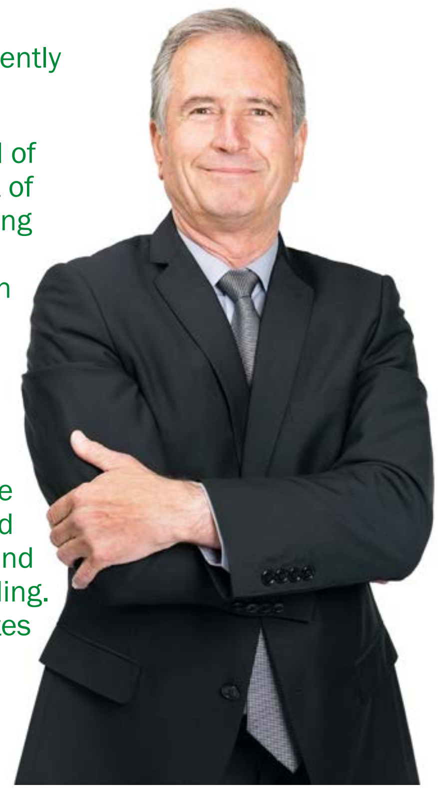
Enterprise Risk

Autumn 2018 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Spreading the word: IRM expands in APAC / **Everybody gets to play:** testing the case for diversity / **State-sponsored mayhem:** when governments hack / **Reframing risk:** what does COSO ERM mean to the profession? / **Common causes:** global threats to infrastructure projects

It's not about the manual: Paul Mather on risk management at Shell



Enterprise Risk

Autumn 2018

Editor
Arthur Piper

Produced by
Smith de Wint
Antenna Business Centre
Beck Street, Nottingham, NG1 1EQ
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

Sponsorship and Advertising Sales Manager
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

Enterprise Risk is the official publication of the Institute of Risk Management (IRM).

ISSN 2397-8848

IRM is the leading professional body for enterprise risk management. We are an independent, not-for-profit organisation that champions excellence in managing risk to improve organisational performance.

We do this by providing internationally recognised qualifications and training, publishing research and guidance and setting professional standards across the world. Our members work in all industries, in all risk disciplines and across the public, private and not-for-profit sectors.

Institute of Risk Management
2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

Editorial

Navigating the way

Over the summer, I found the time to read two classics texts from the beginning of Western literature: Homer's *Odyssey* and Aristotle's *Ethics*. In part, both are concerned with how we treat other people.

In the *Odyssey*, for example, a key theme is how to treat guests and strangers. At one extreme, the one-eyed Cyclops Polyphemus wants to eat the homesick hero Odysseus – not the best of welcomes. At the other, the goddess-nymph Calypso intends to keep Odysseus for her own pleasure for the rest of eternity by making him immortal. All the while, suitors are eating Odysseus' wife Penelope out of house and home because she refuses to marry one of them.

As Odysseus is buffeted from one trial to another, the book seeks to discuss the right balance between being rude and being open and hospitable – but because circumstances and local customs vary so much, there can be no definitive answer.

In a more analytic vein, Aristotle reaches a similar conclusion. He discusses the various personal attributes a good person ought to display – courage, generosity and so on. For example, too much courage ends up turning into rashness; not enough, into cowardice. He likens finding the middle way to attempting to locate the exact centre of a circle without proper measuring tools – in ethics such technologies do not exist.

It is better to aim at developing diversity goals and navigate the difficulties rather than wallow in a metaphorical cave

These problems have not gone away, despite attempts to put the analysis of behaviour and culture on a more scientific footing. People are complex – the interactions between them unpredictable.

Sometimes, in risk management, doing the right thing can mean acting without sufficient empirical evidence to support your views. Sarah Christman in this issue – "Everybody gets to play" – argues that while studies are thin on the ground which support the view that diversity in organisations enhances performance, this should not be a cause of inaction.

It is better to aim at developing diversity goals and navigate the difficulties rather than wallow in a metaphorical cave. Only by achieving the indirect, ethical goal of treating people fairly will organisations have the opportunity to learn the value of diversity.

Aristotle would have perhaps been happy with this approach. For him, being ethical was something you could only become good at by practice and habit. It involves trial and error, but most of all continuous effort – wishing for the best, deliberating how to achieve those ends, then voluntarily choosing those actions most likely to succeed.

Arthur Piper
Editor

Contents

10

16

20

24

26

FEATURES

REGULARS

Will your next move put your company at risk?

LexisNexis® Due-Diligence Solutions enhance your ability to:

Still puzzled about your next move?

bis.lexisnexis.co.uk/lexis-diligence

020 7400 2809

BIS@lexisnexis.co.uk

LexisNexis®

Coding for success

The Financial Reporting Council has placed risk management at the centre of its revised guidance for companies. It's time for risk managers to grasp their moment

The revised *Corporate Governance Code* issued by the Financial Reporting Council (FRC) places greater emphasis on the management of risk. Of course, IRM is delighted that this should be the case – proper risk management focuses, after all, on the risks and opportunities an organisation faces when it strives to pursue its strategic goals. Risk management is now explicitly mentioned in section one of the code – Board leadership and company purpose – as IRM and others advocated during the consultation period earlier this year.

Section one now says that the board should establish a framework of prudent and effective controls which enable risk to be assessed and managed. The provisions go on to say that companies should describe in their annual report how opportunities and risk to the future successes of the business have been considered and addressed.

Along with the code, FRC also published *Guidance on board effectiveness*, in which risk management is given a significant role to play in the running – and therefore success – of businesses.

The emphasis of the guidance is on longer-term planning and value creation, issues such as culture and in managing the expectations of different stakeholders. There is also greater emphasis on looking to the future – something that IRM has been engaging with in its *Risk Agenda 2025* project.

The very first question in the guidance offers both a challenge and an opportunity to our profession. It asks, "how do we know that management is identifying and addressing future challenges and opportunities, for example changes in technology, environmental issues or changing stakeholder expectations?" These are big issues and demand the development of forward-looking risk management techniques that need to draw upon a mixture of quantitative and qualitative data. Risk managers have historically been more comfortable with hard facts, and this will need to change.

Procedures for risk analysis and risk evaluation against risk appetite need to be established along with information on "near misses" as well as early warning key risk indicators (KRIs) and risk limits. How many risk management departments can truly say they allocate time in their current schedules for analysing near misses, learning their lessons and disseminating those findings throughout the organisation?

The same challenge arises when it comes to helping the board assess corporate culture. "Monitoring culture will involve regular analysis and interpretation of evidence and information gathered from a range of sources," the guidance says. "Drawing insight from multiple quantitative and qualitative sources helps guard against forming views based on incomplete or limited information."

> **How do we know that management is identifying and addressing future challenges and opportunities?**

It is to these larger questions that risk managers must turn if they are to enhance their role and effectiveness.

The new code adds greater impetus for all risk management professionals to take a leading role in addressing both current and emerging risks and opportunities. In doing so, risk management professionals should be proactive. An experienced risk professional is best placed to help with strategy formulation and business tactics. The risk manager reinforces their valuable contribution by testing strategy, reviewing new initiatives and helping to improve operational efficiency within the business.

As IRM members, we have the skills and tools available to us to make that contribution. Our qualifications can help us occupy those top positions in organisations where we can add significant value. It is time for us to grasp the nettle.

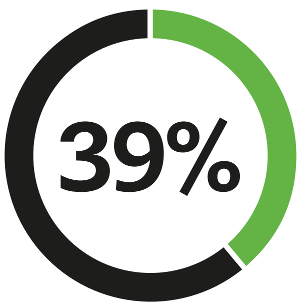
Socrates Coudounaris is IRM chairman.

The latest stories and news affecting the wider business environment as interpreted by our infographics team

Active cyber defence “highly effective”

Getting hackers to focus on honey-pots and other decoys pays dividends for the companies employing such techniques

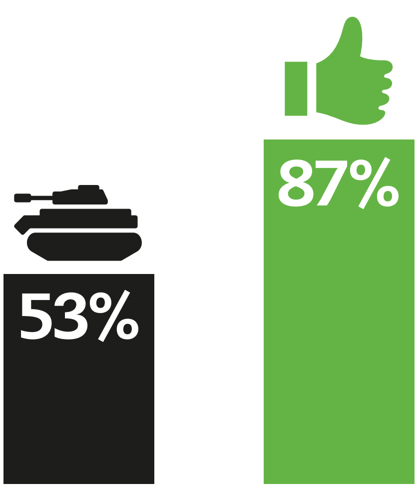
ORGANISATIONS FAMILIAR WITH ACTIVE DEFENCE:



Not-at-all/Slightly

Moderately

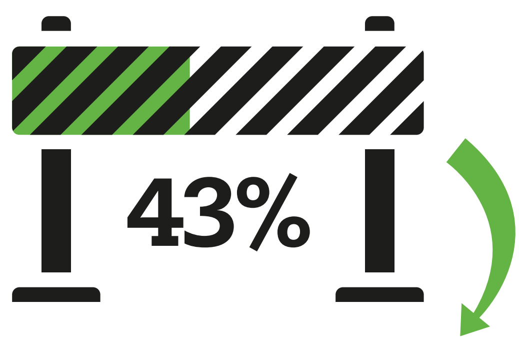
Very/Extremely



Percentage of organisations using active defence

Percentage of those who found it effective

MAIN BARRIER TO IMPLEMENTATION:

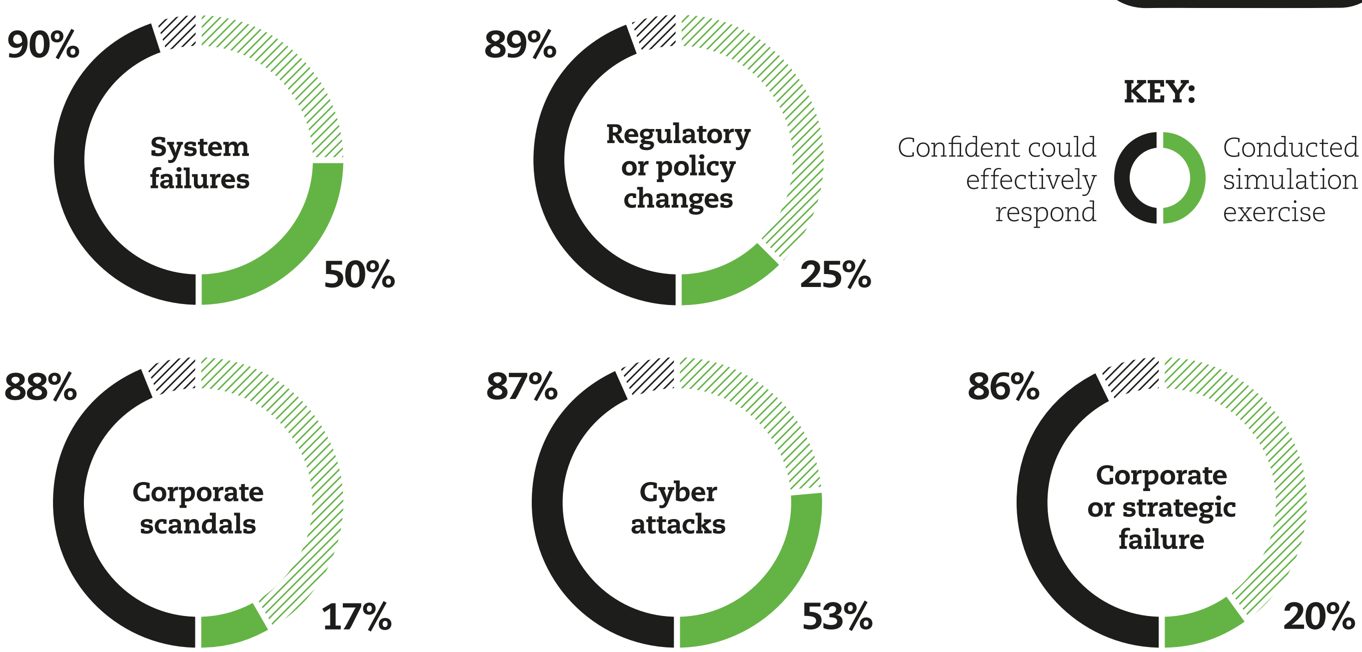


Skill and resource limitations

Source: State of cybersecurity 2018, part 2: threat landscape and defence techniques, ISACA

Confidence in crisis management systems untested?

While many organisations claim they are confident that their crisis management systems are robust, far fewer have tested them in reality



Source: Stronger, fitter, better: crisis management for the resilient enterprise, Deloitte

Banks and analysts disagree over Brexit impact

If the ongoing negotiations between the UK and EU end in disorder or inconclusively, do you expect material negative impacts to bank profitability?

71%
Banks say **NO**

52%
Analysts say **YES**

Source: Risk assessment questionnaire – summary of results July 2018, European Banking Authority

It's not about the manual

Risk managers need to develop their processes to suit the specific needs of their organisations, rather than allow standardised ways of working dictate their role, according to Paul Mather, Shell's group head of enterprise risk management

BY ARTHUR PIPER

In 2015, governments came together in Paris and achieved a landmark agreement to tackle climate change. The Paris Agreement's goal is to keep the rise in global average temperature this century to well below two degrees Celsius (2C) above pre-industrial levels and to pursue efforts to limit the temperature increase even further to 1.5C. In pursuit of this goal is a vision for the world to transition towards a net-zero emissions energy system.

"Shell aims to play a role in meeting these challenges by exploring solutions in areas of our technical expertise, such as natural gas production, efficient future fuels – for example, biofuels and hydrogen – and carbon capture and storage, and also in emerging energy system technologies," Paul Mather, Shell's group head of enterprise risk management (ERM), says. "We know our long-term success as a company depends on our ability to anticipate the types of energy that people will need in the future in a way that is both commercially competitive and environmentally sound. We find the goal of a better life with a healthy planet to be an inspiring ambition. But navigating the

> **To be effective in risk management, risk needs to be embedded in the mindsets and behaviours across the organisation**

necessary transitions will require extraordinary and unprecedented co-ordination, collaboration and leadership across all sectors of society. This includes risk management."

The Intergovernmental Panel on Climate Change indicated through energy scenario-based climate modelling in their Fifth Assessment Report (2013, 2014) that limiting the rise in global average surface temperature to 2C would require greenhouse gas emissions to reach net zero by around 2070. This needs to be achieved while recognising that the rising living standards of a growing population mean that energy demand could double over the course of the century.

Since no one can know how energy transition will work in reality, managing risk is going to continue to be a major priority for the sector. "Businesses like ours need to make sure there is an appropriate balance between short and medium-term strategic priorities, while ensuring that longer term there's a recognition that the energy system in the future will change. The business will need to negotiate the right balance between resilience and opportunity. In addition, it is important that the industry learns lessons from past cycles and that cost discipline is maintained in the future," says Mather.

Broad

Risk management has an important role to play – not just as a discipline, but as an approach to doing business. "Risk management is broad, it's what we do and ultimately it is what our industry does; managing risk versus cost versus value to drive the best economic performance," Mather says. "Consciously, or subconsciously, most of us take risks daily in some shape or form in any organisation. For me to be effective in risk management, risk needs to be embedded in the mindsets and behaviours across the organisation, across decision-makers and across people who take operational decisions on a day-to-day basis."

Mather says that people also need to understand that specific risks should not always be discussed in isolation particularly in an organisation the size of Shell.

There are no prizes for the size of a risk register; rather it needs to be focused and actionable with clear accountability. One of the key messages he is promoting in the business is to ensure that there is appropriate consideration given to balancing risk with cost and value: “When people think about risk, they may want to ask why they want to mitigate it or whether indeed to accept the risk and how much the mitigation would cost, for example.” Mather says that it is a mistake to think of value purely in terms of cash. There may be value, for instance, in protecting one’s licence to operate, or in behaving in a way that protects the organisation’s reputation.

Mather accepts that it is not an easy message to get across. Managers need to understand the value chain of their own organisations and how this fits in with the wider business. Shell has aimed to overcome this by promoting more of an explicit focus on risk appetite. Enabling a clearer and more transparent expression of the level of risk people are prepared to take can inform better decision taking because those decisions are grounded in a clearer articulation of controls, risks, assurance and of the associated value component. “It is different to the discussion that you would have at a bank, where risk appetite revolves more around issues such as capital requirements,” Mather says. “It’s about the discussion, and it’s about having that transparency, it’s having that challenge, it’s having that accountability and it’s having the ownership associated with that process.”

Another important focus for Mather is the link between risk management and strategy. “Research has shown that more than 80 per cent of the greatest losses in shareholder value for publicly listed companies in the last decade were attributable to ‘strategic blunders’. Organisations are therefore looking to strengthen the integration between strategy and ERM,” he says.

Pragmatic

Given Mather’s determination to make ERM relevant to the business and designed to promote intelligent and informed risk-based

> **Whatever organisation you work for, you need to understand the business and you need to understand the value chain, and then, and only then, can you start to think about providing meaningful advice and support as it relates to risk**

decision making at Shell, it should come as no surprise that he does not feel overly constrained by adhering to specific frameworks or methodologies. It is not that he does not find them useful, but he is cautious of risk methodologies becoming an end in themselves – rather than the means to an end.

An example of this approach can be seen in a recent project to refresh the organisation's approach to ERM. One area that changed was the promotion of three different risk appetite lenses ('Strategic', 'Operational' and 'Conduct'). Mather says that aligning some of the discussions, say between strategic and portfolio risk, with those that are more operational in nature, through those lenses can provide for a more transparent and purposeful discussion. Also, it should also be recognised that an organisation's principal risks are complex and have both a portfolio and operational dimension.

One question that has come up several times during 2018 from industry peers has been in respect of the recently issued COSO (Committee of Sponsoring Organizations of the Treadway Commission) 2017 ERM guidelines. Significant engagements by PricewaterhouseCoopers (PWC) across various industries helped shape the different components, but it should not be viewed as a manual, more as a relevant point of reference. It can be an idea to map across the different building blocks of an organisation's risk framework to the different components and principles of the COSO guidelines. In addition, one of the core elements behind the COSO ERM 2017 guidelines is to look to elevate the discussion of integrating strategy and risk.

Conduct

Culture has become a recent focal point for discussion not only because of the increased interest by regulators but also because internally organisations recognise that the wrong behaviours in extreme can have a significant material impact on shareholder value.

For instance, recent guidance issued by the UK's Financial Reporting Council (FRC) talks about there being an increased expectation that organisations have mechanisms in place to measure culture from a range of different sources and that, where appropriate, corrective action is taken. Measuring culture is challenging, Mather says, but there are quantifiable sources of information that many companies already capture, such as around people surveys. By bringing together information and collaboration between human resources, internal audit, compliance and risk you may start to build up a holistic picture of culture within an organisation.

The challenge is then to critically consider, discuss and propose for the different leading and lagging risk indicators that may be available, and where is an acceptable range for these to fall into, he adds. Also, social media tools can provide insights on sentiment and external perspectives, which can clearly have a risk dimension.

Career

Mather has been with Shell for 12 years. After graduating from the University of Newcastle with a PhD in chemical engineering in 1996, he started his career as a chartered accountant with the firm PWC and did a brief stint as finance director with the medical devices company Boston Scientific, before joining Shell in a finance position in London. In 2010, he took on the role of head of governance, risk and assurance within trading and supply, before moving into his current position in February 2015.

Mather says he enjoys the experience of seeing the breadth of risks that Shell is exposed to and having the opportunity to try to change and influence the risk management process in a targeted way. "It's the way we execute our strategy and it's how we make decisions on a day-to-day basis across a number of challenging environments. It's how we support the business and functions to think more critically in respect of risk versus cost versus value."

While he says that the term risk manager is still fit for purpose for the kind of work he does, he is keen to emphasise the shift that has occurred in the profession over the past ten years. This has

> **Risk managers need to be inquisitive and comfortable forming relationships with different levels in the organisation**

moved risk management out of the strict compliance space and over into a position of being a trusted advisor to support the organisation with a decision-making process that helps them think holistically about their choices.

Challenge

"A lot of people will do risk reporting, which is viewed in many organisations as a compliance type exercise," he says. "People should reflect on why that is and what they can do to change that. Risk reporting should not just be an outcome of risk management but can influence risk management decision making and approach in a positive way. To do this successfully you need to understand the business and you need to understand the value chain, and then, and only then, can you start to think about providing meaningful advice and support as it relates to risk."

Mather again returns to his worry that too many risk managers are constrained by the tools, techniques and processes that are designed to help them develop their role, rather than using them as a springboard to help them manage risk in a way that best suits their businesses. "It is clearly important for risk managers to have a process and some form of assessment and methodology," he explains, "but that process should not drive risk management's role, activity and remit."

Similarly, while technical knowledge can be crucial in some risk management roles, non-technical attributes are fundamental. "Risk managers need to be inquisitive and comfortable forming relationships with different levels in the organisation," he says. "I think they need to be prepared to challenge senior stakeholders in both decisions they make and in respect of questioning the status quo."

"I think smart automation is beneficial from an efficiency perspective and the data-driven insights that it can provide, as it relates to risk reporting and risk management. However, the potential danger is that you can dilute the level of challenge, discussion and inclusion of corporate memory and personal experience."

Mather's thoughtful and evolutionary approach to developing risk management at Shell should stand it in good stead for the unpredictable changes ahead in the energy sector. There is no roadmap for how those changes will impact the business, so why would there be a prewritten manual for how risk management should change to meet those challenges?

Paul Mather will be speaking at IRM's Ninth Annual Risk Leaders' Conference, November 15, 2018. Book now: https://www.theirm.org/events/risk-leaders-2018.aspx

> **Process should not drive risk management's role, activity and remit**

Spreading the word

A new regional interest group covering the Asia Pacific (APAC) region is aiming to bolster support for risk management professionals and IRM membership

BY JO POWELL

The Asia Pacific (APAC) region, which includes India, South East Asia, China, Japan, Australia and New Zealand, is one of the world's fastest growing, with a huge amount of growth and investment underway in all industries. Its burgeoning economies offer a great opportunity to implement good practice and pragmatic risk management. There is a growing appetite from risk professionals across the region to ensure risk management is effectively embedded into the organisations they are part of.

The APAC regional interest group (RIG) includes a number of IRM ambassadors, each with experience in the region, who will help bring more direct engagement with the institute into their countries. As active contributors to thought leadership in risk management, both in the context of the APAC region and within the IRM globally, they also liaise with IRM special interest groups (SIGs) and other partner organisations to maximise the support for the risk profession in the region.

Identifying the main risks in the region

In his contribution to the IRM's review of risks for 2018, Gareth Byatt, independent risk management

> Focused training and on-the-ground trainers can be of real value

Above: Gareth Byatt

> Many companies aren't taking the initiative on risk management

Below: Sonjai Kumar

consultant and IRM APAC ambassador, highlighted threats and also opportunities arising from technology and cyber risk, economic uncertainty, geopolitical uncertainty and instability, and the possibility of change to the regulatory environments of many countries in the region. Other regional ambassadors across APAC also highlight the risks of fraud, including internal fraud and embezzlement, as a significant issue.

Sonjai Kumar, an IRM ambassador to India and specialist in insurance risk, says that the RIG will provide focused training and on-the-ground trainers that can be of real value and will help with horizon scanning for any emerging risks and global events that may have local impacts.

"In India, enterprise risk management (ERM) is generally in a very early stage of development," says Kumar. "However, it is relatively developed in the banking sector and the insurance regulator issued corporate governance guidelines in 2016 to strengthen ERM.

"The application of ERM is slowly increasing, set against the challenges of the current risk culture including the levels of risk ownership within the first line of defence, acceptance of risk within an organisation, thinking of risks as impediments rather than enablers, the status of risk management within an organisation, and a very limited number of qualified risk professionals."

Kumar says that risk managers in the region need to have the confidence to talk about risk and its mitigations freely in their organisations and to encourage risk management education within their company. For example, he points to the IRM's new certification course on digital risk as being very pertinent to the local market, as good management of digital risk in the future will differentiate between success and failure for companies.

Risk management could be a risk in itself

Risk management across the region is highlighted as an issue in itself by Saman Bandara, IRM ambassador for Vietnam, Cambodia and Laos and an expert in insurance, forensics and IT risk.

In his home base of Vietnam, a huge amount of inward investment has led to high levels of competition between businesses, which he feels has resulted in too great a focus on top line growth. "Vietnam is becoming a major player in the global market through inward investment from developed areas such as Europe and the US, as it's a good area to get that first regional footprint in before expanding into other areas

Above: Saman Bandara

in the region," says Bandara.

"Competition is very high and top line growth is being given an undue emphasis as a key performance indicator. Companies are waiting to hear from regulators about risk management and many aren't voluntarily taking the initiative. They don't have proper risk management functions, or if they do, the people in them often aren't formally educated in the discipline."

Bandara says this is an area that needs immediate attention and that with its range of courses designed for everyone from new starters up to seasoned risk professionals, increased engagement with the IRM could bring many benefits to companies in this area.

However, he does acknowledge differences across the region.

"When you look across the APAC region there is a lot of variety – for example, Singapore is only an hour and a half away on a plane from Vietnam but when it comes to risk management there's a big difference between the two in terms of the guidelines and the levels of risk appetite," says Bandara.

"This makes it challenging for the new RIG as companies in different areas may all be talking about different things from different points of view and be facing different challenges."

Challenging and changing risk cultures

Abhishek Paul, an IRM ambassador for India and risk specialist in the financial services sector, says that the transition from a reactive to proactive risk culture is one of the biggest challenges today, combined with a general lack of awareness of the need for best practices in risk management. "I feel that there is a difference between what the role of risk managers is and what it should be, due to some fundamental gaps in the approach to understanding inherent and residual risk," says Paul.

"Risk management today in the majority of cases is reactive, which means it is very similar to an audit function, highlighting the gaps after a review of the risk and controls. However, the risk manager does not own the action that follows, with companies citing reasons of scope of roles and responsibilities between the first and the second lines of defence."

Paul feels that, in the region, external risks such as geographic conditions, natural disasters, environmental hazards, political unrest, social pressures and perception management can highly impact the sovereign risk aspect, which can either make or break the future of a booming economy. The addition of some major internal factors including money laundering, bribery, corruption and fraud, which contribute significantly to financial crime and conduct risk in the region, make it even more important for businesses to take a proactive approach to managing risks and building an organisation that does not need mandates and regulations to think about its sustainability in the future.

Paul is looking forward to supporting the RIG and spreading awareness of the benefits of risk qualifications, not only when starting a new career but also when professionals are considering whether their experience or qualifications need to be enhanced or even when implementing the best practices within their own business or function as a part of the first line of defence.

He says: "Through the RIG we will focus on knowledge building and will be sharing content through our web page that will be kept as simple as possible and easy to understand. We will also look at skill building through tie-ups with some of the national level institutes as a focal

> A focus on knowledge building, skill building and connecting people

Below: Abhishek Paul

TAKING THE IRM TO APAC

IRM directors Carolyn Williams and Sanjay Himatsingani visited Kuala Lumpur (Malaysia), Singapore and Hong Kong in August to raise the profile of the IRM, visit people interested in running IRM training and meet local members.

The pair also spoke at the Asia Risk and Resilience conference on 'Fit for the Future' and strengthened local relationships with the Hong Kong Federation of Insurers, the local risk association MARIM and the Risk and Insurance Management Association of Singapore (RIMAS).

"The IRM board predicts that the fastest growth for the Institute is likely to come from parts of the world where fast economic growth and rising infrastructure investment are combined with a commitment to achieving world class standards in training and competency and an understanding of British educational and business practices," said Carolyn.

"The APAC region (along with the Middle East and Africa) is likely to be a key growth area for the IRM and during this visit we saw encouraging recognition that IRM does set the international 'gold standard' for risk management education and training. The courses may be hard work, and they may be more expensive than lower quality competitors, but that's what makes them worth doing."

The IRM's first Fundamentals of Risk Management (FoRM) training course in Kuala Lumpur will take place in October and the first in Singapore will be delivered in November.

For more information about regional groups, email andrea.gale@theirm.org. Details of courses in the region are on the IRM website.

point for face-to-face sessions, and connecting people by bringing together risk professionals to share thoughts and opinions and discuss best practices on discussion boards."

Leveraging skills and experience already available

Gareth Byatt says that while there are certainly good risk institutes in different countries around the world, the IRM can provide broad international coverage which spans countries, while also linking into country institutes, and can really make a difference in regions like APAC.

"One of the things we intend to do is leverage the skills and expertise of different groups that already exist in the IRM. For example, in our first regional newsletter in June we included a focus on infrastructure in the APAC region, produced in collaboration with the IRM special interest group (SIG) for infrastructure risk," says Byatt. "We are also linking into other groups, such as the Innovation SIG. We want to tailor our communications for professionals within APAC by looking at three tiers of general global practice, moving down to a regional focus, and then highlighting country-specific news or issues."

Byatt says the RIG's role includes linking up with other institutes across the region. He says: "We are already talking to national institutes across the region and linking with organisations like the Business Continuity Institute and the Risk Management Institute of Australasia, to name just a few, making sure that there is a good quorum of people talking about and delivering good risk management, underpinned by things like the certification and training that the IRM already offers.

"We hope to increase the membership base in the region by showing people we are proactively informing them about good practices in risk management. We're not just sitting on our hands saying 'we're the IRM, come to us'. We want to be able to encourage people to join the IRM in the APAC region from all the countries in our geographic area by showing the added value that risk managers and organisations can gain from membership.

"It's about sharing examples of what's going on around the world, leveraging what's going on in the IRM and attracting new members to the IRM because it delivers a good service that adds value to organisations large and small."

Jo Powell is an assistant editor at *Enterprise Risk*. Find the APAC RIG web page at www.theirm.org/events/regional-groups/apac.aspx

Everybody gets to play

While defining the benefits of diverse organisations is difficult, it should not be an excuse to do nothing. Partnering with others is a good place to start

BY SARAH CHRISTMAN

Recent studies are strengthening the link between company performance and diversity. However, distinguishing between cause and correlation can be difficult. For example, the consultant McKinsey & Company wrote in an article called *Why diversity matters* that "companies in the bottom quartile for both gender and ethnicity/race were statistically less likely to achieve above average financial returns than the average companies in the dataset (that is, they were not just not leading, they were lagging)." What remains to be proven is whether diversity drives results of top-performing companies. It may be that top-performing companies are better at embracing diversity and maximising the benefits it brings.

An alternative to waiting for the link to be proven is to assume that performance and diversity have a shared root cause. Failing in either one may indicate that root cause exists within and affects your organisation. Duncan Wardley, PwC director and a subject-matter expert in behavioural and cultural change, proposes the approach of "aiming off," which entails setting and tracking targets that may relate only obliquely to their actual goals.

In a blog post with that title, he writes, "aiming off is a navigational strategy often used in orienteering or mountain walking where targets can be difficult to reach. Rather than taking a direct route to the target and potentially missing it, the walker heads to a line feature

> What remains to be proven is whether diversity drives results of top-performing companies

> With new levels of transparency and comparability come the threats of employee, customer and stakeholder backlash

near the target such as a stream or wall which helps to guide the way to the destination. This technique is safe, saves time and maximises the chances of you reaching your goal."

If top performance and greater diversity are linked, organisations can use the approach of "aiming off" with diversity as the target that relates obliquely to a goal of top performance. Achieving diversity and then sustaining and maximising its benefits could be the feature that leads you to your goal.

Organisations should establish diversity targets, develop a plan of action, monitor progress towards that target and adjust the plan as needed. Applying the tried and tested approach of Plan-Do-Study-Act to diversity with the same rigour as other critical objectives can shift your organisation towards the profile of a top-performing company. Of course, this doesn't guarantee high performance, but it can rule out one potential hindrance to success.

The gender pay gap

The gender pay gap reporting implemented in the UK this year is a timely example of the consequences of missing the target on diversity goals. Awareness that a pay gap exists is not new. The Organisation for Economic Co-operation and Development (OECD) has been publishing reports on the topic for more than a decade. What's new, however, are the consequences for allowing a pay gap to exist.

Regulations under the Equality Act 2010 require British employers with over 250 relevant employees to annually publish specified metrics on the pay gap between men and women. The results aren't surprising – in aggregate, men earn more than women, both by mean and median pay. Narratives published alongside the metrics offer explanations. Many point to higher numbers of women in junior low-paying roles and lower numbers of women in senior high-paying roles.

It's tempting to explain this disparity away, pointing to life choices made by women to study and take jobs in less lucrative fields or to take career breaks for family care. However, research published this year by Stanford University and Uber – *The gender earnings gap in the gig economy: evidence from over a million rideshare drivers* – shows a gender pay gap of 7 per cent exists for Uber drivers despite the gender-blind nature of the Uber platform and the workplace flexibility of the gig economy.

Previously, organisations could turn a blind eye to the issue. With new levels of transparency and comparability come the threats of employee, customer and stakeholder backlash. Organisations need to respond to these threats while maximising the opportunities from diversity.

From diversity to inclusion

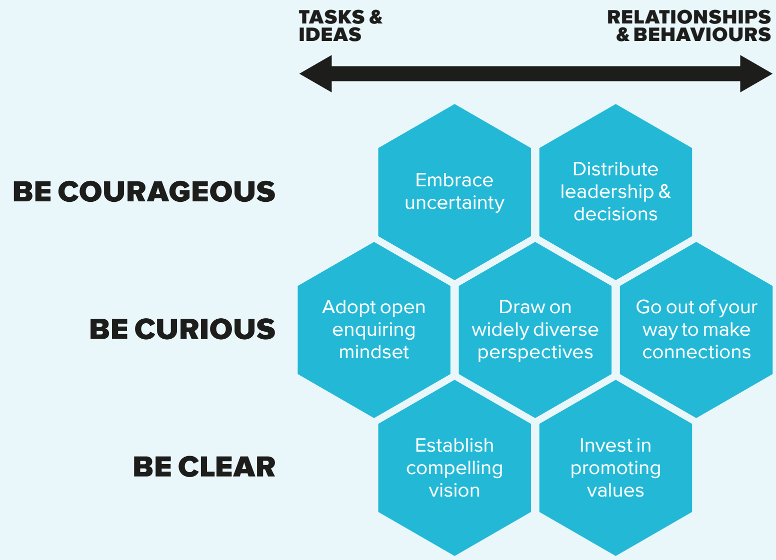
Diversity describes the differences in representation by headcount, or who is part of the organisation. Inclusion describes the actions taken to welcome, engage and benefit from diversity, or how people participate in the organisation.

Efforts to drive gender diversity in boards have been spreading globally. Scandinavian countries are leading the way with Norway having detailed legislation and severe penalties for non-compliance in place for over a decade.

A study published by the National Bureau of Economic Research – *Breaking the glass ceiling?* – into the effects of the Norwegian quotas, however, shows a disappointing outcome with respect to inclusion. Boards achieved the 40 per cent target for membership of the least represented gender without encountering many of the traditional objections such as lower-quality candidates or excessive stretch for those serving multiple boards. However, this hasn't translated to increased women in executive management or a decreased pay gap between genders below the board level, primary objectives of the legislation.

Although companies are achieving the representation at the top, they appear to be falling short on action required to benefit from full inclusion. The answer may lie in how the board interacts with the executive management and the wider organisation.

DESIRED CHARACTERISTICS FOR WHOLE SYSTEM LEADERSHIP



Source: *https://www.theirm.org/media/3814171/IRM-Extended-Enterprise-Resources-for-Practitioners-Full-Document.pdf*

> Risk practitioners can support leadership in being clear, curious and courageous to support diversity and inclusion through their actions and advocacy

Engaging the board

Leadership teams dealing with complex problems in complex organisations can't rely on codes, policies and procedures to make real change. IRM offers an alternative in their practitioners' guide *Extended enterprise: managing risk in complex 21st century organisations.*

Professors Welbourn and Fathers present a leadership model that raises questions about the behaviours of leaders as they face risks and decisions in complex organisations. They challenge leaders to consider their clarity, curiosity and courage.

How clear are your leaders? Have they created and communicated a compelling vision? Does that vision align to enduring values that the leadership continually reinforce?

How curious are your leaders? Do they continually seek new information and different perspectives from diverse sources? Do they use their unique position to connect ideas and people and help others to do so?

How courageous are your leaders? Do they go beyond accepting uncertainty and embrace it to get beyond superficial solutions? When uncertainty rises, do they empower frontline decision-makers to maximise speed and agility?

The risk practitioner's role

Risk practitioners can support leadership in being clear, curious and courageous to support diversity and inclusion through their actions and advocacy.

If the board does not sustain its commitment to diversity and inclusion and gives conflicting messages, people will respond accordingly. Your risk framework should provide reinforcement and accountability on diversity and inclusion goals, reflected in your risk appetite statements and risk reporting against objectives.

The board can't foster diversity if they don't invite and welcome a variety of messages and messengers. You should consider how you use your time with the board and executive management. Devote some of your risk agenda to guest speakers with diverse ideas and backgrounds to provide new views and connections for the leadership to draw upon when considering risks.

Make the board a beacon for diversity and inclusion. Advocate for increased visibility of board members and seek opportunities for them to explain their unique values, contribution and perspective. This encourages people to do the same. Q&A sessions can be a useful and time-effective way to engage. If your organisation is large or geographically dispersed, these can be held online.

For specific diversity risks, like large and persistent wage gaps, risk practitioners need to find the facts. The ability to undertake research, read regulations, gather information, identify the biases in that information and understand what it all means are key competencies.

In the case of wage gaps, find the facts about the gap in your organisation, your industry, your regions. There are factors widely acknowledged to contribute to the problem that you can investigate. Factors such as the language used in role profiles, the make-up of interview panels, the specificity of goals and the analysis of data against goals.

Addressing culture has to be part of the solution. Command and control approaches may reduce litigation, but don't offer sustainable solutions. Mentoring, job rotations and cross-training can increase contact between groups with positive effects for diversity and inclusion without needing to be built solely for diversity and inclusion programmes.

Risk practitioners need to share what they learn with internal business partners and leaders. The ability to communicate the facts and their implications in a way that helps inform and empower decision-makers will improve the decision quality.

How you share what you've learned internally will be unique to your organisation. Use numbers, pictures or narratives that will engage your audience. Address the question "so what?" Show how the facts and the remaining uncertainty relate to the organisation's objectives.

Ask the open and provocative questions that can change the lens others are looking through. Then ask the simple question, "what else?" Be the person that tolerates the awkward silence, and ask again. Throughout the conversation, remain focused on the end question – how can we succeed in our objectives?

Risk practitioners should also share what they learn externally. Systemic issues like wage gaps won't be sustainably solved within a single organisation. The IRM Regional and Special Interest Groups are useful forums for discussion.

A partnership approach

At Equifax, we're investing to continuously improve diversity and inclusion. Equifax was created to improve financial inclusion, outcomes and fairness for consumers and creditors. Our very name is derived from the word "equity". We have a diversity and inclusion vision, which states: "Together, we're going to make Equifax as diverse as the consumers and clients whose financial outcomes we work to improve. We will challenge the past and the present. We will be different and are striving for constant evolution."

We recognise that diversity and inclusion are complex problems with roots deep in society. We can't solve them entirely on our own, so we look for partners.

We have committed to the Women in Finance Charter (see box out), set up to deliver on recommendations from Jayne-Anne Gadhia, CEO of Virgin Money, in her review of representation of women in senior management in financial services.

This is a commitment by HM Treasury and signatory firms to work together to build a more balanced and fair industry. Signatories are pledging to be the best businesses in the sector. We agree that a hard day's work deserves a fair day's pay. For this reason, we are an accredited Living Wage employer, meaning everyone within our supply chain is paid the Living Wage by their employers.

Being an accredited Living Wage employer is about much more than what we pay our employees. It's about being a part of a community of employers and taking a stand for what is right in society.

By working in private–public partnerships and across industries we can address issues that prevent people from fulfilling their potential. As McKinsey found, less diverse companies lag on performance. Achieving diversity goals may become a competitive advantage for those that pursue them. However, organisations should still be willing to share ideas to accelerate change. Ultimately, we want a better world where we can all have the opportunity to excel. A world where we all get to play.

Sarah Christman (GradIRM) is risk director at the credit reference agency Equifax Ltd and technical director on the IRM Board of Directors.

WOMEN IN FINANCE CHARTER

The Charter reflects the government's aspiration to see gender balance at all levels across financial services firms. A balanced workforce is good for business – it is good for customers, for profitability and workplace culture, and is increasingly attractive for investors.

The Charter:

- commits firms to support the progression of women into senior roles in the financial services sector by focusing on the executive pipeline and mid-tier level;
- recognises the diversity of the sector and that firms will have different starting points – each firm should therefore set its own targets and implement the right strategy for their organisation;
- requires firms to publicly report on progress to deliver against these internal targets to support the transparency and accountability needed to drive change.

Download the Charter here: https://bit.ly/2ucJeUa

State-sponsored mayhem

Governments are increasingly using their investments in cyber initiatives to go on the offensive. Is it time to sue for peace?

BY ARTHUR PIPER

During the summer of 2018, a major cyberattack on Singapore's largest healthcare group netted the personal details of over one-and-a-half million patients, including the country's prime minister, Lee Hsien Loong. The data raid on SingHealth is the biggest yet in Singapore's history and could have been the result of a sophisticated and carefully planned state-sponsored sting, according to *The Telegraph* newspaper in the UK.

"It was not the work of casual hackers or criminal gangs," Singapore's Health Ministry told journalists. "The attackers specifically and repeatedly targeted prime minister Lee Hsien Loong's personal particulars and information on his outpatient dispensed medicines."

The attack is just one of many cybercrimes attributed to state-sponsored actors – a fancy name for hackers paid by a country's government to steal information or disrupt events and democratic elections. Just as the perpetrators of the so-called Olympic Destroyer virus – which shut down the website of the winter games in March – have not been traced, so the authors of the recent Singapore

"Cyber is increasingly political, with private sector companies being caught in the crossfire of internal and geopolitical activities

hack have slipped back into the invisible strands of the dark web.

Political crossfire

"Cyber is increasingly political, with private sector companies being caught in the crossfire of internal and geopolitical activities," say the authors of *Cyber risk outlook 2018* from the Centre for Risk Studies at the Judge Business School, University of Cambridge. "Data exfiltrations, server take-downs and destructive malware attacks on thousands of businesses are suspected as originating from external nation state cyber teams."

Such hacker groups have benefited from years of taxpayer investment in government defensive cyber capabilities. Now, though, many have gone on the offensive in ways that are almost impossible to detect, according to the cyber consultancy Venafi. And they are enjoying major returns on their investment in the form of increased data theft, security breaches and worse, Jing Xie, a senior threat intelligence analyst at the firm, has said.

"With every major nation-state expanding both offensive and defensive cyber war spending, public and private critical infrastructure and communication providers should expect to be caught in the crosshairs of cyber warfare," he told Global Insight magazine.

What is to be done?

Since the risk of state-sponsored cyberattacks is unlikely to be mitigated by private companies alone, some form of global peace pact seems to be in order. Microsoft's president, Brad Smith, has been calling for over a year for a Digital Geneva Convention to help contain today's situation. His convention would get its legal clout from six key principles (see *Digital Geneva Convention's Principles*) that aim to end the excesses of state-sponsored cyber conflict.

Speaking at the World Economic Forum's Davos event in Switzerland in January this year he said: "This is supposed to be a time of peace ... so the world has literally, in that regard, been turned upside down from protecting civilians in times of war to attacking civilians in times of peace."

Bold and fuzzy

The proposals are both bold in scope, but fuzzy in how they could work in practice. There have been previous initiatives to stem the rise of state-sponsored hacking. For example, 20 countries from a United Nations' group have proposed "limiting norms" in an attempt to curb online activity that could damage national critical infrastructure, or the use of cyber defence experts to go on the offensive. But the recent spate of high-profile hacks throws doubt on how well those norms are working in practice.

Smith's suggestion that "system vulnerabilities should be reported to vendors rather than stockpiled, sold or exploited" may represent the best way forward. It could open the door for the private sector to help governments and businesses combat cyberattacks without surrendering weapons to those who would exploit them.

That move does not necessarily need a Geneva-style peace convention for it to work – just co-operation between competing software vendors and potentially governments. Large technology companies have the clout, cash and knowledge to develop practical solutions in this area. And they are well positioned to define the scope and nature of cyberattacks and develop the weapons to defend against them. If the proliferation of state-sponsored cyberattacks is to be stemmed, urgent action is needed by those closest to the problem.

Arthur Piper is editor of *Enterprise Risk*

SIX PRINCIPLES OF A DIGITAL GENEVA DIGITAL CONVENTION

1. There should be no targeting of high-tech companies, the private sector or critical infrastructure.
2. The private sector should be assisted in its efforts to detect, contain, respond to and recover from cyberattacks.
3. System vulnerabilities should be reported to vendors rather than stockpiled, sold or exploited.
4. Restraint should be exercised in developing cyber weapons, and any that are developed should be limited, precise in their targeting focus and not reusable.
5. There should be no proliferation of cyber weapons.
6. Offensive operations should be limited to avoid mass and indiscriminate cyberattacks.

Source: *The proposed "Digital Geneva" Convention: towards an inclusive public-private agreement in cyberspace?*, Maria Gurova, Geneva Centre for Security Policy

Reframing risk

As the major revision of one of the world's most influential pieces of guidance on risk turns one year old, what does COSO ERM mean to the profession?

BY MARK BUTTERWORTH

Risk managers are increasingly under the spotlight in regard to the structure they bring to risk management in their organisations, and the credibility of their approach. In using a well-established code or framework the risk function can give management and other stakeholders the assurance they are seeking that risk is addressed in a coherent, formalised way. One year after the publication of updated guidance from the Committee of the Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise risk management – integrating with strategy and performance*, analysis can be undertaken of the value that this framework adds.

The previous 2004 guidance had a long and successful "shelf life", majoring on a three-dimensional "cube" that blends eight features of risk management (for example, event identification, risk assessment and controls) with key objectives and looks at these from the entity level, division and subsidiary perspectives. The emphasis on the integrated framework has now evolved to become a management tool that addresses the critical issues of strategy and performance – seeking to enhance the chances of success and resilience in the face of increasing complexity in the risk universe.

> **By taking an 'audit' of the organisation's actual compliance with each of the COSO principles, a picture can be formed of the strengths and weaknesses of the current risk management approach**

> By demonstrating how risk management forms part of good governance and direction, the risk function sits firmly at the forefront of organisational management

New, helpful features

Other than for expert users, applying the COSO cube could be a daunting experience and lead to confusion and lack of focus for many risk managers and their organisations. There is no doubt that taking an enterprise-wide approach to addressing risk makes sense, and the 2004 guidance set many risk managers along this righteous path. The 2017 revised framework has an easy-to-follow and logical structure of five interrelated components – and each has explanatory principles, twenty in total.

The components make sense if your aim is to blend risk management seamlessly into strategy design and selection and performance monitoring. The COSO "double helix" as shown below weaves together the framework's components, ultimately flowing through to producing enhanced value for the organisation.

The list of 20 principles can be used by risk managers as a checklist of risk management maturity – indeed Principle 17 ("*pursues improvement in enterprise risk management*") is itself a call to develop further the organisation's risk management capabilities. By taking an "audit" of the organisation's actual compliance with each of the principles, a picture can be formed of the strengths and weaknesses of the current approach. A number of the principles may be partly addressed, and so I recommend that a scoring system is applied (red, amber, green, for example) from which priorities for action can be developed. The action plan, required resources and time frames should be agreed with senior management.

Culture

The importance of active culture management is gaining greater traction, not least following the publication by the Institute of Risk Management of its thought leadership guide: *Risk culture – resources for practitioners*. In COSO 2017 the principles require organisations to embed culture management within their governance practices. This is achieved by linking board risk oversight and support of executive management with commitment to core values and is manifested by defining and monitoring the behaviours that characterise the desired culture.

But measuring progress on risk culture management is not easy. Risk managers should spend time with colleagues to define the appropriate culture metrics, which indicate

ENTERPRISE RISK MANAGEMENT

Governance and culture
Governance sets the organisation's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding of risk in the entity.

Strategy and objective-setting
Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

Performance
Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

Review and revision
By reviewing entity performance, an organisation can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

Information, communication, and reporting
Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organisation.

> "COSO proposes that enterprise risk management needs to employ techniques such as visualisation of potential outcomes that detailed data modelling can give to organisations

improvements in risk awareness, positive behaviours and risk management coherence. While some existing performance data will be helpful in judging the culture, such as employee absence rates, customer complaints and product quality, risk managers should expand the metrics to include culture monitors such as an analysis of employee satisfaction surveys, sign-up numbers for training programmes, media commentary analysis – positive and negative, employee involvement in corporate initiatives such as charitable time-giving, disciplinary factors and timeliness in risk and event reporting.

Analyses of reasons why firms fail often cite poor culture as a key factor. Setting a plausible strategy and monitoring performance could be undermined if culture metrics are inappropriate or even ignored.

Challenges

As with all aspects of risk management, gaining tangible senior management buy-in is crucial. Nothing new there, so how is the COSO framework going to help risk executives achieve the partnership approach to risk? Certainly a thorough and effective communication (and if necessary, training) programme is required as a platform for shared knowledge, but COSO really requires a redefinition of the risk function.

Given the emphasis on strategy and performance in the framework, the risk executives need to be involved in the essential initial phase – strategy setting, or what COSO calls strategy selection. This is not easy – conceptualising and developing strategy is often held close to the chests of the main board or senior managers. The challenge for risk managers is to show how effective risk analysis can lead to better decision making. Assisting senior executives with scenario analyses and modelling of potential outcomes to the strategic options that the board are considering gives much greater assurance that the selected strategy is achievable, with acceptable potential downside.

The COSO focus is on getting the best from upside risk. Certainly good risk management practices identify and address the negative aspects of risk, but real organisational value comes from a mindset of gaining a thorough understanding of the risks associated with the selected strategy. Risk managers will seek to reduce volatility in outcomes by moderating the effects of risks that do occur.

Many commentators observe that risk managers' influence at board level should be developed further. The focus of COSO 2017 on strategy and performance gives clear positioning of risk management in regard to the essential focus of the board, that of building a sustainable, resilient strategy and proactively measuring performance. Directors have an inherent interest in understanding the status of risks that could influence performance and how well these risks are being controlled. By demonstrating how risk management forms part of good governance and direction, the risk function sits firmly at the forefront of organisational management. COSO adds that going forward, intelligent use of the framework will bring identifiable financial benefits that more than offset the cost of risk management activities, again affirming the enhancement of value by the risk function.

International relevance

While COSO is strongly US oriented, it is equally relevant to all types of organisations, across all geographies. It is also a practical framework for uniting risk management approaches throughout a divisionalised organisation. Indeed, the COSO publication

COMPONENTS AND PRINCIPLES

1. **Exercises board risk oversight** – The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes operating structures** – The organisation establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines desired culture** – The organisation defines the desired behaviors that characterise the entity's desired culture.
4. **Demonstrates commitment to core values** – The organisation demonstrates a commitment to the entity's core values.
5. **Attracts, develops, and retains capable individuals** – The organisation is committed to building human capital in alignment with the strategy and business objectives.
6. **Analyses business context** – The organisation considers potential effects of business context on risk profile.
7. **Defines risk appetite** – The organisation defines risk appetite in the context of creating, preserving, and realising value.
8. **Evaluates alternative strategies** – The organisation evaluates alternative strategies and potential impact on risk profile.
9. **Formulates business objectives** – The organisation considers risk while establishing the business objectives at various levels that align and support strategy.
10. **Identifies risk** – The organisation identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses severity of risk** – The organisation assesses the severity of risk.
12. **Prioritises risks** – The organisation prioritises risks as a basis for selecting responses to risks.
13. **Implements risk responses** – The organisation identifies and selects risk responses.
14. **Develops portfolio view** – The organisation develops and evaluates a portfolio view of risk.
15. **Assesses substantial change** – The organisation identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews risk and performance** – The organisation reviews entity performance and considers risk.
17. **Pursues improvement in enterprise risk management** – The organisation pursues improvement of enterprise risk management.
18. **Leverages information systems** – The organisation leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates risk information** – The organisation uses communication channels to support enterprise risk management.
20. **Reports on risk, culture, and performance** – The organisation reports on risk, culture, and performance at multiple levels and across the entity.

Source: *Enterprise risk management – integrating with strategy and performance, COSO, June 2017*

> It is essential that the risk function agrees the nature of reporting with senior management so that causes of diversion from the strategy, mission, vision and values can be acted upon without delay

cites entity-wide identification and management of risk as a key benefit of applying the framework. This of course requires a risk policy that adopts a hybrid approach consisting of a single centralised reporting framework, applied in a flexible and dynamic fashion within divisions and subsidiaries.

Many organisations adopt elements of the IRM risk management framework or the ISO31000 risk management guidelines, so what does COSO add? The answer lies in the positioning of the COSO approach firmly in the strategy space, aligning the selected strategy with the organisation's mission, vision and core values. Risk managers would benefit from adopting the strategic concepts in COSO, with operational aspects of risk management based on or derived from the IRM or ISO31000 processes. It's about selecting the most beneficial aspects of these frameworks and using the terminology and processes effectively.

Risk reporting

One of the constant challenges to the risk function is managing the flow of information from operational teams through to decision makers. Assessment of the implications of the chosen strategy, ie monitoring the known and emerging risks, is a key management tool. Thought should be given to the nature and timing of reporting – linked to the perceived volatility of the relevant risks. For example, for a holiday tour firm, the status of security in the countries visited would be assessed on a daily basis, whereas staff turnover statistics may be subject to monthly reporting. The importance of timely risk information cannot be over-stressed – management response relies on a dynamic reporting regime.

COSO 2017 notes that "*the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision, and the implications from the strategy*". It is therefore essential that the risk function agrees the nature of reporting with senior management so that causes of diversion from the strategy, mission, vision and values can be acted upon without delay.

Forward looking

The updated COSO framework has been around a year, and during that time we have seen widespread discussion on the benefits, and dangers, of data analytics. COSO proposes that enterprise risk management needs to employ techniques such as visualisation of potential outcomes that detailed data modelling can give to organisations. Further, COSO emphasises the benefits of leveraging artificial intelligence in identifying previously unrecognised relationships. Modelling the relationships and risks such as in the supply chain will provide increased resilience to interruptions.

For many risk managers this advancement in their role could represent a skill they don't have. Recruitment into risk teams could in the future focus much more on analytics and modelling proficiency.

Enterprise risk management will need to be agile and adaptable to be able to reflect the changing risk environment. If the strategy for an organisation is dynamic, responding to the fast pace of change, then risk management must be fully integrated with this process and inform the decisions driving the strategy.

Mark Butterworth is managing director at the governance and risk consultancy Condie http://condierisk.co.uk

Image credit: mmuenzl / Shutterstock.com

Common causes

Specific problems in some regional infrastructure projects point to common challenges for the effective management of such risks

BY DARREN MULLEN

The Institute of Risk Management's Infrastructure Risk Special Interest Group (SIG) recently held a webinar, during which presenters from the Kingdom of Saudi Arabia (KSA) and Australia outlined some of the current infrastructure project risk management challenges being faced in these regions.

While every global region and infrastructure domain will always have its specific characteristics,

> **There has been a mixed track record of delivery within Saudi Arabia with project delays, cost overruns, a poor safety record and inconsistent build quality**

the webinar highlighted common challenges which we all face as risk professionals – developing and introducing a risk management framework, and contingency management and risk allocation.

Methodology

KSA, as acknowledged by the G20's Global Infrastructure Hub, lags behind many other nations when it comes to successfully delivering infrastructure projects. This has resulted in a mixed track record of delivery within Saudi Arabia with project delays, cost overruns, a poor safety record and inconsistent build quality.

With a current portfolio of infrastructure projects valued at over £100 billion, many of which support KSA's 2030 vision of delivering economic and social benefits, the Kingdom established a new organisation called Mashroat. Mashroat's mandate is to develop and implement a new project management methodology, with risk management as one of its explicit disciplines. The body initially identified six core root causes of poor project delivery (see, *Key focus areas for reform of project delivery within Saudi Arabia*. Its new methodology is made up of 16 volumes to tackle these root causes, which are being implemented across three key phases.

The first is alignment. This looks to deploy international best practice procedures and processes across the full project life cycle, in particular focusing on the project planning and commissioning phases. The second is enablement. This seeks to develop inherent project delivery capability and capacity across the Saudi Arabian government and project delivery entities. Finally, a support and evaluation strand aims to introduce transparency and accountability by, for instance, providing project stage gate reviews and project performance reporting.

Tackling root causes

Many aspects of both the methodology itself and the three-phase approach to implementation, are specifically designed to tackle the previously identified root causes of poor project delivery. These can be seen in the right-hand column of *Key focus areas for reform of project delivery within Saudi Arabia*. The Saudi Customs Authority has been the first government entity to adopt the new methodology.

However, despite the work of Mashroat being specifically focused on infrastructure delivery within KSA, some of the challenges it identifies are common across all infrastructure projects. As risk professionals, there are two main aspects that we should consider.

At the start of a new project, and/or if current project delivery is weak, risk managers should consider the list of focus areas identified by Mashroat in its key focus areas as potential issues that could give rise to project delivery risk and consider how best to tackle them. Where such project delivery risks are identified, risk management's proposed response should consider a phased implementation approach similar to Mashroat's align, enable and support model.

> **"Where project delivery risks are identified, risk management's proposed response should consider a phased implementation approach**

Risk Allocation and Contingency Management

Since 2001, Australia's poor delivery of transport infrastructure projects has resulted in cost overruns of $28 billion, which equates to about a quarter of these projects' value, according to a Grattan Institute report, *Cost of overruns in transport infrastructure*. A key recommendation is to achieve better clarity in risk management. "The Commonwealth should provide model guidelines, which states and territories may adopt or adapt, that recommend a consistent approach to measuring and managing project risk, including a statement of seniority where specific guidelines would otherwise conflict with one another," it says.

Furthermore, this poor delivery is taking place within a wider global context of the cost of contractual disputes in infrastructure projects trending upwards, and an estimated quarter of joint ventures ending in contractual dispute. A recent report by the design and consultancy business Arcadis found that the global average value of disputes amounted to $43.4 million, with the time it takes to resolve them increasing slightly to almost 15 months (*Global construction disputes report, 2018*). Among its top three findings was the insight that "avoidance approaches and assessing risks continue to be a best practice."

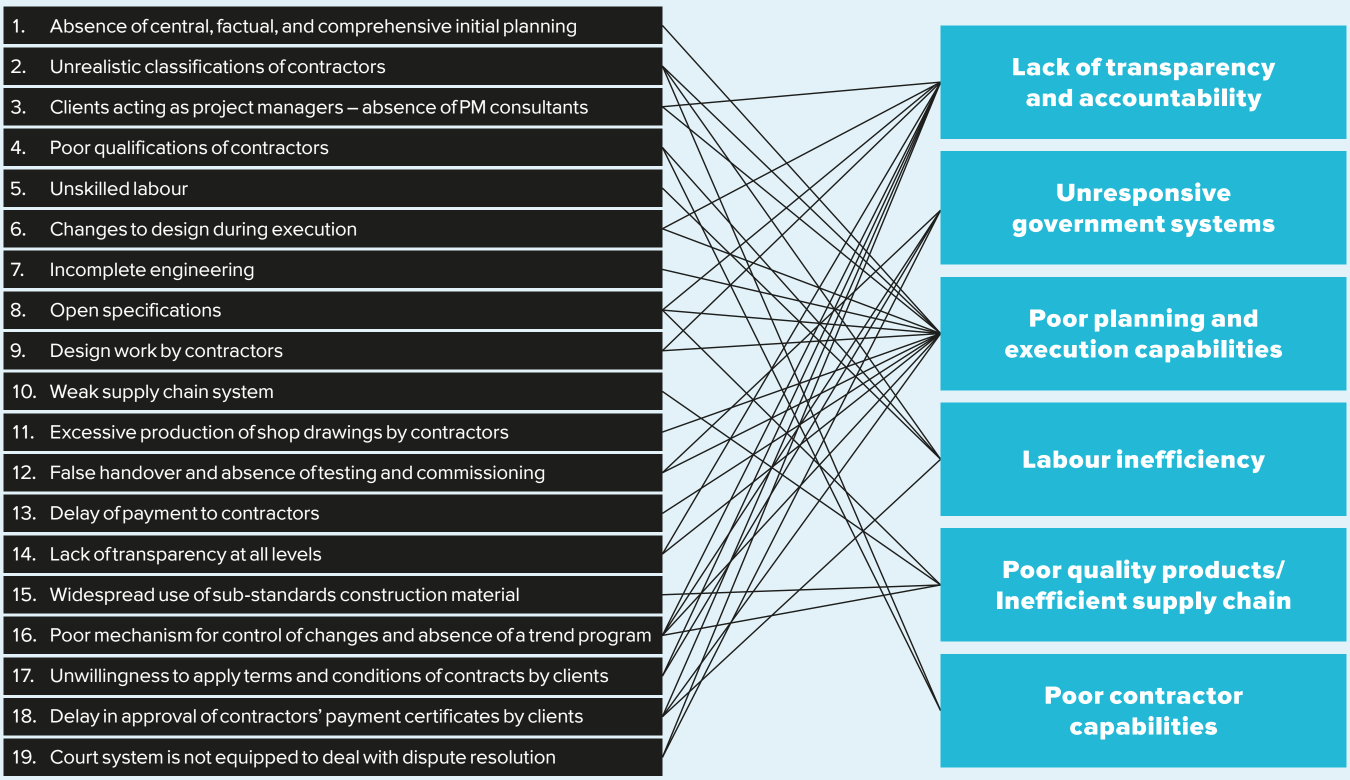
The Risk Engineering Society (RES) of Australia have identified two potential drivers behind this trend – the unreasonable allocation, or transfer, of risk, and the ineffective calculation of contingency.

Disputes

The first point is highlighted by the ongoing dispute between the New South Wales (NSW) government, who are the client for the Sydney light rail project, and Acciona who are a subcontractor to the main ALTRAC consortium delivering the project. The interesting point with this case, according to local news outlet ABC, is that Acciona is apparently suing the client, even though its only contractual relationship is with the main ALTRAC consortium.

Acciona's argument is reported to be that the client had allegedly not been clear about the number of utility pipes and cables that would need to be moved or the complexity of the work in the lead-up to signing the contracts. In turn, the NSW government is arguing that its contractual relationship is with ALTRAC, not Acciona, and that this risk had effectively been transferred to, and accepted by, ALTRAC. Whatever the actual facts of the case turn out to be, the dispute shows that there

KEY FOCUS AREAS FOR REFORM OF PROJECT DELIVERY WITHIN SAUDI ARABIA



has been a lack of clarity about risk transfer at some stage in the process.

The second point regarding contingency calculation is a key theme for technical guidance issued by RES (RES contingency guideline – first edition), which emphasises the need to make sure any contingency calculations adopt a probabilistic, rather than deterministic, approach – especially where the risk (for instance rainfall) can have a broad range of impacts. It also stresses the need for risk managers to consider secondary impacts, such as the cost and schedule impact of any necessary clean-up activities.

As such, even where the client is satisfied that the risk allocation is appropriate, the client also has a responsibility to make sure that the level of relevant risk contingency is also appropriate. Again, lessons from an Australia-specific context highlight common themes which we, as risk professionals, should consider.

While every project will have its specific characteristics, often driven by their regional and infrastructure domain, the recent IRM webinar has highlighted that many of the challenges that risk professionals face are common and transferable. As a result, we should broaden our horizons when looking for lessons to transfer and learn from when it comes to helping our projects improve their performance.

The IRM's Infrastructure Risk Special Interest Group's overarching aim is to help improve project performance within the infrastructure domain, both in the UK and internationally, by helping to improve the application of risk management thinking and practices. Darren Mullan is chair of the group and, at the time of writing this article, was a freelance risk manager supporting the King Abdulaziz Public Transport Project in the KSA.

> The global average value of disputes amounted to $43.4 million, with the time it takes to resolve them increasing slightly to almost 15 months

Due diligence solutions

Minimise risk by maximising the data that supports your most critical business decisions. LexisNexis is a leading provider of aggregated global content and powerful business intelligence tools. Protect your organisation from the risk of heavy fines and damage to corporate reputation by accessing the information you need on people, companies and countries. Our cost effective and flexible product modules include: PEP, sanctions, watch list and negative news screening. Enhanced due diligence and reporting. Proactive supply-chain and third-party risk media monitoring. Outsourced due diligence, compliance and risk advisory. Content integration and data feeds (APIs) into proprietary systems.

Rebecca Gillingham
+44 (0) 20 7400 2809
bis@lexisnexis.co.uk
bis.lexisnexis.co.uk
LexisNexis
30 Farringdon Street
London
EC4A 4HH

Risk and audit management software solutions

Symbiant are one of the world's leading providers of Risk and Audit management software. The solution is designed for collaboration and comes as a complete suite which can be separated in to Audit or Risk sets. Symbiant is designed for non Risk / Audit specialists to use, simple and intuitive but with a lot of back end flexibility and automated functions. CIO magazine have rated Symbiant as one of the top 20 risk solutions in the World. They have off the shelf or custom solutions to fit all budgets and requirements. Install on your own infrastructure or SaaS. 30 day free trial.

Andrew Birch
+44 (0) 113 314 3339
irm@symbiant.co.uk
www.symbiant.co.uk
Symbiant
1 Whitehall Quay
Leeds, LS1 4HR
United Kingdom

Risk management software

4C Strategies is one of the world's leading providers of risk management solutions. Combining expertise with an innovative approach, our advisory services and software solutions help organisations to build, verify and track the Readiness capabilities they need to deliver on their strategic and operational objectives. Our Exonaut™ software delivers a platform from which organisations can identify and assess risk, implement mitigation strategies, record validation activities, track real-time performance and respond dynamically to major incidents. The Exonaut™ suite of integrated modules is supported by an enterprise-wide mobile app, which enables staff to log and access critical risk data, wherever they are in the world, to support risk-informed decision-making and performance optimisation.

Peter Munksgaard
+44 (0) 203 318 2706
peter.munksgaard@4cstrategies.com
www.4cstrategies.com
13-14 Buckingham Street
London
WC2N 6DF

Risk management software

AgenaRisk is a model design and execution environment for Bayesian Networks, designed for organisations that need to assess and manage risks in areas where there is little or no data, where direct measurement is not possible, and in the face of new, often novel, circumstances. Organisations use AgenaRisk to model a variety of problems including operational risk, actuarial analysis, intelligence analysis risk, systems safety and reliability, health risk, cyber-security risk and strategic financial planning. Models developed in AgenaRisk can be integrated into a wider service using AgenaRisk Developer and ultimately deployed using AgenaRisk Enterprise.

Ed Tranham
+44 (0) 1223 263880
sales@agenarisk.com
www.agenarisk.com
11 Main Street
Caldecote
Cambridge
CB23 7NU

Risk management software

ALYNE – is an industry leading and award-winning, Regulation Technology Software company – that makes it easy for organisations to reduce the cost – of managing risk and compliance obligations and is built by industry experts. ALYNE – is a next generation, cloud solution that makes risk and compliance management as easy as browsing social media. ALYNE – with its unique pre-built library of controls, integrated risks and assessment templates – mapped to regulations and standards, is ready to use out of the box – with dynamic reporting and real-time risk insights. ALYNE's – innovative approach – enables organisations to make the right executive decisions and outcomes – and to drive business advantage.

Pierre Silavant
+44 (0) 7767 444 755
pierre.silavant@alyne.com
www.alyne.com
41 Luke Street
Shoreditch
London
EC2A 4DP, UK

Risk management software

The Protecht Group is a leader in Enterprise Risk Management Software and Services that enables organisations to achieve their strategic objectives through efficient, effective and agile Risk Management. Protecht. ERM™, Protecht's flagship product, has been deployed in a SaaS model since development commenced in 2002 and remains ahead of the curve on innovation and functionality. Used by government agencies, regulators, commercial and not-for-profit organisations of all sizes and risk maturity, Protecht. ERM™ allows companies to seamlessly integrate risk management into their day-to-day activities and gain operating efficiencies through its flexible web-based forms, workflow engine and highly adaptable reports and dashboards. Protecht is more than a software company, we guide you through your risk management journey.

Keith Davies
+44 (0) 7828 163 802
keith.davies@protechtgroup.com
www.protechtgroup.com
131 Finsbury Pavement
London
EC2A 1NT
United Kingdom

Influencing the influencers

Celebrities and popular online personalities have been using their status to subtly promote products on the internet. Now the regulators are stepping in

Image credit: PixieMe / Shutterstock.com

> Your material connection to that company should be clearly and conspicuously disclosed in your endorsements

Last September, the US Federal Trade Commission (FTC) successfully acted against two online influencers – people who often use their status on the internet to persuade others to buy products or services.

The Commission found that Trevor Martin and Thomas Cassell – known on their YouTube channels as TmarTn and Syndicate – "deceptively endorsed the online gambling site CSGO Lotto without disclosing that they owned the company." In brief, the two influencers owned a business that acted as a gambling site where punters could play with their "skins" – collectibles from the online shoot-em-up game Counter-Strike: Global Offensive (CS:GO).

They allegedly created videos and other online content directing people to their own lottery site without telling people they had a commercial interest in it.

For instance, the FTC said that "Cassell promoted CSGO Lotto … posting videos that were viewed more than five million times. In addition, he tweeted "Bruh.. i've won like $8,000 worth of CS:GO Skins today on @CSGOLotto. I cannot even believe it!" Getting with the online patois, the FTC continued: "Well, Bruhs, while we're on the subject of things we cannot even believe, did either of you like consider clearly disclosing that you like owned the company – a material connection requiring disclosure under FTC law?"

Most importantly, the FTC claimed that their videos and social media posts – and the videos and posts of the influencers they hired – were dressed up to reflect the independent opinions of impartial users. The two were reprimanded in November 2017 and warned that if they infringed these laws again, they would be fined over $40,000 per infraction.

The FTC has written to other influencers warning them that "your material connection to that company should be clearly and conspicuously disclosed in your endorsements." In the UK, the Competition and Markets Authority (CMA) has also woken up to those influencers who are thought to be blurring the boundary between genuine endorsement and using their celebrity to push brands without declaring a commercial relationship.

George Lusty, the CMA's senior director for consumer protection, told the industry magazine *Marketing Week*, "If people see clothes, cosmetics, a car, or a holiday being plugged by someone they admire, they might be swayed into buying it. So, it's really important they are clearly told whether a celebrity is promoting a product because they have bought it themselves, or because they have been paid or thanked in some way by the brand."

The problems regulators face in enforcing this kind of honesty are all too familiar for those who follow internet law. First, the practices of influencers are likely to change at a much more rapid rate than the regulators can track. Second, the global nature of the internet makes enforcement difficult because the laws prevalent in one jurisdiction may not exist in another. Finally, tracking the volume of content created would require the application of sophisticated artificial intelligence algorithms to sites such as Twitter, Instagram, Facebook and many more – something the CMA is planning to do, but which will be hard in practice.

Businesses are beginning to wake up to the potential reputational damage that having the wrong kinds of friends can bring. Unilever's chief marketing officer Keith Weed, for instance, has reportedly said he will no longer work with influencers that buy followers – a common practice. To purloin an old adage, it could be time for businesses to keep their friends close and their influencers closer.