job requirements
As a key member of the executive management team, the CRO is expected to be a seasoned industry professional with significant industry experience and strong management abilities. Specific requirements include at least 15 years management experience in the financial services industry with emphasis in strategy, finance, operations, risk management and regulatory compliance; and specific industry experience in the case of a mono-line company, e.g., mortgage, insurance and so on.

At least five years experience leading a risk management function is necessary, along with a familiarity with bank laws and regulations, and a Bachelor’s degree – although a MS or MBA is preferred. CROs should have a sound understanding of enterprise risk management, including risk assessments, reporting, alignment and the major risk frameworks, and understanding of all risk types, including: credit, market, operational, compliance, liquidity, interest rate and reputational risk.

To function effectively as a chief risk officer, individuals must be able to analyse and interpret large amounts of data. The CRO needs experience interfacing with bank regulators in a liaison role. Exceptional communication skills, both written and verbal, are key as the CRO plays a highly influential role within all levels of the organisation.

With the complexity of risks facing the industry today, institutions of all sizes must remain vigilant about the risk in individual portfolios and how those risks correlate across the enterprise. We recognise that the industry has made significant strides in implementing enterprise risk management, but we all know too well that our work will never be finished. **RC**

---

**Bill Githens**  
President and CEO  
The Risk Management Association  
T: +1 215 446 4124  
E: bgithens@rmahq.org
Some of the most important risks that need to be managed are the psychological pitfalls that characterise our thinking. Daniel Kahneman, psychologist and Nobel laureate in economics, tells us in his recent best seller that all people engage in two types of thinking: thinking fast, when they spontaneously and automatically search for intuitive solutions, and thinking slow, when they engage in more deliberate, effortful, conscious analysis. Although there are situations where one type of thinking is better than the other, Kahneman urges us to remember that neither type of thinking guarantees perfect decisions, especially when risk is involved.

Corporate managers make decisions just like everyone else, by sometimes thinking fast and sometimes thinking slow. And this goes for business decisions, not just personal decision, which prompts the question: What do managers need to know about their reliance on both types of thinking? The
short answer is that managers need to know how to balance the two, and to recognise the relative strengths and weaknesses of each. It is easy to get the balance wrong. Specifically, it is easy to err by placing excessive reliance on intuition instead of careful analysis when it comes to tasks such as planning, budgeting, and making acquisitions. A particularly important behaviour pattern that results from such an imbalance is known as ‘the planning fallacy’.

There is risk involved in project completion times. Managers who commit the planning fallacy are consistently and negatively surprised by how long projects take to complete, how much over budget the projects tend to be, the degree to which finished projects feature fewer features than initially anticipated, and the amount by which acquisitions turn out to be less valuable than originally estimated. The planning fallacy is more than bad luck. It’s about the failure to learn from experience, so that negative surprises keep arriving more frequently than managers anticipated. The planning fallacy is common, and in some cases has proven to be extremely expensive, if not deadly.
Kahneman describes how he and his late colleague Amos Tversky experienced the planning fallacy first hand when, as young academics, they were working on the development of a new high school curriculum for teaching decision making skills. Amazingly, the group was far too optimistic and overconfident at the outset about how long it would take them to complete their task, despite the fact that one member of the group was a curriculum expert. Had the expert used some slow thinking to draw on his own knowledge about past success rates, he could have guided the group to set realistic expectations. However, the expert instead relied on his intuition, with the consequence that his excessive optimism led his group to set unrealistic expectations for the completion of their task.

Psychologists identify three major psychological pitfalls to which people are vulnerable: biases, heuristics and framing effects. Excessive optimism and overconfidence are examples of biases which are especially relevant when it comes to the planning fallacy. One of the most vivid and recent instances of the planning fallacy involves Boeing’s new aircraft, the 787 Dreamliner. In line with excessive optimism and overconfidence, the 787 came to market in 2011, four years late, well over budget, and with battery problems so severe that in early 2013 the US and Japan grounded the planes for several months after a series of fires and emergency landings.

Software projects are well known to be routinely over budget, completed late and failing to have all the features that were anticipated at the outset. Large software projects are especially prone to these problems. A case in point, and one currently in the news, involves the web portal for the new online insurance marketplace in the US. Since the project roll out at the beginning of October, a system with a price tag of more than $400m, which was promoted as a one-stop shop for citizens in search of health insurance, has stymied the efforts of millions of Americans just to log on.

A heuristic is a simplifying rule of thumb. When people use mental shortcuts to make decisions, such as relying on information that is easily recalled, or basing a judgment on a stereotype, or trusting their gut instinct, they are using heuristics. Some managers explicitly acknowledge reliance on gut instinct instead of textbook techniques. Michael Lehman, the former CFO of Sun Microsystems, is a case in point. Intuition did not do Sun much good, as the company lost value for a decade and was finally acquired by Oracle in 2010.

Framing effects concern the way people describe the decision tasks they face. How people frame a decision can affect what they choose to do. People who remind themselves ‘not to cry over spilled milk’ are more likely to ignore sunk costs than people who describe their decisions in ways that make the sunk costs salient. Such framing is important because when people see themselves as facing the possibility
of accepting a sure loss, they become prone to taking unwise risks in an effort to avoid that loss. This is especially important because the planning fallacy leads companies to go over budget and find themselves in the domain of losses. Examples are BP’s fiasco in the Gulf of Mexico during the summer of 2010, and the US government’s much publicised and ill fated decision to provide loan guarantees to solar firm Solyndra. In both cases, executives took value destructive risky decisions when reality began to diverge from their rosy expectations.

How can managers reduce their organisations’ vulnerability to psychological pitfalls such as the planning fallacy? The answer is to bake techniques into their corporate processes and culture. Doing something to combat the planning fallacy requires a cultural shift from what psychologists call ‘the inside view’ to ‘the outside view’. The inside view is what detail oriented managers tend to do well: looking at the specifics of projects being evaluated at the time resources are being allocated. The outside view is engaging in peer comparison, by asking how long others, peers, tend to take to accomplish similar tasks. Taking the outside view involves placing oneself in the position of an outsider who is being asked to make the same forecasts as the insiders, but using peer comparison data, rather than project specific data. Making the change from taking the inside view to the outside view requires some serious slow thinking.

There’s a classic story from the 1980s about Intel president Andy Grove and CEO Moore’s Law legend Gordon Moore being conflicted about how to deal with the decline in their major business – memory chips. Their company faced a fork in the road, with one path leading them to continue competing in memory chips against lower cost producers and the other path leading to the substitution of microprocessors for memory chips. In the course of feeling conflicted, Grove asked Moore what path he thought the company would take if the board replaced the two of them. Because the answer to the question seemed obvious, as staying in the memory business was a very bad risk, Grove suggested that they symbolically fire themselves and behave accordingly. In other words, Andy Grove had the imagination to get himself and Gordon Moore to take the outside view; and it dramatically affected Intel’s decision to move into microprocessors, an industry that they came to dominate. Managers might do well to remember the lesson that symbolic firings can prevent actual firings. RC

Dr Hersh Shefrin
Professor of Finance
Santa Clara University
T: +1 408 554 6893
E: hshefrin@scu.edu
Corporate directors around the world have become increasingly aware of the need to provide a holistic view of a business enterprise, incorporating financial as well as environmental, social and governance frameworks, in order for key stakeholders to make economic decisions.

Globally, much work has been done to align international accounting standards, which form the basis of reporting annual financial statements; at present that task is incomplete. There has also been an increased focus on developing a framework for integrated reporting, with the International Integrated Reporting Council (IIRC) driving forward this body of work. The IIRC’s goal is to create a framework that brings together the varying reporting requirements in a “clear, concise, consistent and comparable format”, which will “support transition to a more sustainable global economy”, according to the IIRC’s mission statement.
The IIRC’s Consultation Draft on the international Integrated Reporting framework defines an integrated report as “a concise communication about how an organisation’s strategy, governance, performance and prospects, in the context of its external environment, lead to the creation of value over the short, medium and long term”.

There are numerous participants in this movement, which includes the Sustainability Accounting Standards Board (SASB), which is currently developing sustainability accounting standards for use by publicly listed entities in the United States for disclosing their material sustainability issues in their SEC Forms 10-K and 20-F. Other participants include the World Intellectual Capital Initiative (WICI), a global movement to encourage sustainability reporting, and the Global Reporting Initiative (GRI), which has produced the leading framework for sustainability metrics. GRI released its revised G4 guidelines in May 2013.

All of these participants have added value to the dialogue; however the global realities of applying this vision may limit its success.

The ultimate purpose of any form of corporate disclosure is to provide material information to the market and stakeholders. There is no point in devising an elaborate structure of disclosure if no one is listening. Consequently, we need to be certain that there is genuine investor demand for what is disclosed – that it adds value to their investment process and is not just ‘nice to know’.

The Global Network of Director Institutes (GNDI) is just one group arguing that there should be improvements in the way organisations report to their shareholders and other stakeholders, including in ways guided by the International Integrated Reporting Framework; however, any changes to the way organisations report should reduce the overall reporting burden on organisations.

The GNDI’s members are the Australian Institute of Company Directors (AICD), the Brazilian Institute of Corporate Governance (IBGC), the European Confederation of Directors Associations (ecoDa), the Institute of Corporate Directors (ICD) in Canada, the Institute of Directors in New Zealand (IoDNZ), the Institute of Directors in Southern Africa (IoDSA), the Institute of Directors (IoD) in the UK, the Malaysian

“We need to be certain that there is genuine investor demand for what is disclosed – that it adds value to their investment process and is not just ‘nice to know’.”
Alliance of Corporate Directors (MACD); and the National Association of Corporate Directors (NACD) in the United States.

The GNDI believe that corporate reporting should result in concise, simple and focused reports that identify the material business risks and opportunities that an entity faces, how that entity manages those risks and opportunities and how they determine their success in managing those risks and opportunities.

However, they have significant concerns that should integrated reporting be mandated, it is likely to result in overly prescriptive, compliance driven corporate reporting. By mandating integrated reporting we will continue the failings of the current corporate reporting frameworks, for example boilerplate disclosures and vanilla statements.

The GNDI has specific concerns with integrated reporting mandates (as outlined by the IIRC consultation draft) which include: (i) the potential to significantly increase the cost of compliance for entities, as well as increasing the volume of reporting; (ii) the need to ensure that there is genuine investor demand for the disclosures in an integrated report; and (iii) the potential increase in directors’ liability for the disclosures in an integrated report and the lack of an internationally harmonised safe harbour for forward looking statements.

Before any integrated reporting framework can be agreed to, the IIRC must identify the types of entities that would apply an integrated reporting framework and ensure global consistency.
They must also provide guidance on how the integrated reporting framework would fit within individual countries’ corporate governance framework, tax and corporate laws and determine the cost, benefits and implementation implications for entities and their shareholders.

The GNDI is supportive of entities and their boards effectively communicating those issues of significance to their shareholders in their corporate reporting.

These factors must be addressed and encompassed within a principles-based, non-regulatory, ‘if not, why not’ framework that recognises the diversity of business, encourages innovation and promotes entrepreneurial activity.

RC

John Colvin
Chair
Global Network of Director Institutes
T: +61 2 8248 6600
E: gndi@companydirectors.com.au
One only has to look at the recent regulatory enforcement environment to gauge just how significant regulators, especially the US Securities and Exchange Commission (SEC), view insider trading and misuse of material information. According to the SEC’s 12 August 2013 Spotlight, the SEC’s enforcement section brought 58 insider trading actions in 2012 against 131 individuals and entities. If one was to examine the SEC enforcement actions over the last three years, then one would find that the SEC has brought more insider trading enforcement actions (168 total) than at any other time in the SEC’s history. Why? These actions were filed against over 400 individuals and entities to the sum of $600m in illicit profits and losses avoided.

Many of those caught within the SEC’s crosshairs come from positions that one would naturally expect; financial professionals and senior corporate executives who are likely to have insider information at first hand. However, more and more of those
violating insider trading rules are people one might not ordinarily suspect. Recent violators include lawyers, accountants, doctors, corporate board members, public relations professionals, professional athletes, movie producers, former government regulators, consulting experts and line workers. No doubt, the advent of new technologies has made it easier for the average person to trade on the financial markets. Additionally, the ability to conduct illicit trading via this technology is easier and, when executing a scheme through a third-party such as a friend, parent and or sibling, it becomes much more difficult to detect.

However, there are reasonable and significant controls that management can implement and test to make sure that their compliance infrastructure is one that can detect and help prevent instances of insider trading and the leaking of material inside information.

For management to be effective in addressing this type of risk, first and foremost, they must create a documented process that identifies the who, what, how, when and why of the risk factors for the company. Establishing control procedures establishes a framework for all stakeholders. Good practices dictate that that the compliance framework includes: (i) process for defining and identifying key data; (ii) a system with checks and balances, (iii) training; (iv) effective self-auditing; and (v) a method to effectively measure the risk of each employee.

In contemplating the design of the compliance structure, it behoves management to adopt a macroscopic view of the organisation to determine current key intellectual or tangible capital.
Management will need to address key questions, such as “Are the guidelines based on quantifiable measures or definitions of materiality?” Furthermore, for the system to be deemed effective it should be designed and incorporated as a continual filter for the organisation to ensure that all future key data or capital is flagged for monitoring.

Once the significant intellectual or tangible capital has been identified, it should be treated just as one would cash or valuables. A well tested and recognised methodology that may prove to be effective is the implementation of The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. The framework allows for the interrelatedness of risk across the organisation with a focus on operations, reporting and compliance and different levels of the organisation such as entity, division and operating unit, as well as governance activities that impact the organisation such as control environment, risk assessment and information and communication.

The implementation of such a system will provide management with the necessary ‘checks and balances’ needed to be in place to allow for sound decision making. Essential to ensuring that the control framework continues to operate effectively, it is imperative to have competent and recurring training of employees across the enterprise.

Lastly, management will need to address the implementation of an internal control effectiveness monitoring and audit program. This audit program can either be manual or supplemented with automated quantitative processes that will serve to verify the integrity of the process, namely, that it exists, it is utilised and it identifies potential risks.

“Once the key tangible assets of the organisation have been identified, a risk measurement system for each employee must be put in place.”

Once the key tangible assets of the organisation have been identified, a risk measurement system for each employee must be put in place. It should consist of more than a typical static background check and include dynamic elements such as workplace situational elements and ongoing personal data. As seen in recent events, the highest insider risk may not be from those at the forefront. An effective way to view personnel risks is to gauge them in a framework that encapsulates the multi-dimensional aspect. For example, one could
rate a person high to low across three elements: access to information, ability to utilise and ability to detect. Then one would add those factors to gain a total risk score for the employee. For example, in such a framework, an administration assistant might garner as high a risk factor as an analyst. A multidimensional approach could be the following: (i) position/access score – both high; (ii) utilisation score – high / low (analyst/administration assistant); (iii) detectability score – low / high (administration assistant/analyst).

Quantifying risk from all perspectives will allow for better allocation of monitoring resources. This risk score can be further enhanced by incorporating regular background reviews to incorporate perpetually changing personnel stressors such as dependencies, familial stress or psychological issues. The addition of unique workplace factors can also add value such as bonus incentives, trading positions, exposure to earnings pressures or even geographic proximity. Taken together, management can now have risk factors that incorporate all aspects of the individual.

Combining the aforementioned processes, procedures and risk factors will serve to enhance personnel security controls. To be effective, evaluation must be ongoing, utilising either random or regular scheduling, or using evolving technology to create automatic reviews. Systems can be developed that dynamically measure the aforementioned employee risk factors and can trigger automatic reviews when a statistical threshold is breached. For example, a former low risk factor employee may trigger a review when the background check system reveals a recent issue with dependency and a corresponding drop in credit score.

As technology continues to advance, and the ability for employees and interested parties to have access to sensitive and critical information increases, the need for management to implement strong controls is greater than ever. The very same technology that one relies upon to conduct the malfeasance can be harnessed to prevent and detect such behaviour. RC

Brian Vahey
Principal
Berkeley Research Group
T: +1 646 862 0954
E: bvahey@brg-expert.com

David Martin
Principal
Berkeley Research Group
T: +1 646 205 9381
E: dmartin@brg-expert.com
Every business venture involves taking risk in the hope of returns. The question is, what kind of risk, and what kind of returns? Expectations vary. So do standards for balancing the two. This is why the fields of accounting, finance, management, politics and law all concern themselves with risk management.

This article concerns the specialised area of risk management known as ‘due diligence’ as it applies to the mergers and acquisitions of commercial banks. We will focus on the preliminary due diligence conducted in the early stages of acquisition; the later phase, confirmatory due diligence, can also be instructive but lies outside the scope of this brief article.

Our choice of subject may seem narrow but in fact it could well have broader application. Mergers in general (in all industries) form an important part of the economy, and bank mergers are a very common type of merger. Bank M&A due diligence may offer lessons that extend beyond the world of commercial banking to a broader realm of acquisitions in other industries.
Bank M&A: an active sector

In the first half of 2013, the financial sector including banks accounted for one in 10 deals and dollars that changed hands in M&A. Specifically, according to Thompson Reuters, they accounted for 10 percent of the 16,808 announced deals and 10.1 percent of $996.8bn in deal value. If present trends continue, this year may rival last year for active bank M&A. In 2012, financial mergers accounted for 13 percent of 37,923 announced deals and 8.6 percent of their $2.6 trillion value. In that year, more than $200bn in value in bank M&A globally – boosted by heavy deal volume, and by an average 34.2 percent premium paid for targets in these kinds of deals – left financials with a number 5 ranking for M&A activity out of the 12 main sectors, ranging from the most active M&A sector, energy, to the least active, retail.

Due diligence standards

Bank M&A typically generates controversy within and outside banks due to a variety of risks including potential for antitrust challenges by government, employee layoffs, employee and customer attrition and loss of shareholder value after the merger. The greater the number of banks that undergo mergers, the more likely the emergence of anecdotal evidence of one or more of these risks. Over time, however, bankers learn from experience, and the due diligence conducted before mergers continually improves.

Today, bank acquirers know to look for these and certain other certain high-risk elements.

Appropriate valuation and evaluation of a target bank for preliminary deal pricing is of course one of the major goals in bank M&A. Many traditional technical valuation standards – e.g., fair market value, fair value and investment value – and technical methods – e.g., income, market and asset approaches – apply to banks. However, the end goal is to consummate a desirable deal at the right price based on perceived risk. It is impossible to value a bank (ultimately a quantitative measurement) without simultaneously evaluating a bank’s processes in managing its on and off balance sheet activity (a more qualitative and somewhat less technical measurement). The question is not only what is the value of a target bank but how well does the management of the bank maintain it and protect it against future risk. These two considerations are co-dependent. Hence, to value a bank one must know how to assess its risks as well as its approach to managing them. This article will focus on the more qualitative and less technical aspects of preliminary bank valuation and due diligence.

Stress testing

In 2011 stress testing became required for all large banks overseen by the Fed, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) – the three main bank regulators in the United States.
Stress testing, fundamentally a ‘what if’ risk analysis, is a series of exercises used to assess the potential impact of various possible future adverse events and scenarios on a banking organisation. For example, the stress test used by the Board of Governors of the Federal Reserve System (Fed) in 2012 ran bank holding companies through a hypothetical scenario that assumed equity markets plunged by 50 percent, home prices declined 21 percent and unemployment rose to 13 percent from the current 8.3 percent—all events that could conceivably occur. Such stress testing makes sense as a process to be used by any potential acquirer making a bank acquisition. In more recent stress tests, the scenario includes an eventual rise in interest rates, including an extreme one. The same concept of ‘what if’ scenarios can be employed in the preliminary evaluation stage of practically any target and in almost all industries.

It is important to note that stress testing merely studies the quality of the bank’s assets and the pressures of its liabilities. It should be noted that stress testing does not pretend to pass judgment on a bank’s internal controls. Sometimes, despite a healthy balance of assets and liabilities, a bank can experience financial challenges as a consequence of weak internal controls. This is why the Federal Reserve devotes extensive coverage to internal controls in its Commercial Bank Examination Manual. Those contemplating mergers with or
acquiring banks would do well to study the results of past bank examinations in assessing potential acquisition targets. While bank examinations are hardly infallible, it makes little sense for an acquirer to go over ground that has already been covered by others. On the other hand, there is a role for sound financial analysis that may or may not be reflected in the examination. Some banks believe that the standards used by federal examiners are flawed and inconsistent. Finally it should be noted that the focus of examiners are also often a function of the broader economic situation at any given time.

**Operational risks**

Acquirers, bank examiners and others put much focus on bank’s financial risks but it is often operational ones that lead to insolvency. It is now known, for example, what kinds of risks most often lead to a bank’s demise within its first seven years. These soft risks (as identified by the FDIC) include: rapid growth; over reliance on volatile funding sources; concentrations without compensating controls; significant deviations from approved business plans; non-compliance with FDIC guidelines (e.g., the requirements for deposit insurance); weak risk management practices; unseasoned loan portfolios; significant consumer protection problems; or problematic third party relationships.

Most of these bank-killers could be called operational rather than financial risk. Of course they are ultimately financial in consequence. The Basel Committee, under the Bank of International Settlements, is the primary global standard-setter for the prudential regulation of banks. It defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It may also include other classes of risk, such as fraud, legal risks, physical or environmental risks. Operational risks may be understood as those risks incurred involuntarily or consequently to operating a business, as opposed to risks voluntarily incurred in order to generate income, such as interest rate, credit and similar risks intrinsic to balance sheet activities.

Banks generally use an approach called the ‘advanced measurement approach’. In this
approach, analysts try to measure operational risk (including the risks inherent in off-balance-sheet, fee-based activities or fiduciary risk). To do so, they aggregate statistical data and use sophisticated modelling based on the number of negative incidents occurring in the past and the magnitude of losses associated with those occurrences. Probability theory is then applied and estimates of future risk are derived.

Another challenge is strategic and reputational risks, which are not considered under operational risks by the Basel standards. Yet they can have an enormous impact.

Strategic risks relate to decisions. Consider poor expansion decisions, changes in business activity focus, encroachment of competition and similar risks. In assessing strategic risks, an acquirer needs to ask this: how does this bank stand in relation to its competition? What are its competitive strengths and weaknesses?

Reputational risks can be ongoing (when a bank has a bad reputation for customer service, for example) or they can be single-incident driven and difficult to predict and contain. The question here is how the public views the target.

Management and management policies are where it all begins. Modelling and stress testing should be viewed as situation analysis – important but insufficient. By contrast, close management and management policies are the ongoing lifeblood of risk management. These need to be reviewed carefully in due diligence, at times in the preliminary stage to derive an overall impression and at other times in the final stage to confirm and verify. Again the point of this article is that these soft risks are as important as the more obvious and conventional ones in the preliminary evaluation of a possible acquisition target or merger partner, whether in or outside of banking.

Balance sheet risks

Preliminary due diligence on a bank involves not only projecting its future earnings but also understanding the quality of its assets and the nature of its liabilities. In the sense mentioned above, ‘a bank’s balance sheet is the business’ – more so than in most other types of business. In a normal business the balance sheet reflects a snapshot at a particular point in time of the assets and liabilities accumulated on any given date as a result of the external operations of the business. In the case of a bank the balance sheet reflects more than just the cumulative results of operations as measured by assets and liabilities at a snapshot in time; it reflects all of the bank’s core financial operating factors. As such, it is a good starting point for evaluating any target bank and its future prospects. And in general this will be truer for banks than for other non-bank businesses.

Operationally, it is a fact that most banks are quite similar. They make loans, take deposits, keep some cash on hand, pursue customers and (usually)
open branches. Indeed – despite banks’ efforts to distinguish themselves by their cultures, it has long been a problem for bankers to distinguish themselves in such a commodity business.

Financially, however, banks do vary. Every bank balance sheet is different. If you want to know a bank, know its balance sheet. This is not to say that there are no other important factors like the number of branches, the types of business lines, the quality of management, geographical location, etc. Nor is it to neglect the importance of future earnings—another important aspect of bank valuation. But the balance sheet is the natural starting point for determining the degree of actual collectability of the assets as well as the future timing of interest income, collections of assets and repayment of liabilities. It is also an excellent starting point for future income projections.

Indeed, a bank balance sheet can also be seen as a cash flow statement showing the source and use of funds – the source of bank funds constituting most of its liabilities, especially deposits; and the use of bank funds constituting most of its assets, especially loans. So the balance sheet plays a special role in banking – and an important part of the balance sheet is knowing the risks it can reveal.

Most of the asset side of the bank’s balance sheet is made up of securities and loans or leases ‘in bank credit’.

Securities in bank credit are securities held in trading accounts owned by the bank (other than derivative securities). These include securities issued by the US Treasury and federal agencies, including mortgage-backed-securities. They are considered held to maturity and available for sale; in other words they aren’t restricted. The accounting for securities in bank credit is complex due to ‘mark to market’ standards that require current valuation rather than historic cost, and that offer various options for this accounting.

Loans and leases in bank credit include commercial and industrial loans, real estate loans and consumer loans, and typically constitute from 60 to 70 percent of a bank’s assets.

“The balance sheet is the natural starting point for determining the degree of actual collectability of the assets as well as the future timing of interest income, collections of assets and repayment of liabilities.”
Most of the liabilities on the books of commercial banks today are in the form of deposits. Some of these are non-transaction and large time deposits – money market or savings accounts with restrictions on withdrawal. Most, however, are deposits that have no such restrictions, the so-called checkable or transaction deposits. Banks take custody of the money that is in bank accounts but owners of those accounts can claim it at any time; as such, the deposits are accounted as a liability to a bank. In addition, if the accounts are interest bearing, the bank owes interest on the amounts.

The remainder of a typical bank’s liabilities come from borrowing and from trading (including derivative instruments with a negative fair value).

Banks (and their balance sheets) have various risks: interest rate risks, credit risks, liquidity risks and trading risks are usually the primary ones encompassed by the balance sheet. Since banks mostly borrow short and lend long, they are exposed to increases in short term interest rates (interest rate risks), and this would lead to lower net interest margins (NIMs). The credit risk is that too many of those assets will go bad. The liquidity risks also come from the necessary reliance of banks on their mixes of assets and liability types and terms. Trading risk comes of course from the daily vicissitudes of trading and owning securities and their derivatives. Although commercial banks are not exposed to the kind of trading risk that can cause the rise and fall of major investment banks, the fact remains that commercial banks too can be exposed to market vicissitudes, and bank acquirers need to know how well their new partners are handling them.

Concluding comments

Preliminary bank valuation and due diligence contains a lesson for all businesspeople: evaluation, valuation and due diligence are inseparable. To develop even the most general idea of the value of any bank it is necessary to take close look at risks, both quantitative and qualitative. RC

Alexandra R. Lajoux
Chief Knowledge Officer
NACD
T: +1 202 280 2185
E: arlajoux@nacdonline.org

Dennis Roberts
Chairman
The McLean Group, LLC
T: +1 703 827 0200 ext. 101
E: droberts@mcleanllc.com
Many UK businesses are ill-prepared for handling a terrorist incident even though the government has maintained a high state of alert. The chances may be small, but the impact could be devastating, and there are simple steps that a company can take to become more resilient.

“This war, like other wars, must end,” Barack Obama declared in May during a set-piece address on terrorism. “That is what history advises. That’s what our democracy demands.”

He was speaking shortly after the shocking attack on the Boston Marathon in April and the failed conspiracy in Canada at about the same time, both of which reminded the world that terrorism continues to be a serious threat – and that you cannot predict when and where it will take place. In the long run, the president may be right and the problem will one day be overcome, but terrorism is
not a threat that can be talked away, as he himself was soon to discover.

At the time of writing, the US, UK and other western countries have recently closed many of their embassies and advised their citizens to stay away from certain countries following reports of planned Al-Qaeda activity. The World Economic Forum’s eighth report on Global Risks (2013), where it examines threats on a twin axis of impact and likelihood, continues to put terrorism towards the higher end of the risk spectrum. At an international level, terrorist activity has been rising steadily over the past decade.

Closer to home, Great Britain remains on a high level of terrorism alert. The fact that the last attack in this country to have any significant economic impact was in 2005 has lulled some people into a false sense of security. Although there has been no hurricane in the UK since 1987, it is safe to assume that there will eventually be another; by the same token, it would be foolhardy indeed to rest on our laurels as far as security is concerned. As the government adviser David Anderson QC put it recently, the UK is not yet “out of the woods” with regards to large-scale threats.

In the UK, the brutal murder of Lee Rigby in Woolwich in May is a reminder that we cannot relax. The lack of any other serious incident since 2005 reflects the success and expertise of anti-terrorism measures rather than any reduction in the desire of some terrorists to inflict damage.

Forty-three people were charged with terrorism-related offences last year in Great Britain, excluding Northern Ireland. Among recent cases, a gang accused of planning large-scale destruction was recently found guilty at Woolwich Crown Court. A completely separate group admitted planning to bomb a rally held by the English Defence League. Yet the security services would be the first to admit that they cannot guarantee to thwart all such activities. Indeed, the revelations by the former CIA agent Edward Snowden published in the Guardian can only make things more difficult for them.

According to the Home Office, the threat in mainland UK from international terrorism remains substantial. To quote Jonathan Evans, the recently retired Director General of MI5, in a rare public speech: “In back rooms and in cars and on the streets of this country there is no shortage of individuals talking about wanting to mount terrorist attacks here.”
What are the implications of terrorism to your business?

So what does this mean for company security? It should be remembered that the potential operational and financial consequences of a terrorist atrocity are devastating for a business. Contrary to a commonly-held belief, they are not routinely covered by most property insurance policies. Clearly, the response to any threat should be proportionate. Companies cannot afford to devote too much of their time and resources to fearing the worst. Nonetheless, there are simple steps that can be taken to address terrorism, and many of them will dovetail naturally with other types of risk management.

All stakeholders (primarily government, insurers and business) must take it seriously and treat it as they would any risk of similar potential. For businesses, this means dealing with terrorism within their internal risk governance framework, which would typically include: identification – considering the type of terrorism the business might face, including the knock-on impact from an attack in the surrounding area, or on the supply chain; prevention – considering if and how an attack may be prevented or discouraged through security measures, intelligence or liaison with counter-terrorism agencies; quantification – assessing the financial impact of potential types of attack; mitigation – planning how to reduce the impact of an attack, for example, through business continuity planning; and risk transfer – via insurance. Your property policy probably excludes terrorism cover, unless it has been specifically requested and an extra charge made, so you may need to check that this is in place.

It is important to remember that your business does not have to be hit by terrorists to be affected by them. You may be forced to shut down as part of an exclusion zone, for example, or your staff may be unable to get to work, or an attack might disrupt your supply chain. As with other types of emergency, scenario planning in cooperation with key suppliers and customers can be very helpful.

“Clearly, the response to any threat should be proportionate. Companies cannot afford to devote too much of their time and resources to fearing the worst.”

Reducing the risk and potential impact of a terrorist incident

While firms may not be able to prevent the occurrence of terrorist incidents, certain steps
can be taken to reduce the risk and minimise their impact. First, companies must maintain control of access to all their properties, making sure they channel any visitors or contractors who require access to their premises. Visitors must sign in and wear badges and contractors such as cleaners must undertake sufficient pre-employment checks. Firms must ensure they lock away any materials that might be useful to a potential terrorist such as volatile liquids, fertilisers and flammables. They must also understand their environment – does the Business Continuity Plan deal with prevention of access issues?

More broadly, organisations should ensure their Business Continuity Plans are firmly embedded within their operations. The plan should address terrorist incidents and threats both to their premises and in the vicinity. It is also prudent to run scenario tests to assess the company’s preparedness to respond to an attack and identify areas for improvement. As part of planning, firms should liaise with police, fire and ambulance services.

Regarding insurance, firms must ask their insurers or brokers to outline what cover they have for terrorism under all property, liability, personal accident and motor policies, and consider whether this is sufficient. They should ensure their broker provides costed options for buying terrorism insurance plus details of what will and will not be covered.

**Insuring against terrorism**

While companies may be limited in what they can do to prevent a terrorist attack with its potential human consequences, they can at least cover the financial losses incurred, should there be an attack on one of their properties. The UK was one of the first countries to realise that terrorism insurance cannot be left to the market alone, that it requires collaboration between the insurance industry and government.

In 1992, during the IRA bombing campaign, insurers indicated that they could no longer provide terrorism cover for commercial property losses without government financial support. The solution was to establish Pool Re, a mutual reinsurer that enables its members, which are all insurers active in the commercial property market, to provide terrorism cover in mainland UK. Profits are used to build up reserves for any future claims, and the government undertake to step in should these funds prove inadequate.

This protection is not sold on a standalone basis, but as an extension to existing property policies for any organisation that so chooses. Crucially, it has open-ended financial support from the Treasury (subject to the limits in your property policy) and, for an extra cost, can provide business interruption cover.

The value of this arrangement was brought home by the 9/11 attack in New York, which demonstrated to a global audience the catastrophic losses a
terrorist attack can cause. Following that event, Pool Re extended its cover to protect against CBRN (chemical, biological, radiological and nuclear) and other attacks.

The fact that such arrangements exist does not mean that everyone should buy terrorism insurance. The process of considering the risk and what to do about it should be no different to any other peril. The danger is that the decision may be taken by default; it is possible the gap in cover will only be noticed when it is too late. RC

Steve Coates
Head of Market Operations
Pool Re
T: +44 (0)207 337 7170
E: smc@poolre.co.uk
The title of this article seems like an oxymoron, especially to companies that have been the subject of prominent media reports highlighting the extraordinarily costly FCPA investigations in which they have been involved for months and even years. Investigations costing hundreds of millions of dollars in legal and accounting fees have burdened companies, before even reaching the point of settling the amounts of fines and penalties they will be paying to the US Department of Justice (DOJ) or the Securities and Exchange Commission (SEC). It has been widely reported that one major US company was incurring investigative expenses at a rate of over $600,000 per day on its FCPA case.

In response to the global reach of the FCPA and increasing enforcement of other anti-corruption laws by ever more aggressive prosecutors, how can companies, which must undertake investigations to protect themselves, contain their costs? In regularly
handling these FCPA cases before the US authorities, we have developed several key strategies to contain costs, while meeting the demands imposed on companies to conduct thorough and effective investigations into potential misconduct. Substantial costs can be saved from the beginning to end of the process if companies and their counsel focus on: (i) effective planning, particularly in the allocation of personnel and resources; (ii) disciplined scoping of the investigation; (iii) maximising efficiencies in conducting the investigation; and (iv) implementing critical compliance enhancements that can contribute to a more favourable resolution of the case.

**Effective planning**

Because of the real possibility that an FCPA issue arising at a global company will come to the attention of the DOJ, the SEC, or another anti-corruption regulatory body as enforcement increases throughout the world, the first step in planning an FCPA investigation is to plan as though the company will be required to defend not only substantive FCPA charges but also the procedures it has followed in investigating the potential misconduct.

The starting point to contain investigative costs is an effective investigation plan that takes into account the priorities of law enforcement agencies as well as the company’s interest in determining what happened. The only situation worse than having to endure a costly, time-consuming FCPA
investigation is having to repeat that painful process because critical investigative steps were overlooked or mishandled. FCPA prosecutors confirm that such procedural missteps often require additional work and can have a very negative effect on the outcome of the case if, for example, evidence is lost or witnesses become unavailable to the government.

The first priority in developing an effective plan is assembling a team that has the requisite competence and independence. The DOJ and SEC will insist upon these characteristics, as will the company’s outside auditors. The team may consist entirely of outside advisers, primarily a law firm and a forensic accounting firm, or entirely of in-house legal and accounting resources, provided that those latter resources have the requisite expertise and experience, are sufficiently removed from the business units and employees being investigated (independence), and can be made available for the investigation on a priority basis for an extended period. Often the team is a blend of both approaches, combining appropriate outside and in-house expertise. There is no question that the judicious use of effective in-house resources can reduce FCPA investigative costs dramatically.

Staffing decisions should include geographic considerations. There is a trade-off between keeping the team small or broadening the team by using resources that are located in or near the country in which the alleged misconduct occurred. For example, we recently completed
an investigation in the Far East and were able to
efficiently deploy our firm’s lawyers in Hong Kong,
China, and surrounding countries who were in far
closer proximity than our FCPA team in Washington,
DC. This approach only worked because those
lawyers were well-trained and experienced in
handling global anti-corruption investigations and
worked closely with our US FCPA team.

The next set of significant potential cost-savings
are internal to the company: the reporting lines and
points of contact for the investigative team. It is
critical at the outset to determine how, to whom and
when the investigative team will report. Related is
the question of who or which corporate body will be
vested with the authority to make decisions about
the investigation as it proceeds. This latter point
is important because FCPA investigations tend to
be iterative, dynamic processes that require ‘real
time’ decision-making about issues such as new
leads to pursue, documents to review or witnesses
to interview. Depending on a variety of factors, the
team may be reporting to, and under the direction
of, the general counsel or perhaps of the board of
directors or a committee of the board, but making
reporting clear at the outset minimises confusion
and overlapping responsibilities and facilitates
communication, all of which contribute to cost
reduction.

As important as reporting line clarity to the
efficiency of an investigation is the deployment of a
knowledgeable employee within the company who
possesses the necessary authority to obtain access
and information for the investigative team. Wasteful
expenses are incurred when the investigative team
cannot get information or access to company
personnel, including HR and IT personnel, because of
competing priorities.

Attention to the composition of the team and to
how it will report and get access and information
underscores two points which, though somewhat
self-evident, deserve mention because of their
critical impact on cost. The two most significant
drivers of cost in an FCPA investigation are
people and time. Obviously investigations that are
conducted by large teams over many months and
years will be much more costly than investigations
that are done by smaller, more focused teams,
over several months. Of course, sometimes speed
requires more staffing, but in trying to maximise
efficiency, it is usually a better choice to add more
resources short term than to permit the process to
drag on. Indeed, most of the ‘high cost’ FCPA cases
featured in recent media reports are investigations
that have been going on for years. It is not possible
to control how long the DOJ or SEC will take to
complete their investigations, but careful attention
to people and time are critical to greater efficiency in
conducting internal FCPA investigations.

Documenting the procedures and the allocation
of responsibilities among team members in a written
investigative plan is a useful way to keep focus.
Often these plans include a schedule for performing
each component of the investigation, which can add to efficiency. In addition, agreeing on a budget, even if it requires regular updating, is an effective way to keep abreast of, and manage costs, in an investigation.

**Disciplined scoping**

Millions of dollars of cost savings are possible if the investigation is properly scoped to address the potential misconduct. The key components of scope are the geographic range of the investigation and the period under review. Regarding the former, misconceptions abound. Despite what is commonly heard from companies that have endured FCPA investigations, the discovery of a corruption problem in one country does not necessarily require a global investigation of the company’s operations or even a complete investigation of its operations in all emerging markets. Whether the scope should extend beyond a single country depends on a variety of factors, such as whether personnel implicated in misconduct in one country have similar responsibilities for other countries, how high up within the company knowledge of that misconduct exists, similarities in business structure, customer base and level of corruption risk, and the overall quality of the company’s compliance controls. Not only is it reasonable for a company to limit the geographic scope of its investigation, such limits can be effectively negotiated with the DOJ and the SEC. For example, we handled an FCPA case for a service business that operated in over 90 countries, and the DOJ was willing to allow the company to focus on only nine countries for thorough investigations and only provide information on discreet issues that had arisen in another 20-30 countries – a process that involved limited investigative work. That resolution alone saved the company tens of millions of dollars. Be sceptical when a global investigation is suggested.

The period under review can be somewhat flexible. The rule of thumb has been five years, largely because the general statute of limitations for FCPA offences is five years. Companies frequently phase the period, starting by looking at the last two to three
years and making judgements about going back further depending on what the first phase reveals.

**Maximising efficiencies in conducting the investigation**

Considerable savings can be realised through the exercise of experienced, well-informed judgement about the conduct of the investigation, primarily in prudent staffing and thoughtful transaction testing. Of course, it is vital that a thorough, comprehensive investigation be done to satisfy the standards of the SEC and the DOJ.

The typical first step in conducting an investigation is collecting evidence, most of which is electronic data from servers and employee computer hard drives. Once data is collected and loaded on to a software platform for review, the next essential step to contain costs is a sensible strategy to strategically focus the review of what can be millions of potential documents.

The development and refinement of search terms have historically been the most effective tools to narrow and focus data sets for further review. Time well-spent in refining terms to more precisely identify potentially relevant documents has a significant cost-savings ‘ripple effect’ throughout the evidence evaluation process.

Once the data set is refined for review, the first level review of documents can be handled by low-cost contract lawyers, which often results in dramatic savings because their billing rates are so much lower than the rates of junior attorneys at law firms. Of course, the law firm should actively oversee the contract lawyers, exercising robust and engaged quality control. Second level review of documents to confirm relevancy decisions is usually done by the law firm. By way of example, in a recent investigation, the use of contract lawyers overseen by our lawyers, as described above, resulted in $6.7m in savings for the company. Additional savings in document review may result from the use of predictive coding and other emerging document review technologies.

Transaction testing offers other opportunities for savings in two key respects. As the forensic accountants assimilate and begin to test basic accounting information, patterns may emerge that permit the deployment of sampling methodologies.

“Considerable savings can be realised through the exercise of experienced, well-informed judgement about the conduct of the investigation, primarily in prudent staffing and thoughtful transaction testing.”
that have a high degree of predictive accuracy and allow the company to avoid reviewing ‘every last transaction’ in a particular data set. In addition, in situations where there are repetitive transactions, reasonable projections can be made about what may be hundreds, if not thousands, of similar transactions, which avoids the expensive proposition of reviewing each one. Evaluating the materiality of transactions for review should also be part of the process, and reasonable judgements can be made that certain types of transactions or transactions involving low dollar amounts will be exempted from review or at least from the level of review of other, more important transactions.

During the course of the investigation, it is also possible to engage the government in discussions when evidence is particularly difficult or expensive to access. Recovery of electronic data from storage tapes can be a cumbersome and expensive process, and the government has been willing in certain circumstances to engage in ‘cost-benefit’ discussions about the processing and review of such data.

Selecting witnesses for interviewing should be subject to the same considerations of efficiency. Not every witness with relevant information need be interviewed if reasonable judgements can be made that such interviews would be repetitive or unlikely to add to the evidence already developed. Caution of course is necessary in cases where multiple witnesses are important to corroborate key facts or to ensure that the full story is told.

**Deploying strategic compliance enhancements**

One of the most overlooked aspects of cost savings in FCPA investigations is the importance of evaluating possible case resolution outcomes throughout the investigation period and taking steps that may have the effect of reducing the overall fines and penalties, as well as limiting costly ongoing reporting or other accountability measures that the SEC or DOJ may impose.

Often companies are hesitant to embark on compliance program enhancements during the course of the investigation for fear that such activity might be considered by the authorities as an admission of wrongdoing that requires correction. In fact, rarely is this a legitimate concern. While it is true that a complete and effective remediation plan depends to a great extent on the results of the investigation so that it is clear exactly what remediation is necessary, compliance program enhancements as investigations progress can have an important impact on the outcome of the case.

For example, we represented a company under investigation by the DOJ that had no compliance program whatsoever. The case involved serious and extensive criminal conduct over many years, much of which was known by senior management. When coupled with no compliance program, that pattern of
conduct would almost certainly have caused the DOJ to impose an independent compliance monitor for at least three years after the case had been resolved. Such a monitor could easily have cost the company tens of millions of dollars. However, from the early stages of the case we worked with the company to establish and train its newly appointed chief compliance officer and his staff, as well as to involve them in investigation activities. The DOJ reviewed the credentials of the compliance staff and even interviewed them. Over the course of the three year investigation, the DOJ became comfortable with the company’s commitment to compliance as well as with its compliance staff. At the end of the process, the DOJ did not recommend a monitor, but rather agreed to a much less expensive and less intrusive compliance consultant. That decision alone probably saved the company over $20m.

It is also important to take the mystery out of dealing with the DOJ and the SEC. Despite the appearance of FCPA case resolutions, which, in the case of the DOJ, seem to involve precise calculations of fines and penalties under the US Federal Sentencing Guidelines, or, in the case of the SEC, calculations of profits for the purpose of disgorgement, these agencies have broad discretion in assessing fines, penalties and disgorgement. Negotiation is possible and can yield significant savings. For companies that cooperate in DOJ and SEC investigations, as indicated earlier, these agencies have also been receptive to discussions about scoping and conducting investigations, and reasonable in many instances about the company’s desire to follow procedures that would reduce investigative costs. RC

Nancy J. Rosenfeld
Of Counsel
Baker & McKenzie LLP
T: +1 202 452 7099
E: nancy.rosenfeld@bakermckenzie.com

Richard N. Dean
Partner
Baker & McKenzie LLP
T: +1 202 452 7009
E: richard.dean@bakermckenzie.com
In November 1991 the US Sentencing Commission issued Chapter 8 of the federal sentencing guidelines, which raised two new risks regarding crimes in the workplace: (i) a personal threat; and (ii) a corporate threat. The personal threat said that executives could be subject to civil and/or criminal charges if an employee of theirs committed a crime in the workplace. Whether they know about or participate in the crime is irrelevant. Wilful blindness is not a defence. And in such instances, the corporate threat could impose mandatory fines up to $290m (a threshold long since pierced). However, the Commission did something very creative, offering that the existence of an effective ethics and compliance program can reduce, mitigate or eliminate those risks. Thus the ethics profession was born.

In early 2010, the OECD Working Group issued its Good Practice Guidance that essentially adopted the US federal sentencing guidelines for 45 signatory
nations. This has become the global standard for corporations regarding the prevention and detection of criminal activity, and for reputation risk management. Even today, emerging market multinational corporations are adopting similar internal safeguards to protect against corruption and malfeasance.

Despite considerable progress in addressing both internal and external organisational risks, there’s no shortage of malfeasance that threaten corporate reputations. The stunning growth of social media, mobile technologies, and ‘big data’, along with the rapid rise of micro-bloggers and public and in-house helplines, have ushered in an era of transparency that is unprecedented, exposing illegal transactions and raising profound new ethical questions in the way business is conducted. Quite simply, in an age of information there are no secrets anymore, and no place to hide. These new technologies are also driving hactivism, thus blurring the lines between research, due diligence, espionage and privacy issues.

**Current risks**

Certainly, among the most visible risks these days are bribery and corruption. From Illinois to Indonesia, and from Shanghai to Siberia, bribery abounds. Even marquee names like IBM, IKEA, Ralph Lauren, Microsoft and Alstom have been embroiled in corruption scandals. In particular, China has very recently stepped up to assert the rule of law in pursuing corruption charges. Investigations include the pharmaceutical, medical device and energy industries, and also include numerous high-level and transparent cases of party officials. Taken together, it is clear that China’s new president is sending a powerful message of the government’s intolerance for corruption.

“Building appropriate internal safeguards, and strengthening third party due diligence, are essential to limiting the exposure that many companies experience.”

Building appropriate internal safeguards, and strengthening third party due diligence, are essential to limiting the exposure that many companies experience. This much we know – wherever there is money, there is the threat of corruption. And wherever there is lots of money, there is the potential for lots of corruption. No one is immune. Those engaged in insider trading are more easily identified today given improved access to
information. Data scientists can reverse engineer or follow algorithmic patterns in our public markets, allowing regulators to more easily follow money flows where insider trading exists. Galleon’s founder Raj Rajaratnum was found guilty and sentenced to eleven and a half years in jail. He took down with him Rajat Gupta, ex-McKinsey CEO and Goldman Sachs director, who has been found guilty of insider trading and sentenced to two and a half years. Currently SAC Capital, the giant hedge fund, has been charged with failing to supervise and is currently in negotiations with federal regulators.

Recently, the US Securities and Exchange Commission announced that it is stepping up its focus on accounting fraud. Names like Enron and WorldCom were the face of large-scale frauds in the US, while Satyam Computer in India and Olympus Corporation in Japan are stunning examples on a global scale.

Since the Great Recession, wherein the credit markets froze in late 2008 setting off a global economic tsunami, the global banking industry has been under siege by regulators. Numerous money centre banks have been charged with manipulating LIBOR rates, which have resulted in settlements against Barclays, UBS and others exceeding $2.5bn, with banking authorities in the US, the UK and Japan. In addition, money laundering investigations have resulted in HSBC agreeing to a $1.9bn settlement, and Standard Chartered paying $340m.

Meanwhile, a number of banks continue to be the focus of civil and criminal investigations for their method of conducting business. In particular, JPMorgan Chase has become the focus of substantial settlements. In late September 2013, the bank settled with authorities for over $920m concerning the London ‘Whale’ trades, and another $389m for credit card fraud. In addition, most recent discussions with the US Department of Justice suggested Chase may face as much as an $11bn settlement regarding its role in underwriting mortgage-backed securities.

Notwithstanding these extraordinary new risks and settlements, there are several recent actions that offer the potential for measureable progress in the years ahead.

First, in November 2009, 150 nations became signatories to the UN Conventions Against Corruption. Not only did these nations pledge to enact laws against corruption, but also to enforce them. Importantly, in an historic move, these nations agreed to hold public peer-to-peer assessments regarding how well respective nations’ are pursuing enforcement. In addition, the OECD Conventions Against Corruption have established very clear guidelines for corporations to establish anti-corruption measures, also holding public accountability by peer countries.

Second, in the US there have been more prosecutions for violations of the Foreign Corrupt Practices Act (FCPA) in the past three years than in
the previous 30 years combined. Violators include both US headquartered companies, as well as non US based corporations who access US capital markets.

Third, in 2010, the UK Bribery Act came into effect, which goes further than the US Foreign Corrupt Practices Act on two measures: (i) any company doing business in any jurisdiction of the United Kingdom that is found guilty of corruption is subject to the act, whether the bribe took place in a UK jurisdiction or not, and; (ii) it pertains not only to bribing public officials, but also to commercial bribery. The Serious Fraud Office is actively engaged in numerous investigations.

Lastly, beginning in October 2010, the G-20 adopted an anti-corruption platform for discussion. Since then, the G-20 has advanced its discussions in subsequent meetings in Paris, Mexico City and, most recently, in Moscow. This is evidence that there is a serious effort to create collective action and a high-level of cooperation among these countries.

Summary
Ethics and compliance executives have come a long way in developing sophisticated measures to prevent, detect and mitigate the risk of malfeasance in their organisations. So, too, have those who wish to violate the rule of law and gain unfair advantages.

Clearly, there is an increasing resolve by both the public and private sectors worldwide to strengthen internal controls, while prosecuting those who violate the rule of law. No one company or country by itself, however, can mitigate the existence of fraud and corruption. For sure, it will take collective actions and practical partnerships between government, business and the NGO community to effectively mitigate risk. Looking ahead, however, by working together, these efforts combined with an increasingly transparent world and collective intolerance for corruption offer hope and promise for a better world. For whatever shortcomings we may experience, in the end we must remember that ethics is about progress, not perfection. RC

Keith T. Darcy
Executive Director
Ethics & Compliance Officer Association (ECOA)
T: +1 781 647 9333
E: kdarcy@theecoa.org
HOT TOPIC

RISK AND COMPLIANCE ISSUES ARISING FROM THIRD-PARTY BUSINESS RELATIONSHIPS
John Hurrell was appointed as Chief Executive of Airmic in January 2008 following a career of almost 30 years in the Marsh and McLennan Group of Companies. Prior to joining Airmic, Mr Hurrell was the Chief Executive of Marsh’s Risk Consulting business throughout Europe and the Middle East. Having been educated in London, Mr Hurrell entered the insurance industry in 1968 and qualified as a Fellow of The Chartered Insurance Institute.

Karina Bjelland is a senior managing consultant in the Financial Institutions practice at Berkeley Research Group, LLC. The Financial Institutions Practice advises clients and their counsel in the areas of operational risk, regulation, accounting and finance and serves the needs of hedge funds, funds of funds, private equity funds, alternative investment funds, investment advisers, broker-dealers, insurance companies and banks. Prior to joining BRG, Ms Bjelland held various positions in the areas of financial institution supervision and regulation, and securities litigation consulting.

John Ivanoski serves as the Leader for KPMG’s Regulatory practice. He has over 25 years experience providing audit and risk advisory services to global organisations. Mr Ivanoski has extensive experience in managing large global projects related to regulatory and risk transformation, third-party risk management, enterprise risk management, operational risk including third-party vendor management, and target operating models. He also served as a US Peace Corps Volunteer in Malawi, Africa assisting in the development of a credit cooperative system.
RC: Could you provide a general overview of the potential risk exposures that may arise when dealing with third-party business partners and vendors?

Bjelland: The list of potential risk exposures is quite extensive. There are privacy risks, transaction risks, technology risks, credit risks, compliance risks and risks to reputation. In addition, there are numerous other specific issues to consider that fall under the more general categories such as copyright and patent laws, and concerns related to ownership, liability, consumer protection and compliance monitoring and records retention. Finally, there are risks specific to an industry or type of business. Third-party risk exposure is relevant to all industries, not just financial, and each one of these has their own additional industry-specific risk issues to consider. For example, an oil company has to consider the additional risk of pollution-related liabilities in their contracts with third-parties, such as drilling contracts.

Ivanoski: Third parties such as service providers, alliance members, consultants and suppliers can expose their business partners to a range of risks. While specifics depend on the industry, service or product being offered, potential third-party risks include the following. First, reputational risk from delivery of substandard products and services, disruption of services, and failure to meet the expectations of customers. Second, compliance risk from violations of laws and regulations such as consumer protection, securities filings, anti-bribery and corruption (ABC) and anti-money laundering (AML), or nonconformance with internal policies. Third, operational risk related to the potential failure of people, processes or systems. Fourth, credit risk related to services and transactions involving extension of credit such as origination, underwriting, servicing and processing. Finally, strategic risk from failure to implement business decisions or poor execution of those decisions.

Hurrell: Recent research would suggest that the majority of the value chain in most companies is now provided by outside entities such as subcontractors, suppliers and distribution networks. This means that more than half the risk to the brand or reputation of a company is outside its direct control and often operating in countries which are relatively unfamiliar to the principal. This will have been very different only a few years ago, and some companies have been better at making the adjustments to risk management strategy demanded by their changed business models than others.

RC: In what ways can third-party violations and misconduct negatively impact a company’s brand and reputation? Have there been any notable examples in recent years?
Hurrell: There are multiple examples in the consumer clothing and food industries, such as dangerous sweat shops and horse meat. The challenge here is the prevalence of all forms of social media closely connected with traditional news media which potentially turns every human being on the planet into a news reporter. The traditional media will seek brand connections and the impact will be instant – often faster than any company’s contingency plan can respond.

Ivanoski: A company’s reputation can be affected negatively if its third parties do not deliver products and services at the right level of quality, and in line with contracts, policies and customer expectations. This failure can produce a variety of negative effects for the company, including reputational risk through brand impact and unfavorable press, as well as regulatory inquiries, fines and other enforcement actions. In the financial services industry, the Consumer Financial Protection Bureau (CFPB) has handed out enforcement actions to several banks whose third parties were, in the eyes of regulators, causing consumer harm due to sales of add-on products that did not benefit the customer or where customers were incorrectly foreclosed on. A critical point to note is that, along with the reputational impact of the enforcement actions, there were significant monetary penalties.

As a result of notable high-profile issues, banks have made significant enhancements in third-party risk management.

Bjelland: The public assumes that you have vetted a vendor or service provider when you choose to enter a business relationship with them. They become an extension of your company or image and you may become associated with their conduct, whether positive or negative, even if you were even aware of it prior to the event occurring. Recently, a group of banks sued a third-party payment company after the customers’ personal data was breached. Unfortunately, this has happened quite often over the last few years and has damaged companies’ brands because customers lose faith that their information will be protected, and customers may then choose not to continue the business relationship. In addition

“A company’s reputation can be affected negatively if its third parties do not deliver products and services at the right level of quality, and in line with contracts, policies and customer expectations.”

John Ivanoski, KPMG
to reputational damage, there can be significant financial costs associated with this sort of incident, including litigation costs and reimbursement costs to customers. Currently, the Office of Comptroller of the Currency (OCC) and Consumer Financial Protection Bureau (CFPB) are looking into concerns that JP Morgan may have misled customers who purchased credit cards with identify theft protection through a third-party vendor.

**RC:** Audits, inspections, and other processes enable companies to evaluate third-party controls and compliance measures. What steps can a company take to strengthen the due diligence it performs on third-parties?

**Ivanoski:** Inventorying and assessing third parties based on the risks they expose the business to allows for a risk-based approach to management of third parties, which is vital given limited resources. A due diligence process that quickly identifies the risks a third-party exposes the organisation to, and directs the appropriate oversight function to exercise-focused control, is essential to avoid information overload. Each third-party may have a different combination of risks, requiring an appropriate blend of risk management activities from the oversight functions. Clarifying roles and responsibilities across the oversight functions, business lines and internal audit assists with ensuring the appropriate risk management functions are aware of the risk and managing it accordingly. Executing contracts that clearly set out requirements, expectations and responsibilities, and provide the ability to conduct on-site reviews, collect relevant risk and performance information, are key to managing the risk third parties expose the organisation to. The focus of on-site reviews should include understanding how well the third-party’s risk management functions work, how it monitors and manages compliance risk and how well it is performing.

**Bjelland:** A company should thoroughly evaluate third-party service providers prior to entering into a business relationship, and should also continue to regularly monitor controls and compliance measures throughout the relationship, and ensure that the third-party shares the same goals and adheres to the same policies. Due diligence on the third-party should include researching their reputation, checking references, and using all available resources of information such as state attorneys general or the better business bureau. If a third-party organisation is new, a company should exercise additional caution. It is also critical to review a third-party’s financial information and insurance coverage. Audit and regulatory reports should be reviewed, such as an SAS-70, if one is available. The evaluation should be just as thorough as if the company were to enter
a financial transaction with the third-party, as the risks can be equally significant.

**Hurrell:** Most organisations do have good oversight of their tier one suppliers but the challenge very often is to achieve a line of sight into tiers two and beyond. This is where many of the problems arise. We see two distinctly different types of approach to the problem – a strictly legal approach with clear penalties; and a more partnership style of approach, which often encourages more openness between the parties. Circumstances will dictate the best option in any given set of circumstances but the second option should always be considered – this is not always the case at present.

**RC:** Employees at third-party organisations should be encouraged to report compliance or ethics violations. What processes can firms put in place to ensure this occurs, and to remedy any shortcomings at third-party organisations?

**Bjelland:** Make sure that reporting policies are clearly and regularly communicated to third-parties and employees through training and other measures, and establish a channel for employees to easily escalate any issues or ask questions, such as a confidential hotline devoted to answering questions related to potential issues and for reporting issues, such as a whistleblower hotline. Companies should encourage employees to timely and accurately report concerns, and ask questions early on. It is also important to provide protection against employee retaliation as this can discourage employees from speaking up. If there are shortcomings at a third-party, perhaps the company has resources that can be utilised by the third-party, whether technological resources or staff resources. However, if a third-party is not adequately equipped to handle the increased business or services required of them in the proposed business...
arrangement, the company should seriously consider whether they should really be entering into that business partnership.

Ivanoski: Depending on the sophistication of the risk management infrastructure at the third-party, there may or may not be a mechanism, such as a hotline, to report compliance or ethics violations. This should be considered during the due diligence review. Third parties should, where appropriate, be required to implement ethics and compliance hotlines, for example, in line with better practices to ensure that there is a reporting mechanism for employees. Training the third parties’ employees on the client’s internal policies and procedures, expectations, and requirements drives an understanding of what is expected, keeps employees abreast of changes, and allows them to assess and decide on violations and shortcomings. An appropriate monitoring problem should ensure employees are adhering to internal policies and procedures.

RC: Do any particular risks emerge when working with third-parties in the emerging markets? What steps can firms take to reduce potentially damaging exposures in these regions?

Hurrell: The starting point is to understand the likely differences in approach locally on critical issues such as ethics, employment practices such as health and safety, respect for intellectual property, the legal system and local infrastructure. Many firms will work through a strong local partner rather than simply trying to impose ‘head office’ standards and procedures locally. The challenge is to operate according to local best practice whilst recognising that western media will always apply a western lens to their reporting of any failures. In particular this will always take place where a big consumer brand is involved.

Ivanoski: Operating in emerging markets exposes companies to country risk – the risk that economic, social and political conditions and events in a foreign country will adversely affect the company’s financial interests. In today’s environment, the most
notable risk facing organisations operating outside the United States include violations of anti-bribery and corruption (ABC) laws, and requirements under the Foreign Corrupt Practices Act (FCPA). Given the complexity of US laws and regulations, a growing number of US companies are retaining the regulatory and compliance responsibility in outsourcing/offshoring relationships, and pricing the requisite oversight activities into their agreements because the risk of non-compliance is perceived to be too great. Steps that can be taken to manage this risk include: incorporating specific risk assessment criteria for offshore characteristics; retaining knowledgeable skilled resources to draft contract provisions and understand the legal jurisdictions where the third-party is based; conducting on-site reviews to determine quality of management and staff, and gaining a firsthand understanding of the culture and business operating conditions.

**Bjelland:** The laws and ways of conducting business are clearly different in other regions, especially emerging markets, where some regulations may not have even been established yet or are not clearly defined. It is hard to avoid using a third-party when entering a new market because a company should hire or consult with individuals who have experience in that region and are familiar with the laws and potential problems that could occur by doing business there. There are many issues to consider in these markets. Foreign Corrupt Practices Act (FCPA), money laundering concerns, and employee safety are just a few of the issues to consider. FCPA and other legislation require companies to perform due diligence on foreign third-party business partners, and the Department of Justice (DOJ) and the Securities & Exchange Commission (SEC) have fined US companies for not performing sufficient due diligence on these partners. Choice-of-law and jurisdictional issues – and the possibility of dealing with foreign courts – need to be considered when working with international third-parties and drafting contracts. Political and socio-economic factors can increase the difficulty of conducting business in certain regions. Additionally, a company needs to consider economic and trade sanctions, and potential concerns related to terrorist financing, bribery of government officials or commercial bribery, risk of child labour, and product safety concerns. A company should consider whether all of these risks outweigh the benefits of doing business in that region. Also, if the business model of the company and economies of scale permit, perhaps there should be a trial period or testing of only limited products or services before fully committing to that region. As an example, outsourcing to offshore contractors by financial institutions has increased in recent years because of savings due to lower wages and other reduced costs. However, instances of fraud and identity theft have increased. Offshore outsourcing of data services or call centers occurs
frequently and both pose risks to customer and other confidential information.

**RC: Have you seen, or do you expect, any regulatory or legislative changes to affect third-party relationships in your region?**

**Ivanoski:** In November 2012 the Securities and Exchange Commission (SEC) and Department of Justice (DOJ) released guidance on what is expected in developing and monitoring an effective ABC compliance program. Further, the SEC has established a unit focused on FCPA, and continues to pursue companies, officers and directors when violations are suspected. The US federal bank regulators have extensive examination guidance on third-party risk management and they conduct comprehensive examinations in this area. Further, they are planning to release updated guidance on the management of third parties in the near future. Initial expectations suggest they may expand the term ‘third-party’ to include a wider swath of entities, such as suppliers, alliances, joint-venture partners and vendors, as well as require more reporting on third-party risk to the board. In addition, under the Bank Service Company Act, the U.S federal bank regulators comprising the Federal Regulated Institutions Examination Council (FFIEC) have authority to examine banks’ third-party service providers. In the financial services industry, public consent orders and other enforcement actions related to regulatory violations have occurred with a resultant increase in regulatory scrutiny of these relationships. This focus has lead to an increase in control and oversight of third parties by banks. Regulators have sent a clear message that banks can outsource operations, but can’t outsource responsibility for the conduct of their third-party providers.

**Bjelland:** Both new regulations and increased enforcement of existing legislation will increase the importance of third-party oversight. A company’s liability for the actions of their third-party relationships is becoming increasingly defined through actions by regulators and in litigation, and this process will be ongoing. Last year, a landmark $25bn settlement was reached between five large banks and 49 state attorneys general which requires lenders to boost their oversight of third-party vendors. In addition, the CFPB has new mortgage rules that will become effective in January 2014 and will affect third-party business relationships. The news also reports the Federal Deposit Insurance Corporation (FDIC) and DOJ have been reaching out to banks over concerns related to certain online lenders. There have also been numerous recent legislative efforts related to protecting individuals’ privacy, which becomes more of a risk when third-parties are involved.
**RC:** When working with a third-party, management should ensure that the specific expectations and obligations of both the firm and the third-party are outlined in a written contract. What risk-related issues should firms address when structuring such a contract?

**Bjelland:** This phase is crucial because poor planning and consideration of potential scenarios in the early phases of an agreement can lead to increased risk. The contract needs to address who is responsible for specific tasks, all rights and obligations for both parties, and also indemnification, business continuity planning, dispute resolution, locations, use of equipment, and ownership of data and IT contracts, for example. A company should review guidance from their relevant regulators, such as the FDIC or OCC in the case of financial institutions, on third-party business relationships. The contract should include a detailed business plan, service level agreements and sections on audits and monitoring and vulnerability assessments. The board and key management should be involved in the entire process. The contract should clearly define what the exit strategy is if the relationship does not work out, including the timeline and cost. A company should hire experienced staff, or make sure that the third-party has experienced staff, in key areas such as IT and security. They may cost more but it could save money in the long run. The costs associated with maintenance of software and other items should be considered as well. An example of a potential concern is that a company could enter into a contract with a domestic third-party service provider without knowing that the third-party is in fact subcontracting some of their services offshore.

**Ivanoski:** Current financial services regulatory guidance, for example, outlines a variety of topics banks should consider when entering into third-party contracts, including scope of the arrangement, responsibilities, performance measures and benchmarks, information confidentiality and security,
compliance with specified laws and regulations, access to information for performance and risk management, the right to audit third parties and their subcontractors, and business continuity. Companies in all industries need to be comfortable the initial perceived benefits of a proposed relationship will not be offset by reputational risks and non-compliance costs. Performance under the contract should be defined, but as noted, appropriate oversight and management controls should be established, including dispute resolution, indemnification, cost and compensation for non-compliance with contract and default and termination.

**Hurrell:** Contracts must focus on standards and quality and all other aspects which could impact on reputation. However, contracts should be drafted in a way that emphasises the partnership aspect and encourages open dialogue. For example, penalty clauses should usually only kick in if there has not been a voluntary disclosure of a problem within a prescribed period.

**Ivanoski:** As a rule of thumb, third parties should be managed as if they were an internal department of the organisation. Assessing the quality of the products and services delivered by the third-party on a regular basis assists with understanding their performance relative to the contract. Monitoring the contract’s specific terms and conditions is a way to ensure agreed-upon performance, control and risk management. Monitoring of controls through on-site reviews; assessing changes to the business; reviewing policies and training requirements; and assessing the resiliency of the third-party with regards to its financial health and its ability to withstand business disruption, are activities that drive effective risk management.

**RC:** Organisations should maintain adequate oversight of third-party activities and the quality control measures governing products and services provided. What features should be included in a firm’s monitoring program?
**Bjelland:** The first step is to fully understand the third-parties’ business lines and products. If a company does not understand how a product or service works at the third-party, they need to make sure that they become educated prior to beginning the relationship because a company cannot monitor something they do not understand. An example could be how specific software works, or how confidential information is encrypted and stored, or where data is housed. A lack of knowledge could lead to customer complaints or worse scenarios down the road. The features that should be included in a monitoring program are operational audits, vulnerability assessments, fraud monitoring and quality checks and controls. The policies and procedures for monitoring should be consistent across the board. A company should ensure that training of employees is adequate and experienced staff is employed, especially in key areas such as IT and security. These employees may cost more but it will save money in the long run. Examples of insufficient monitoring include recent cases where third-parties performing underwriting led to increases in delinquencies, or weaknesses in security led to information being hacked.

**Hurrell:** There needs to be clear terms in the contract between the parties stating that appropriate standards of quality – safety and environmental protection, for example – will be achieved by the contractor. This requirement should be stated as an expectation of the contractor, but the principal should ensure that it does not assume responsibility. The firm should obtain assurance from contractors that standards are being achieved. Also, there should be confidentiality requirements in the contract.
In today’s global market, a multijurisdictional approach to compliance is essential. With offices in key financial centres and emerging markets, Baker & McKenzie lawyers are already on the ground, ready to tackle investigations. Our approach ensures that your compliance program satisfies the expectations of enforcement authorities around the globe, providing protection where you need it most.

Richard N. Dean
Partner
Washington, DC, United States
T: +1 (202) 452 7009
E: richard.dean@bakermckenzie.com

Joan E. Meyer
Partner
Washington, DC, United States
T: +1 (202) 835 6119
E: joan.meyer@bakermckenzie.com

Paul J. McNulty
Partner
Washington, DC, United States
T: +1 (202) 835 1670
E: paul.mcnulty@bakermckenzie.com
Berkeley Research Group, LLC is a leading global expert services and consulting firm that provides independent expert testimony, litigation and regulatory support, authoritative studies, strategic advice, and document and data analytics to major law firms, Fortune 500 corporations, government agencies, and regulatory bodies around the world. From testifying in high-stakes litigation to consulting on large-scale projects, BRG experts and consultants combine intellectual rigor with practical, real-world experience and an in-depth understanding of industries and markets.

Charles Lundelius
Director
Washington, DC, United States
T: +1 (202) 480 2684
E: clundelius@brg-expert.com

H. David Kotz
Director
Washington, DC, United States
T: +1 (202) 480 2752
E: hdkotz@brg-expert.com

David Martin
Principal
New York, NY, United States
T: +1 (646) 205 9381
E: dmartin@brg-expert.com
KPMG is a global network of professional firms providing Audit, Tax, and Advisory services. We operate in 156 countries and have more than 152,000 people working in member firms around the world. KPMG LLP, the United States member firm of KPMG International, traces its origins back to 1897 and since 1994 has been a limited liability partnership registered in the state of Delaware. With more than 24,000 employees and partners, KPMG LLP is a leader among professional services firms.

John Ivanoski
Partner
New York, NY, United States
T: +1 212 954 2484
E: jivanoski@kpmg.com

Graham Murphy
Principal
Chicago, IL, United States
T: +1 312 665 1840
grahammurphy@kpmg.com

Jeffery Hulett
Managing Director
McLean, VA, United States
T: +1 703 286 6695
E: jhulett@kpmg.com
Airmic is the association for everyone who has a responsibility for risk management and insurance for their organisation. Members include company secretaries, finance directors, internal audit as well as risk and insurance managers. We support our members in a range of ways: through training and research by sharing information; through our diverse special programme of events; by encouraging best practise; and by lobbying on subjects that directly affect risk managers and insurance buyers. Above all, we provide a platform for professionals to stay in touch, to communicate with each other and share ideas and information.

John Hurrell
Chief Executive
London, United Kingdom
T: +44 (0)20 7680 3088
E: john.hurrell@airmic.co.uk

www.airmic.co.uk

The purpose of the Association for Federal Enterprise Risk Management (AFERM) is to be a professional organisation dedicated to the advancement of federal Enterprise Risk Management (ERM). The Association serves its members by providing a forum for discussion of issues relevant to participants in the federal risk management profession, sponsoring appropriate educational programs, encouraging professional development, influencing governmental risk management policies and practices and serving as an advocate for the profession. The Association serves government officials and the public by sponsoring efforts to ensure full and fair accountability for management of risk in achieving organisational objectives.

Dr Doug Webster
Co-Founder
Arlington, VA, United States
T: +1 703 441 2212
E: dougwebster@cambiocg.com

www. www.aferm.org
Australian Institute of Company Directors

Australian Institute of Company Directors is Australia’s pre-eminent organisation for directors, dedicated to making a difference in the quality of governance and directorship. Our role is to provide leadership on director issues and promote excellence in governance to achieve a positive impact for the economy and society. Since our early beginnings, we have developed as an organisation recognised for quality and professionalism.

Michelle Wood
Media and Government Relations Advisor
Sydney, NSW, Australia
T: +61 2 8248 6612
E: MWood@companydirectors.com.au

John Colvin
Chair
Sydney, NSW, Australia
T: +61 2 8248 6600
E: gndi@companydirectors.com.au

www.companydirectors.com.au

Ethics & Compliance Officer Association

The Ethics & Compliance Officer Association (ECOA) is a member-driven association exclusively for individuals responsible for their organisation’s ethics, compliance, and business conduct programs. The only organisation of its kind, its members represent the largest group of ethics and compliance practitioners in the world. The ECOA is credited with formally ‘founding’ the ethics and compliance field in 1991. The ECOA assembles people who are new to the field, as well as those with years of experience to share. Through the ECOA, practicing ethics and compliance officers collectively address the tough issues they face every day.

Keith T. Darcy
Executive Director
Waltham, MA, United States
T: +1 781 647 9333
E: kdarcy@theecoa.org

www.theecoa.org
National Association of Corporate Directors

The National Association of Corporate Directors (NACD) is the only membership organisation focused exclusively on advancing exemplary board leadership. Based on more than 35 years of experience, NACD identifies, interprets and provides insights and information that corporate board members rely upon to make sound strategic decisions, confidently confront complex business challenges and enhance shareowner value. Fostering collaboration among directors and governance stakeholders, NACD is shaping the future of board leadership. To learn more about NACD, visit www.NACDonline.org.

Alexandra R. Lajoux
Chief Knowledge Officer
Washington, DC, United States
T: +1 202 280 2185
E: arlajoux@nacdonline.org

www.nacdonline.org

The Risk Management Association

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry.

Bill Githens
President and CEO
Philadelphia, PA, United States
T: +1 215 446 4124
E: bgithens@rmahq.org

www.rmahq.org
Santa Clara University, a comprehensive Jesuit, Catholic university located in California’s Silicon Valley, offers its more than 8000 students rigorous undergraduate curricula in arts and sciences, business, and engineering, plus master’s, Ph.D., and law degrees. Distinguished nationally by the fourth-highest graduation rate among all US master’s universities, California’s oldest operating higher-education institution demonstrates faith-inspired values of ethics and social justice.

Dr Hersh Shefrin  
Professor of Finance  
El Camino Real, CA, United States  
T: +1 408 554 6893  
E: hshefrin@scu.edu

www.scu.edu

WomenCorporateDirectors (WCD) is the only global membership organisation and community of women corporate directors. In this new era of responsibility, WCD is committed not just to good governance, but to governance with global vision. Our members share information and insights in order to ensure best practices in corporate governance around the world. With over 2000 members in 54 global chapters who serve on over 3500 boards, WCD serves as a terrific catalyst for new thinking and networking. WCD has become a true champion for women directors and a vital source of expertise.

Bonita Z. Dorland  
Advisory Board and Member  
New York, NY, United States  
T: +1 212 628 6067  
E: bonny.dorland@gmail.com

www.womencorporatedirectors.com