Enterprise Risk

Risk Academy: building a career in risk / **Culture special report:** getting to grips with ambiguity / **Coming into the light:** the EU's transparency gambits / **Aiming for the pinnacle:** challenges of ISO 31000

Moral Imperatives: Jacinta Whyte on Ecclesiastical's ethical approach to risk management

NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

FIND OUT MORE AT zurich.com/my-zurich

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.

ZURICH®

Editorial

The trouble with culture

I was talking to a senior figure in the internal audit profession recently and he expressed some doubt whether many financial services businesses were resilient to failure. True, they have increased the capital they hold, put in bigger and better risk and internal controls teams, and have closer contact with regulators.

Those systems have certainly improved the way those organisations manage risk. But if there are devious or lazy people who circumvent, or don't follow, controls procedures, they are back to square one. "That's why," he said, "it's your culture that's the best risk management system there is." People have to care enough to act upon what they notice when things go wrong.

What do risk managers and internal auditors know about culture? How many have training in anthropology, psychology and sociology? And are there systems in place to capture cultural metrics?

> " **Trying to impose risk culture from the top can serve to put responsibility for preventing accidents into the hands of those at the bottom of the organisation with the least power to prevent it**

I invited professor of sociology at MIT Susan Silbey to share some thoughts with us – you'll find her article on pages 18-22. She looks at the issue through the lens of safety culture. Nobody was talking about risk culture before 1980, she says, but now it's a major topic. She believes that this has occurred because of major technological catastrophes and risk management has been an empirically-oriented response to those incidents. The thinking seems to be, if you can measure what goes wrong, you can prevent it.

She gives short shrift to this approach. History has proved it to be wrong. It tends to miss those aspects of disaster that are hard to pin down precisely because they can't be quantified. In addition, trying to impose risk culture from the top can serve to put responsibility for preventing accidents into the hands of those at the bottom of the organisation with the least power to prevent it.

Alex Hindson has kindly volunteered to offer his own thoughts on how risk managers can get to grips with these issues on pages 24-27.

But it seems to me that the financial regulators are asking risk managers to do the impossible. If culture is not as quantifiable as it has been assumed, how can it be managed? And who has the professional qualifications to do so? Are the regulators laying down yet another faulty model in the history of failed attempts to manage catastrophe?

Arthur Piper
Editor

Contents

10

14

18

24

28

32

REGULARS

FEATURES

Gut feelings about Europe

One of the biggest decisions the people of the UK have had to make has also been the one where all the facts are unknowable. Sometimes following your instincts can be a valid reaction, says Ian Livsey

On 23 June 2016 UK citizens vote on whether the UK should remain part of the European Union. By the time you read this, you may even know what they have decided. IRM's members located in the UK and in the EU countries will have taken a close interest not only in the outcome, but also in the process. And I think that all our members would observe with interest because it has provided us with a great case study in risk assessment and decision-making under conditions of extreme uncertainty.

Politicians on both sides in the UK – and some outside as well – have spent the past months warning the British public about the terrible dangers of voting "the wrong way". Every day we saw intelligent, respected people in the media offering their view on the risks of one option, often countered immediately by equally intelligent and respected people arguing passionately in the opposite direction. Faced with a big decision, most engaged individuals attempt to do some sort of rational weighing up of the pros and cons of the various arguments. Some of us in risk management take this further and develop sophisticated mathematical models and scenario analyses representing various possible futures.

But, particularly from the point of view of the undecided voter, it became apparent that when the range of possible outcomes was so great, and so uncertain, you could never reach a position where you would be in possession of "the full facts".

We also saw, and probably experienced personally, the full range of cognitive biases in action. These ranged from the confirmation bias, which means that we are tempted to listen only to information that confirms our existing preconceptions, to the recency bias, which means that we give more prominence to the last thing we heard. Some of the analysis we have seen also recalled IRM's 2012 work on risk culture which explored personal pre-disposition to risk. This may help explain why some people found the idea of a future outside the EU terrifying, when others found it exhilarating.

> **Human beings have developed hard-wired cognitive shortcuts over millions of years because exhaustive calculations were impossible for our early ancestors who were just one step ahead of predators**

It's also interesting to recall the work of IRM Honorary Fellow Professor Gerd Gigerenzer from the Max Planck Institute in Berlin, who has spoken to IRM audiences on several occasions. In his book *Gut feelings* Professor Gigerenzer argues a case for paying more attention to our intuition. This is on the basis that human beings have developed hard-wired cognitive shortcuts over millions of years because exhaustive calculations were impossible for our early ancestors who were just one step ahead of predators.

We are humans not computers and we care about unquantifiable things like freedom, happiness and fairness as well as respecting the tools of logic and rationality. Whichever way the UK is heading, we can be sure that there will be a role for risk professionals in helping organisations make sense of uncertain futures. ⒾⓇ

Trending

Budgets have been tight during the past few years as the economic squeeze in many parts of the world continues. But many risk management departments are beginning to see more investment and support for their work

Investment in risk grows

About half the organisations responding to a recent survey are investing in their risk departments – one in five of those because they perceive its intrinsic value

Firms having a Corporate Unit that is primarily responsible for Risk Management:

74%

In the next 12 months firms anticipate the size of their Risk Management unit to:

INCREASE **40%**

STAY THE SAME **60%**

DECREASE **4%**

50%

Firms have increased their risk management support and focus over the last year

WHY?

EXTERNAL FACTORS **60%**

37% INTERNAL FACTORS

WHY?

20%

Recognition of risk management as a tool for growth

Source: The OHIO State University – The Risk Institute Second Annual Survey on Integrated Risk Management Age

What are the biggest challenges of the past year by sector?

37%

of natural resource companies say **new value creation**

35%

of financial services companies say **risk mitigation**

28%

of manufacturing companies say **cost management**

Source: BDO Global Risk Landscape report 2016

Supply chain resilience rankings of top five economies

How resilient are the supply chains of the top five economies against key risks?
FM Global's index assesses how the risks inherent in certain countries compare

USA **CHINA** **JAPAN** **GERMANY** **UK**
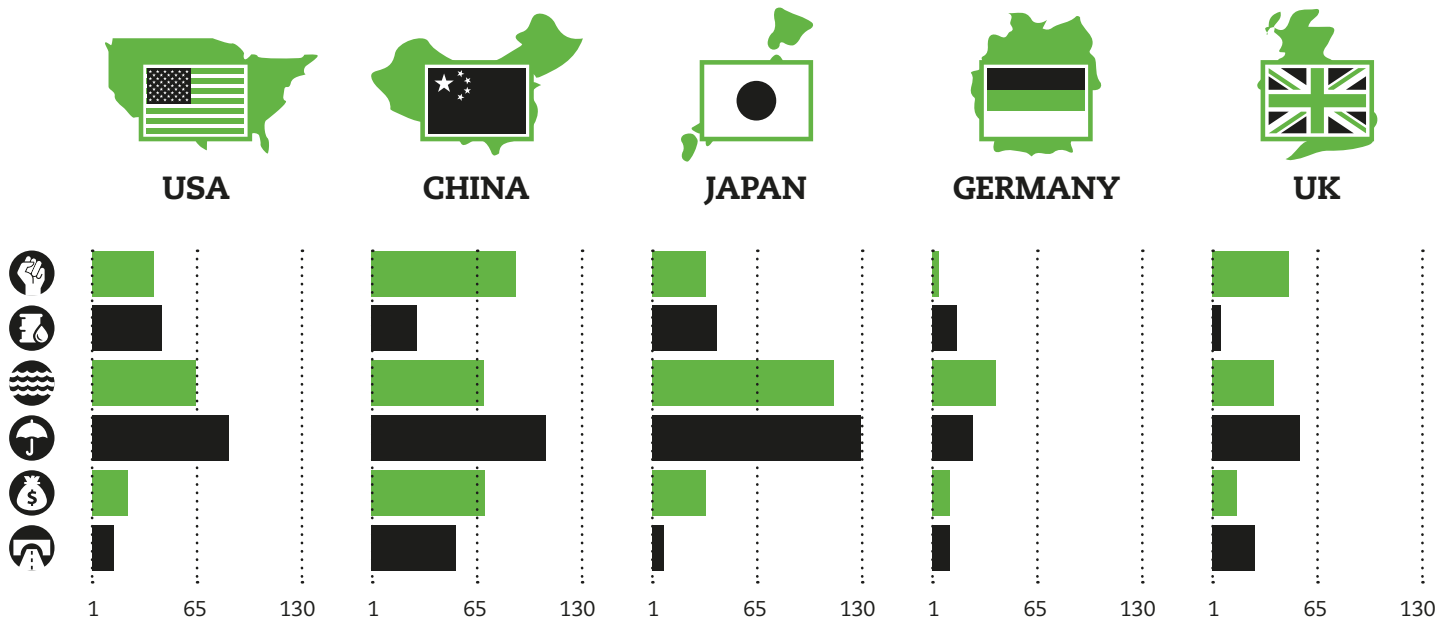
Key risks:

- Political risk
- Oil intensity
- Exposure to natural hazard
- Quality of natural hazard risk management
- Control of corruption
- Infrastructure risk

Source: FM Global Resilience Index, http://bit.ly/248W3Y1

Threat or opportunity?
Key goals in digital transformation strategies

Based on the percentage of respondents that answered "Very important"

Goal	%
Threat/breach mitigation	48%
Improve customer experience and enhance CRM applications	46%
To drive cost savings and operational efficiency	39%
Increased revenue potential	30%
Faster time to market	27%
Creating a more agile business	22%
Become more competitive	17%
Improve supply chain efficiencies	13%
To enter new markets	12%
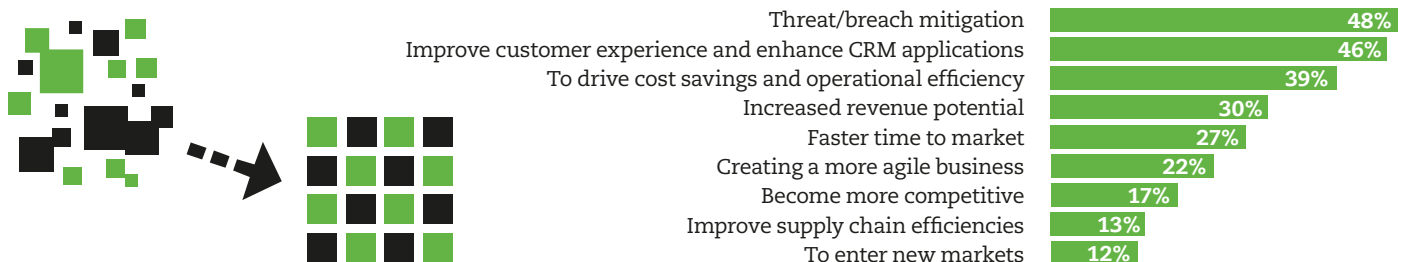
Source: PAC UK – Identity and Access Management in the Digital Age

Moral Imperatives

Ecclesiastical sees itself as an ethical insurer with a moral obligation to its customers to help manage risk. Group Chief Executive Jacinta Whyte explains why

BY ARTHUR PIPER

T he previous evening, Jacinta Whyte had landed in London on a late-night flight from Canada for one of her regular trips to the UK head office of Ecclesiastical, where she works as its Deputy Group Chief Executive with responsibility for the Group's General Insurance business. The next morning, when we meet, she is bright and focused, despite what must be some lack of sleep. The rain is beating on the upper storey office windows of Monument Place, where the views take in St. Magnus the Martyr Church and a sultry, brown Thames: landmarks that bookend both the insurer's past and some of its concerns about the future.

Climate change

"Cyber is an emerging risk, however, I think the biggest issue for the insurance industry revolves primarily around climate change," she says. Flooding affects the property space most obviously, but the effects of climate change reach into other aspects of the insurer's portfolio, such as liability risk, and they also cross over into broader social issues around corporate behaviour. It's a trend that Ecclesiastical takes seriously. The business has invested heavily in producing "huge, comprehensive documents," she says, about the repercussions of climate change – but the exercise is far from academic.

> ❝ There is a huge need to protect our customers and community – and that's what we call the greater good

advice on property maintenance, how the slope of adjacent land can be altered to protect buildings better, where to place flood gates, clearing pathways and building walls, and influencing local authorities in making sure rivers and canals are properly maintained and dredged. The aim is to make properties and areas more flood resilient. On larger schemes, such as major infrastructure projects, the company often works with the Association of British Insurers to lobby government on flood relief schemes and prevention measures.

"The objective is to protect and not to exclude badly hit areas from being able to obtain insurance," Whyte says. It has church clients and other customers in their specialty niches in many different locations, so the idea of defining some locations off-limits is anathema to the company's ethos. "Just because you're in an area that may be prone to weather effects does not mean we will not protect you. What we're trying to do is help you manage that," she says. That can involve getting into the small details – should a church have pews (difficult to move quickly) or chairs, wooden floors (expensive to keep replacing) or concrete ones? The philosophy is to improve risk mitigation when undertaking reparations.

"The implications of climate change not just for the industry but the global economy are quite significant," she says, "and so I think it's really important for us, as specialist insurers, to understand what that means not only for our business but for our customers, and what can we do to help them cope with its impact."

For a global insurer, it can be difficult to generalise about what those ramifications will be on either Ecclesiastical or on its customers. From ice storms in North America, to bush fires in Australia and floods in the UK, the symptoms are as diverse as they are geographically spread. She says the floods in the North West of England illustrate how unpredictable severe weather events are becoming. Over the past six years, there have been two severe floods – each supposed to be a one-in-two-hundred-year event. Chances are, there will be similar floods in the not-too-distant future.

"It's not so much the increasing severity which is of concern, but the increasing frequency," she says. So, even if the size of some of these global weather events is not as big as they used to be, they now occur much more often. Whyte's focus is pragmatic, though, and concentrates on what Ecclesiastical – a company she describes as a specialist, ethical insurer – can do to help people facing these traumatic incidents. Prevention and early intervention are key.

Preventative action

"There are a lot of preventative measures that can be taken, no matter which way you look at it, and I believe the role of risk management is to deal with leading and lagging indicators," she says. The in-house UK risk management team employs sixty or so consultants and surveyors whose job it is to get into the field and advise people how to mitigate risk and prepare for the worst. For flooding, for example, that can mean providing

Phil MacD Photography / Shutterstock.com

Above: Flooding in England is becoming more unpredictable.

As well as the increasing frequency of extreme weather events, Whyte says that the insurance industry is under pressure to change the way it operates because customers have higher and different expectations. She believes that customers are becoming more aware of events and their potential impacts because of the proliferation of media and, in some cases, personal experience. Customers are also more sophisticated about what they believe insurers should be offering. "They don't want a guardian angel," she says, "but they do want help with the things that they don't already know about and they want to know that we are there for them in their time of need."

Consumer savvy is also putting the execution of the service they get from an insurer under the spotlight. If things go wrong, customers can share bad experiences quickly to large audiences on social media. In 2015, according to the company's annual report, 94% of customers were either extremely or very satisfied with the way their claim was handled and a further 5% were fairly satisfied. Customer surveys on general satisfaction levels showed that 99% of home and 98% of commercial customers were satisfied with their new business experience. Whyte believes that these high levels, of which she is obviously proud, are not just down to response times, but also the company's practice of non-adversarial claim response, listening, and helping customers fix, where possible, what has made the property so vulnerable in the first place.

This granular approach to risk management has partly grown out of the fact that many of Ecclesiastical's clients are not-for-profit organisations that do not have the in-house capability of assessing and mitigating risk – and they have increasingly looked to their insurer to help them because they generally do not have budgets to procure expert help.

"Risk management as a specialist is the opportunity for us to broadly identify risks, either emerging or present, to educate those customers around mitigating that risk, or eliminate if they can, and by doing so they reduce likelihood of claims or trauma to their communities if it happens to be on the liability side," she says. As a result, risk management helps stabilise customers' budgets. "Our strategies always take a longer term view,' she says. "Particularly for those who are not resilient. There is a huge need to protect our customers and the community – and that's what we call the greater good."

Regulator's role

From an industry perspective, Whyte believes that the insurance sector is over-capitalised – in simple terms, there is too much money sloshing around. That has the effect of driving down the price of insurance as businesses look to increase market share at the expense of profit margins. If prices go too low, insurers will be unable to service their obligations. She can foresee the possibility of government intervention in the form of public policy on competition and consumer protection, drawing on the practice in some US States to make, say, certain motor and household insurance products regulated as a way of guaranteeing reliable cover.

And that may not be the only area where regulation becomes more pressing. The day of our interview, the BBC reported that the environmental law firm ClientEarth had threatened to sue the UK Government for failing to reduce air pollution, the levels of which breach EU limits. A month later, the UK Government said it would enact law to effectively cut the country's emissions to zero following a global climate summit in Paris.

ECCLESIASTICAL CUSTOMER SATISFACTION LEVELS

94% CUSTOMERS

Either extremely or very satisfied with the way their claim was handled.

99% HOME

98% COMMERCIAL

Customers were satisfied with their new business experience.

Whyte sees a key role for regulators in policing such statements and the standards that come through government to enact them.

Insurers and all other businesses have a role to play too in setting the tone from the top with their own environmental practices, she adds. And that means more transparent reporting to demonstrate how seriously companies take their moral obligations. "Customers may not be all equally competent at assessing these issues today, but they're aware of them," she says. "When they get to be consciously competent, they'll be very demanding. They'll want to check and understand your credentials."

In that sense, the demands of regulators and customers are relatively well aligned. "If you can prove what you're doing is in the best interests of your policyholders or your stakeholders, then that's all that you're being asked to do. So if you can't prove that, this raises the question of why you are doing what you do. It's all back to basics."

In fact, few insurance executives would light up about new initiatives from the Financial Conduct Authority, but that's exactly what happens when we begin talking about the UK regulator's recent focus on business culture. "It's a huge USP for us. I'm very excited," she says.

Why? Because creating the right culture goes back to the founding principles of the business. Clergymen with a concern for protecting the community established Ecclesiastical back in the 1860s – its first customer was St. Paul's Cathedral just a few minutes' walk from where we are speaking. She's trawled through company history and says she has found evidence of risk management from the late nineteenth century and she associates that with the ethos of caring about what happens to customers and helping them avoid or cope with the worst. And while the rise of consumerism has put all businesses under pressure to become more commercial, she says the business still operates on the ideal of "profits with a purpose." Running the business so that ethical concerns are built into the culture gives Ecclesiastical a competitive advantage over more profit-driven insurers, she believes.

It is also one of the reasons risk management is so central to the company's approach. "Risk management, I believe, is a moral obligation we have in terms of preventing things before they occur," she says. "It's also making sure that properties are valued to the appropriate level so that our customers don't carry any gap in their cover or protection."

Deeper knowledge

Ecclesiastical recently signed a corporate membership deal with the Institute of Risk Management (IRM). The risk management function is part of the business' leadership team – not that usual in the industry – and she wants to ensure that the people in the function operate at the highest level of professionalism and competence. "We hope to deepen our knowledge and expertise in risk by formalising our relationship with IRM," she says. "But it is also recognition that as much as we're only one of five insurers with chartered insurer status, we're now part of a professional body on the risk side. This demonstrates to our customers that our people are qualified and educated to give good advice and are seen to be professionals in their field."

Since risk managers are often the first face-to-face contact customers have with the organisation, the right training and professionalism is crucial. Again, it's the kind of pragmatism that seems to characterise Whyte's approach. The skills and knowledge and care that are valued at the very top of the company are also of value on the customer-facing side. It is, after all, a question of doing what is right. ⓡ

> " **Risk management is a moral obligation to customers**

Left: St. Paul's cathedral was Ecclesiastical's first customer back in the 1860s.

The Risk Academy

Jonathan Bloomer wanted to create an environment where people could enjoy a compelling career in risk management. But would any one at Capital One listen?

BY ARTHUR PIPER

Like many people of his generation, Jonathan Bloomer, Director at the financial services firm Capital One and Head of its UK Risk Office, fell into his first job in risk management by accident. "My Dad answered a letter I'd received from Deloitte because I was his last dependent and he wanted to get rid of me," he recalls with a smile. That was back in 1997 when risk management was not a well-recognised career among recent graduates and when entry and progression within the discipline was amateurish and ad hoc in most organisations.

Roll forward almost twenty years and with a spate of high-profile corporate collapses – Enron and WorldCom to name just two – and a fully-fledged financial crisis part of recent history, and things have changed radically. Governments, investors, regulators and, closer to home, company executives have all raised their expectations over the role and responsibilities of risk managers, especially in the financial services and regulated businesses sectors where Bloomer works.

While it is well recognised that businesses such as Capital One, which is headquartered for the UK in Nottingham, are based on sound risk management on the credit side, Bloomer is innovating and exploring what it means to improve operational risk management. If it's

Above: Capital One's UK headquarters in Nottingham.

> **This initiative is about creating a framework for all teams to invest in themselves**

good now, how can it be better? How is it possible, for example, to build the strongest risk management practices throughout the entire organisation when risk is often fragmented into operational silos and has to compete globally for a limited talent pool?

Bloomer's work-in-progress answer is the Capital One Risk Academy. Set up just over a year ago, the network unites all of the risk units within the business under a single group – more of a movement really – one that shares skills, knowledge and talent without creating a hierarchical structure that requires anyone having to be appointed king.

"What we're trying to do is to break down the silos of individual risk teams that exist across the organisation so that we have a compelling career of risk management at Capital One – that's the top line," he says.

This more sharing and collaborative approach among the different functions has resulted in risk management activity that has been supported by cross-functional and cross-disciplinary teams that was unlikely to have occurred previously. For example, risk identification workshops in a particular functional area are now more likely to be supported by a different functional area that has had experience with the task at hand. "We're just seeing more linkages because of the network we're creating and that's great," he says.

This more flexible structure should provide the risk professionals working at Capital One with better experience and career options within the business. Bloomer hopes that will help retain staff that may have been tempted to move on more quickly if they'd hit a perceived bottle neck within one of the risk functions.

In fact, Bloomer wants to provide an environment where members of the risk team can pursue the kind of career path that didn't really exist in 1997. He draws a parallel with the accounting profession. Accountancy has been a popular career option with recognised post-graduate qualification tracks for decades. That has helped to create a mature career path and a deep recruitment market. In risk management, that institutional structure is much more recent. In addition, the demands on risk management have intensified since the financial crisis meaning that all organisations are feeling pressure on the supply side for appropriately qualified staff.

"I can't do that just with my team of 15 people," he says. "But with 150 people it suddenly becomes feasible."

Getting started

Bloomer's idea was just a light bulb moment. He puts it down in part to the general corporate culture within

Capital One that everyone is obliged to change and to dissent from the status quo. That gave him the confidence to approach the board with the idea – just a notion at the time which he'd not fully fleshed out. He spoke to his boss, Chief Operating Officer Vicky Mitchell, and got immediate support to explore it further.

"I think if I told my boss that I was surprised at the support I got, she'd probably be surprised," he says. "But everybody has a voice in their ear saying 'they're not going to go for this'."

They did. Like Bloomer, the board understood the problems risk management faces generally – in recruitment, in raising expectations and in developing its skillset. So, the next step was to go and sell it to all of the risk management section heads, to convince them it was not just a power play from his part of the business.

It took five or six weeks to meet fellow directors, senior managers and talk to them about what the risk academy was, how it was a framework to unite their efforts more effectively, and what the key elements would be. "I wanted to be very clear that this initiative was about creating a framework for all teams to invest in themselves to do better and that it would not be a fully-robust model from day one," he says. "And, in fact, that it would remain thus and be relevant and up-to-date only if people committed to do it because it was relevant to them."

Everybody liked the sound of the idea, so he then presented to all of the teams individually. If he'd been mildly surprised by the support he'd received from the board and his fellow directors, he says he was blown away by how much enthusiasm the broader teams showed on his road show.

"It felt a little bit like there was a latent energy in those groups and all I was doing was lighting the touch paper," he says. He says that the risk managers recognised that the function had a role and identity within the organisation and that the academy would help boost its profile. But Bloomer was just one person and he could not implement it alone. He fired off an invitation to all 150 associates within the academy framework asking for people to volunteer their time in the best way they could. About one in four people came back with an offer of help.

> ❝ There was a latent energy in those groups and all I was doing was lighting the touch paper

They spoke and corresponded and came up with four work streams on which to focus: learning and development, developing the professional network (including putting on larger events), using the internal technology at their disposal to support the academy, and talent management. Then people self-selected which they would help with and how. While there is a steering group, people meet regularly, take on responsibility to get things done and keep the whole program rolling.

"No one's had 25% of their role taken away so they can focus on this," he says. "They're all doing it from goodwill. That is the sense of energy that has genuinely surprised me. I wasn't really expecting it."

Mechanics and measurement

As far as the academy is structured, it relies on a weekly stand-up meeting on a Monday where representatives

Left (left to right): Bryan Maunder – Risk Reporting Manager, Amy Weston – PA, Jonathan Bloomer – Director UK Risk Office, Lotty Thompson – Risk Graduate, Simon Robinson – Business Continuity Analyst, Rob Baxter – Senior Manager, Risk Governance.

from the four work groups report on progress, share ideas and see where they can help each other. There are networking events, an internal website and lots of informal conversations offline to keep things moving. Being in a single building helps, he says. Given that the academy is a volunteer group, finance has not been a challenge. But developing key performance indicators is still a work in progress.

"I don't have them," he says, "because I'm not yet quite sure what I would measure." He says a lot of the benefit is qualitative. "If you want to know whether executive management feel they are getting better support from a risk management team, that's hard to measure properly," he says.

One concrete win, though, has been Bloomer's ability to take on a graduate trainee – the first time the function has taken that route. He says the company had to close the advert when the number of applicants shot to 260 in just two weeks. He read through

"an awful lot" of the application forms and noted that the majority quoted the risk academy as a plus point. He believes the mix of qualifications and the ability of rotating the graduates through the different parts of the risk team is something that helps differentiate the business.

Bloomer has also taken out a group scheme membership with the Institute of Risk Management. Forming the academy has given him economies of scale and the ability to save some money on bespoke IRM courses and events that wouldn't otherwise have been possible. Staff also get a discount on their fees when taking qualifications. He's also looking at the IRM's accreditation scheme which he hopes will help him create an internal way of grading team members through their different ability and qualification levels.

"What I'm trying to do, for those who are minded and want a career in risk management, is to structure learning and development in a

way that helps them through that journey," he says.

Bloomer fully expects the academy to be running two or three years from now. And he'd advise risk leaders to set up their own versions of the initiative if they are facing similar issues. They will need buy-in from the top as a minimum and they will need to be bold. "Don't just imagine," he says, "why not go out and make it happen?" ℝ

> ❝ **Graduate applications quoted the academy as a plus point**
> ....

CULTURE

Talking about safety and culture

Do we really know what we mean when we talk about safety, risk and culture. Sociologist Susan Silbey provides some much-needed perspective

BY SUSAN SILBEY

Between 2000 and 2007, safety culture emerged as a common trope in contemporary scholarship and popular media as an explanation for accidents and as a recipe for improvement in complex socio-technical systems. Over 2250 articles in newspapers, magazines, and scholarly journals appeared in an eight-year period while only 570 references occurred in the prior decade, and none before 1980. What do people mean when they talk about safety culture?

Three conceptions of culture circulate: culture as causal attitude, culture as engineered organisation, and culture as an emergent system of signs and practices. Consider the oldest notion where safety culture is understood as a measurable collection of individual attitudes and organisational behavior. When culture is talked about as a causal agent expressed in workers' attitudes, it drives organisations towards "the goal of maximum safety health, regardless of the leadership's personality or current commercial concerns," James Reason wrote in *Managing the risks of organisational accidents* in 1997.

However, the particular mechanism that shapes the safe or unsafe outcomes of the organisation or technology is usually unspecified, with much of the management and engineering experts debating how to define, operationalise

> " **For those who reject these instrumental conceptions, culture is best understood to be emergent and indeterminate, an indissoluble dialectic of system and practice**

Left to right:
Deepwater Horizon, Chernobyl Nuclear Reactor, Challenger shuttle explosion.

and measure both the mechanism and the outcome. The *Report of the BP Texas City Refinery* explosion marked, perhaps, the quintessence of talk about safety culture with more than 390 references to the failed safety culture distributed across the 150-page document. Although the report began by assigning upper level managers responsibility, the Blue Ribbon panel ultimately devolved responsibility to the workers because management practices are not sufficient to achieve outstanding safety performance; *all* of a company's workers must be engaged and involved.

Learning culture

Others speak less about safety culture in general than more specifically about an organisation's learning culture that characterises "high reliability" organisations. Like the notion of culture

as a set of causal attitudes, the properly engineered organisational culture will produce the desired reliability and efficiency. This work advances culture as attitude notion by its explicit articulation of the organisational configuration and practices that will make organisations more reliably safe; it goes beyond attitudes to focus on states of mind or mindfulness.

Mindfulness and organisational learning is created by a preoccupation with failure, reluctance to simplify interpretations, commitment to and capabilities for resilience, and perhaps most importantly resistance to over-structure or a preference to underspecify the system. In this sense, safety culture can be understood as "interpretive work directed at weak signals", as Diane Vaughan wrote in *The challenger launch* in 1996. Although scholars of high-reliability organisations most often describe

the prevalence of these conditions in military-style organisations, each of which holds itself to a failure-free standard of performance (e.g. nuclear submarines, nuclear power plants, aircraft carriers, space shuttles, and air traffic control), processes of collective mindfulness are promoted in non-military organisations as well.

Unfortunately, despite the logic and persuasiveness of this conception of mindfulness as an effective safety culture, the best empirical tests have found it wanting. Even in military organisations, past errors are repeated, information for learning is not shared, redundancy is often the source rather than protection against mishaps, and protocols for ensuring against accidents are not followed in high alert, crisis situations. Instead, adaptive, yet improvisational decision-making practices of bounded rationality prevail in many complex organisations

where fluid environments, unclear goals, misunderstanding, and happenstance prevail.

Accidents will happen

If optimism characterises those who advocate high-reliability, learning organisations, in effect suggesting that if we only try harder we will have virtually accident-free systems, more skeptical scholars believe "that no matter how hard we try we will still have accidents because of the intrinsic characteristics of complex, tightly coupled "systems," as Charles Perrow wrote in the second edition of *Normal accidents* in 1999. Moreover, too many of the promoters of safety culture imagine easily malleable and homogeneous cultures.

For those who reject these instrumental conceptions, culture is best understood to be emergent and indeterminate, an indissoluble dialectic of system and practice: inseparable signs and performances, meanings and actions that are only abstractly identified as a system of interconnecting elements. Thus, safety culture is used to emphasise that organisational and system performances are not confined to formally specified components, nor to language alone, and moreover that formal and informal actions make sense only because they are systemically associated.

As such, the consequences of safety culture cannot be engineered and only probabilistically predicted with high variation from certain. For those who adopt this sociological and anthropological notion of culture, safety is "situated in the system of ongoing practices…safety-related knowledge is constituted, institutionalised, and continually redefined and renegotiated within the organising process through the interplay between action and reflexivity." Here, safety practices have "both explicit and tacit dimensions, [are] relational and mediated by artifacts, … material as well as mental and representational," as Silvia Gerard and Davide Nicotine wrote in "To transfer is to transform," in the journal Organisation in 2000. Rather than a specific organisation of roles and learning processes or measurable set of attitudes and beliefs, safety is understood as an

elusive, inspirational asymptote, and more often only one of a number of competing organisational objectives.

Thicker notions of culture

Research on this thicker notion of culture has observed that: (1) Linguistic schema, formal categories, embedded norms, familiar artifacts provide both fixed and flexible frames of reference with which people apprehend and interpret information system performances, risks, and safety. (2) Information that might shape more cautious and responsive interpretations is often missing, actively buried, or discredited. (3) Dangers that are neither spectacular, sudden, or disastrous, or that do not resonate with symbolic fears can remain ignored and unattended, and as a consequence do not get interpreted nor responded to as safety hazards. (4) Organisational structures, roles and routines shape

interpretations so that different organisational positions produce very different understandings of risk and error. (5) The larger macro-societal and popular culture embeds particular interpretations of risk and safety and repeated organisational and institutional failures breed generalised and disproportionate fear and uncertainty.

However, too often, the discussions of safety culture ignore just those features of complex organisations and technological systems from which cultural schemas and interpretations often emerge: normative heterogeneity, competitive and conflicting interests, as well as inequalities in power and authority. Thus, what is specifically missing from accounts of safety culture is attention to the mechanisms and processes that produce systemic meanings about risk, safety, authority and control. One is hard pressed to find a reference to power, group interests, conflict, or inequality in the literature

> " Even in military organisations, past errors are repeated, information for learning is not shared, redundancy is often the source rather than protection against mishaps, and protocols for ensuring against accidents are not followed in high alert, crisis situations

Left to right: Bhopal, Exxon Valdez and wildlife affected by the disaster.

> " Recognising the greater power of management, safety culture advocates nonetheless fail to adequately recognise the diminished power of those in subordinate positions

promoting safety culture.

This is not to say that there is no recognition of hierarchy. Indeed, the proponents of safety culture recognise the greater authority and resources of top-level management, and recommend using it to institute organisational change from the top down, mandated by organisational leaders, if designed by management consultants. In fact, the consistent valorisation of clear lines of hierarchy accompanies a surprising failure to see how this very same hierarchy undermines communication and self-reflection about hazards. Recognising the greater power of management, safety culture advocates nonetheless fail to adequately recognise the diminished power of those in subordinate positions. As a consequence, organisations often attempt to institute safety culture by addressing the workers at the lowest, least powerful level of the organisation.

Unintended consequences

Research on accidents and disasters has repeatedly demonstrated what sociologists have known for close to a century: all purposive social action has unintended consequences and, although social action is inherently variable, social solidarity and coordination are sustained by perceptually, conceptually, and morally normalising the variation. Thus, we fail to distinguish novel or threatening from familiar and manageable events, productively innovative from functionally destructive deviance.

To function in a world of many others, we must synthesise and generalise completely the capacity to act. We must challenge the ordinary processes of normalisation across variation. If safety demands seeing what is not there, an absent accident-in-the-making, then safety culture needs to identify the processes that successfully unsettle organisational routines to make the unseen thinkable.

Why has attention to safety culture arisen at this historical moment? Any answer must begin by acknowledging the technological catastrophes of the last forty years: Three Mile Island,

Bhopal, Chernobyl, the Challenger and Columbia accidents at NASA, the Exxon Valdez oil spill, oil rig accidents, Buffalo Creek, contaminated blood transfusion, Deepwater Horizon. In each instance, the accident is usually explained as just that, an accident, not a system or design failure, but the result of some extraneous mistake or mismanagement of a basically well-conceived technology. Because the systems in which the accidents occur are omnipresent, the recurring accidents undermine confidence that catastrophes can be avoided. Alongside concerns about genetically modified foods, the toxicity of commonly used household products, the migration of various synthetic compounds from plants through animals into the human body, the rapid spread of disease and contamination through porous and swift global transportation routes, as well as humanly produced environmental degradation, technological accidents feed a deepening mistrust of science.

But, accidents alone cannot be driving the recent attention to safety

culture. Technological accidents are not a new phenomena and safety has been a lively concern since the middle of the nineteenth century, if not earlier. Indeed, in some accounts, much of the regulatory apparatus of the modern state was institutionalised to protect against the injurious consequences of industrial production by setting minimally safe conditions of work, establishing private actions at law, and spreading the risks (of what could not be prevented) through fair trade practices, workmen's compensation and pension systems, as well as labor unions, private mutual help, and insurance. Safety was one of several objectives promoted by the system of instruments regulating relations between capital and labor.

Responsibility

Talk about safety culture offers a new twist, or possible reversion, in the allocation of responsibility for technological failures, a return to the nineteenth century and earlier regime of individual responsibility but in a context of more hazardous and global technologies. After several decades of sustained attack by advocates seeking supposedly more efficient and just allocations of goods through unregulated markets, the regime of collective responsibility has been dismantled, replaced by one of institutional "flexibility". Rather than attempting to mitigate and distribute risk, contemporary policies and practices *embrace* risk, conceiving and addressing situations in terms calculated probabilities of hazard. Human life, including the prospects of human autonomy and agency, are now conceived in very much the same way and analysed with the same tools as we employ to understand and manipulate physical matter: ordered in all its important aspects by probabilistic calculation and mechanical regulation.

Unfortunately, risk analysis

and discourse narrows analysts' consideration of legitimate alternatives while nonetheless sustaining the appearance of liberal pluralism. Because hard-nosed realism is assumed to reside exclusively in quantifiable measures, unmeasured variables are excluded from official risk discourses. Allegedly empirical analyses become solipsistic, focusing exclusively on the methods and epistemologies internal to technological instrumentalism. This supposed realism is illusory because risk become reactive, self-reproducing moral hazards. Embracing risk also refers to the specific policies and techniques instituted over the last several decades to undo the system of collective security, risk shifting. In place of the regime of risk containment, proponents of flexibility argue that safety and security can be achieved more effectively by embracing and privatising risk.

Thus, contemporary moral entrepreneurs energetically promote as morally desirable risk-taking rather than risk-sharing; the individual more effectively provides for family security, it is claimed, by participating in a competitive, expanding, market economy than by relying on government constructed "safety nets." This moral entrepreneurship directs our attention to safety culture because the concept arises as a means of managing technological risk as the previous security regime has been successfully dismantled.

This is not to say that the nineteenth-to-twentieth-century regulatory system was perfect, nor as good as it might be, nor that it prevented or repaired all or most technological damage. It was, however, a means of distributing, if not preventing, the costs of injuries. Yet, for most of the twentieth century, risk analysts themselves expended a good part of their energy attacking this system, legitimating the risks undertaken, reassuring the public that

Above: Challenger shuttle disaster, black smoke can be seen bottom right.

they were nonetheless being protected, and second guessing the regulatory agencies' attempts to do a very difficult job. Paradoxically, many risk analysts regularly assessed the risks of regulation more negatively than the risks of the hazards themselves.

The endorsement of "safety culture" can be usefully understood as a way of encouraging and allocating responsibility, one response to the dangers of technological systems. However, invoking culture as both the explanation and remedy for technological disasters obscures the different interests and power relations enacted in complex organisations. Rather than forgoing particularly dangerous technologies or doing less in order to reduce vulnerabilities to natural, industrial or terrorist catastrophes, talk about safety culture reinforces investments in complex, hard-to-control systems as necessary and manageable, as well as highly profitable (for a few), although unavoidably and unfortunately dangerous (for many). Talk of safety culture suggests that the risks associated with increased efficiency and profitability can be responsibly managed and contained. ⓔⓡ

··

Susan S. Silbey, Professor of Sociology and Anthropology at Massachusetts Institute of Technology. ssilbey@mit.edu

> " **Paradoxically, many risk analysts regularly assessed the risks of regulation more negatively than the risks of the hazards themselves**

Institute of Risk Management

irm Global Risk
AWARDS 2016

15 April 2016
Venue: Park Lane Hilton Hotel, London.

AWARDS DINNER
celebrating success

IRM's fourth annual Global Risk Awards. Our entrants are internationally recognised for their excellence in risk management.

visit us at **www.theirm.org/GRA2016**

Book Your Table

Prices:

Tables of 10
Table(s) of 10 for awards entrants: £2995+VAT
Table(s) of 10 for non-awards entrants: £3495+VAT

Individual Dinner Places
Individual Dinner Places for awards entrants: £325+VAT

Individual Dinner Places for non-awards entrants: £375+VAT

Booking & Sponsorship Opportunities
Clementina Christopher, Sponsorship & Advertising Manager
t: (0)207 709 9808
e: clementina.christopher@theirm.org

400 guests **40** countries **13** categories **1** amazing night

Headline sponsor

Platinum sponsor

Award sponsor

Award sponsor

In association with

QBE

AON
Empower Results®

ZURICH®

AXELOS
GLOBAL BEST PRACTICE

CITY OF LONDON

irm

CULTURE

Getting to grips with culture

Culture may be difficult to define and control, but regulators have put it squarely on the agenda for risk managers

BY ALEX HINDSON

Enterprise risk management (ERM) has been under the spotlight since the 2008 financial crisis, particularly in the financial services sector. The question is often asked, where was ERM? This reflects a concern that the focus has been on implementing ERM processes but that it has failed to engage people's hearts and minds. This has led to a significant increase in regulation, process and governance. There is however no guarantee that all this regulatory attention will drive a change in staff behaviours. This requires a change in risk culture.

Culture in many ways is what staff in your organisation do when you are not watching them. It is values-based and ethically driven. You can create ever-stronger processes and controls, but if your staff do not understand or buy-in, these will only be paper thin and will probably not stand up to scrutiny in a future crisis.

The Financial Reporting Council (FRC) has raised pressure by publishing *Guidance on risk management, internal control and related financial and business reporting*, which confirmed the board's accountability for defining "the culture it wishes to embed in the company, and whether this has been achieved". The FRC further anticipated that companies would provide information on progress in

> " Culture in many ways is what staff in your organisation do when you are not watching them

RISK CULTURE FRAMEWORK

Source: *Risk culture – resources for practitioners*, IRM

achieving their desired culture within their annual reports.

In the financial services sector, the Financial Stability Board (FSB) issued specific guidance to regulators on evaluating an organisation's risk culture. *Guidance on supervisory interaction with financial institutions on risk culture* provides 35 targeted questions covering four major themes that can be used in appraising an organisation's risk culture: tone at the top, accountability, effective communication, and challenge and incentives.

The IRM has produced a series of papers on risk culture, which provide a working definition: *The values, beliefs, knowledge and understanding about risk shared by a group of people with a common purpose, in particular the employees of an organisation or of teams or groups within an organisation.*

Risk culture can be seen as a complex outcome of a series of concentric and interacting factors – see *Risk culture framework*. Individuals in an organisation each have a set of personal predispositions to risk-taking, which are deeply held attitudes shaped by formative experiences. These are overlaid with personal ethics, the anchors that drive people's values. These aspects of people's personalities are not readily visible but their behaviours can be observed and measured. Collective behaviours, "the way we do things round here," form an organisational culture, and this in turn influences an organisation's collective risk awareness and approach to risk-taking in decision-making.

Developing an approach

The first thing to realise is that risk culture is a complex issue. It is possible to glimpse it through different aspects of a prism but it would be foolhardy of anyone to claim to fully understand it or be able to control it.

The second important point is to understand that any work an ERM function might want to undertake with respect to risk culture will become a change management programme applied to a complex social system. As such, risk professionals need to be humble enough to recognise that they are not always equipped with sufficient understanding of psychology and sociology to tackle this alone, and they should reach out to others to partner on this topic. Human resources and communications professionals can be key allies in seeking to drive organisational change and they may have their own objectives in terms of driving certain behavioural changes.

Although risk culture is complex to

grasp and difficult, if not impossible, to measure, it is possible to diagnose and understand aspects of risk culture.

Tools and methodologies exist for sampling the risk culture of an organisation, and different tools can be used to test at different layers of the onion diagram of the *Risk culture framework*. Psychometric tools are, for example, particularly useful in investigating the innermost two layers, whereas surveys and interviews are more appropriate for the outer layers. The IRM report gives further guidance on available diagnostic tools.

One important facet when thinking about the risk culture of your organisation is to reflect on how best to implement an ERM programme successfully. ERM needs to be implemented in a different manner depending on how an organisation operates more generally. The *Risk aspects culture model* provides a simple way for considering what type of organisational culture you might be dealing with.

Systems of control define the extent to which activity is governed by formal processes which staff are expected to comply with. The other extreme (independence) describes an organisation where staff make their own decisions based on their values. If a common governance spirit exists together with independence, an engaged culture results where people tend to do the right thing because they firstly understand the context and they share common values. A strategic governance approach means that in an engaged culture it is important to understand that ERM needs to be sold to people, they need to understand the benefits to them personally and to the organisation as a whole.

In other organisations with a strong rules focus and weak spirit, a sleepwalking culture might have been created. People tend to blindly follow the rules they have been given without engaging with broader objectives. A minimalist governance approach is warranted in this situation to prevent the controls and processes being counter-productive. The danger is that if procedures are too complex then staff may take the opportunity not to think sufficiently about what they are doing.

Complier culture describes an organisation where there is a strong

RISK ASPECTS CULTURE MODEL

Common Governance Spirit
Widely held system of shared meanings. Rules are adhered to.

STRATEGIC GOVERNANCE

CONTROL GOVERNANCE

Independence
Increasingly independent of other people's pressure to conform. Staff are left to be guided by their own values.

Engaged Culture

Complier Culture

Systems of Control
Strong pressure to conform to shared system of meanings. Rules are set to guide behaviour.

Chaotic Culture

Sleep-Walking Culture

TACTICAL GOVERNANCE

MINIMALIST GOVERNANCE

Weak Governance Spirit
Private system of meanings. Rules are not implemented.

Source: IRM

> **Any work an ERM function might want to undertake with respect to risk culture will become a change management programme applied to a complex social system**

alignment of understanding in terms of common governance spirit as well as a preference for systems of control. In such an organisation, rules are not only welcomed but they are closely followed. There is a desire for compliance, although this may in some ways stifle creativity. In such an organisation a governance approach built on a strong internal control system would work well.

Finally, in an organisation with weak governance spirit and a preference for independent thinking, a chaotic culture could develop with few rules and those that are in place not being followed. In such an organisation, a very tactical approach needs to be taken to governance where only the essential elements are implemented and very much on a needs basis.

Pragmatism

Clearly a risk management function needs to consider both the extent to which the current culture needs to be moved over time; but a pragmatic perspective needs to start from the prevailing situation.

Ultimately if the goal is to create

a risk-aware culture, where people are able to make informed decisions based on a clear understanding of the threats and opportunities associated with business opportunities, then they need to be informed, empowered and encouraged to actively consider risk.

A risk-aware organisation will potentially be more attuned to its external environment and its internal capabilities, and it will also be more agile and resilient in responding to rapidly changing circumstances. A culture where staff are encouraged to consider the threats and opportunities around their business activities will potentially grasp the implications of changes sooner, identify and harness opportunities, and be better able organise its resources in a joined-up manner.

Change or influence

So how does one approach this? Influencing an organisation's risk culture is clearly a significant change management initiative. The IRM offers guidance in terms of the risk aspects culture diagnostic. Eight distinct *Areas of risk culture* are described. The five aspects outlined in pale grey relate to the governance-related, or hard, aspects of culture related to leadership roles and functional responsibilities, reporting and disclosure. By contrast the three dark grey aspects covering societal-related,

or soft, aspects of culture deal with skills, remuneration and dealing with bad news. By considering these eight aspects, it is possible to design a series of interventions to allow cultural change to be initiated.

Risk culture is very important for organisations to grasp, under increased scrutiny by external stakeholders such as regulators and

shareholders, but it is also not an easy aspect of ERM to master.

Creating or shaping a more risk-aware culture is however potentially the greatest value a risk function can bring to the table in terms of preparing their organisation for the challenges of uncertain and fast-changing environments.

An organisation with a risk-aware culture is one that is more resilient to external influences and better able to adapt. The principal benefit of a strong risk culture comes from enhanced and timely decision-making. An agile organisation is able to reach decisions in terms of the risk and reward of different opportunities more quickly and in a more informed manner. These benefits drive external perception of an organisation by its stakeholders such as investors, analysts, credit rating agencies and regulators. Ultimately a risk-aware culture can protect and enhance corporate reputation. ⊞R

Alex Hindson is Chief Risk Officer at ArgoGlobal.

AREAS OF RISK CULTURE

Tone at the top	Risk Leadership	Informed risk decisions	Decision making
	Dealing with bad news	Reward	
Governance	Accountability	Risk resources	Competency
	Transparency	Risk skills	

Source: IRM

Coming into the light

The European Commission is implementing two major initiatives aimed at enhancing corporate transparency, but what is the role of the risk manager likely to be?

BY JO WILLAERT

Since the financial crisis, there has been a strong trend in the European Union in its member states and other bodies for ever greater transparency from large companies, including risk-related information. As risk managers, we believe that we have an important role to play in helping our organisations meet these requirements through enterprise risk management.

Currently, EU pressure for more corporate transparency translates into two main areas. Non-financial reporting, covering issues like the treatment of employees, the environment, human rights and anti-corruption. And country-by-country financial reporting, which came into effect for certain industries in 2014, and now could be extended to all large multi-nationals in Europe.

Non-financial reporting is the latest measure to come to the fore. The Non-Financial Reporting Directive has been agreed and will be implemented by the end of 2016 in all EU countries. The directive specifically asks that the non-financial statement that companies will have to provide from 2017 contains a description of its principal risks and how the organisation is dealing with them. These non-financial elements are principally environmental, social and employee matters, or what are often called corporate social responsibility (CSR). It also applies to the

Above: Jo Willaert, President of the Federation of European Risk Management Associations (FERMA).

gender composition of the board. This transparency is translated in non-financial reporting, containing a description of the principal

non-financial risk exposures under the directive. The guidelines are important because they are meant to give practical help to companies

They are responsible for managing the enterprise risk management process and I believe that risk management tools and people can help companies meet the requirements of the directive and enhance performance.

Fundamental role

In its response to this consultation, FERMA urged the Commission to recognise in the guidelines the fundamental role of risk managers and the value of enterprise risk management (ERM) methodology in the reporting of non-financial or corporate social responsibility elements, which require a deep understanding of the business model of the organisation. Many of these issues will arise through the company's supply and distribution chain.

It is difficult for specialists in

> " The value of reporting risks connected with non-financial elements of business conduct goes far beyond concern for reputation management

risks and how the organisation is dealing with these risks.

Most recently, the European Commission conducted a consultation exercise on the guidelines that will be issued to large enterprises on how to identify and disclose their

in writing their statements, and so facilitate the disclosure of non-financial elements and their risks.

A large proportion of European risk and insurance managers work for companies that are affected by the requirements of this directive.

Left: Marie-Gemma Dequae.

TRANSPARENCY NEEDS ERM

Improvements in corporate transparency are closely linked to enterprise risk management, says Marie-Gemma Dequae

Transparency in non-financial reporting can only be organised in a sustainable way if there is a well-established enterprise risk management (ERM) methodology and framework. This ERM is a substantial part of corporate governance. It is part of the second line within the three lines of defence, working together with the first line of operational and control managers, and with the third line of internal audit. Good cooperation between all lines is of great value in order to reach high quality reporting. This emphasis on cooperation is clear in reports prepared by FERMA together the European Confederation of Internal Auditing (ECIIA) on the most recent European Company Law Directive.

The risk manager pays attention to all risks, current and future. In today's rapidly changing business environment of disruptive technologies with, for instance, shifting cyber and terrorism risks, focus on emerging risks is important. Therefore, it would be valuable for the EU to recognise and ask for formalisation of the role of the enterprise risk manager, in the way that the European General Data Protection Regulation does for the data protection manager. Reporting on risks without a sustainable ERM methodology and framework is in itself a major risk and can damage the competitiveness of European companies on foreign markets and their sustainable performance.

Although country-by-country financial reporting is less part of the risk manager's day-to-day responsibilities than non-financial risks, it is not that remote. In addition to compliance and reputation risks, as Jo Willaert has explained, there could be issues related to global insurance policies with focus on tax issues: when to issue local policies, how to allocate global premiums to local subsidiaries and their tax issues, how to settle claims internationally and so on. Captives may also come under the spotlight.

According to recent discussions with CFOs, good cooperation between risk managers, CFOs and fiscal managers is needed and is already growing. Therefore, good fiscal risk management in the international environment is essential to realise high quality country-by-country reporting and minimise the related risks.

✎ **Marie-Gemma Dequae, member of IRM's technical and education committee and FERMA's scientific advisor.**

separate departments or subsidiaries to connect different aspects of risk across functions, leaving grey areas where awareness and reporting could be incomplete. The overview of enterprise activities that the risk manager gains not only supports compliance but at the same time helps the organisation manage the associated risks, such as non-compliance and reputation, and enhance performance.

> ❝ **Reporting on risks without a sustainable ERM methodology and framework is in itself a major risk**

Risk reporting is a key element of the risk manager's role. Because of the cross-functional nature of the risk manager's mission, he or she is well placed in the organisation to identify the various types of risks and develop mitigation plans.

When deploying an ERM methodology for the organisation, the risk manager is already doing what the directive would like to see about risks related to non-financial issues. If guidelines want to be practical and helpful for organisations, they need to indicate where to look to prepare a correct non-financial statement.

Risk managers also already work with other risk professionals within large companies, such as internal audit, and together they will respond to this pressure for transparency and provide the necessary assurance that the various types of risk have been identified and disclosed to comply with the directive.

The value of reporting risks connected with non-financial elements of business conduct goes far beyond concern for reputation management. The creation of a complete, company-wide risk management policy, including non-financial aspects, leads to thorough risk knowledge that creates a global decision-making tool for the board. Being in control of these

Guidance on the **8th** EU Company Law Directive
article 41
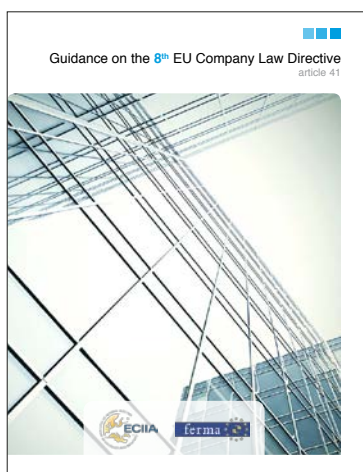
Above: The guidance issued by the ECIIA and FERMA can be downloaded from their websites.

risks, therefore, opens the way for productivity and efficiency gains over the long term.

Country by country

On 12 April 2016, the European Commission published a proposal that would require approximately 6000 large, multi-national companies active in the EU to disclose their tax and other financial data on a country-by-country basis within the EU. Such country-by-country reporting is already required for logging and extractive industries following the new Accounting Directive in 2014.

Even before the revelations in early April about tax matters involving a Panamanian law firm, member states had been pressing for more financial transparency from multi-national companies operating in Europe for some time. They see country-by-country reporting as a measure that hopefully would increase their tax income from international companies operating in their markets. NGOs, likewise, have been lobbying hard to put financial transparency on the top of MEPs' agendas, encouraging them to introduce amendments in several different EU draft laws.

The Commission's proposal, which would involve an amendment to the Accounting Directive, is now being discussed by the European Parliament and Council. It is too early to say what the final outcome will be.

If implemented as it stands now, companies would have to disclose publicly the corporation tax they pay specifically in each member country where they do business. In addition, they would be asked to disclose how much tax they pay on the business they conduct outside the EU. The Commission warns that particular attention will be paid to tax information relating to countries that do not respect good governance standards.

From a risk manager's point of view, pressure for such increased financial transparency carries regulatory and reputational implications, but they are not all negative. First, unprepared or unaware companies could face public naming and shaming for failure to make adequate disclosure and possibly regulatory action and fines. Second, revelation of tax planning which is legal, but regarded as "unfair" by the public, could result in negative public comment and so pressure to change to a more national approach that could involve higher tax bills. Finally, by contrast, companies may gain competitive advantage if they can demonstrate their tax planning follows generally accepted business practice in the markets where they generate their profits.

Country-by-country reporting in the EU for all large multi-nationals has yet to be agreed, but it is not the only source of pressure for increased disclosure on tax matters. Risk managers should be knowledgeable about the financial flows of their organisations, so they can play a role in alerting their board and senior management to the possible risk implications – positive and negative- of the demand for ever greater financial transparency. ⒻⓇ

Jo Willaert is President of the Federation of European Risk Management Associations (FERMA).

Aiming for the pinnacle

The industry benchmark principles for risk management are undergoing change. But the challenges of full implementation are likely to remain

BY SARA KAMIYA

One of the most widely accepted set of principles and guidelines for implementing risk management in organisations is up for revision. Since its publication in 2009, ISO 31000 has been adopted as a national standard by more than 50 national standards bodies covering over 70 % of the global population, according to the International Organisation for Standardisation which publishes the guidance. That includes UN agencies and national governments, especially in the areas of disaster risk reduction and the management of disaster risk.

One of the attractions of ISO 31000 is its flexibility. It builds on a well-known Enterprise Risk Management (ERM) standard published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) back in 2004 – and provides clarity to the meaning of key risk management terms, approaches and their limitations.

"Importantly," says the IRM's guide to the standard *A structured approach to Enterprise Risk Management*, "the guide recognises that risk has both an upside and downside."

Why revise?

So, why revise it? "A need was expressed by risk practitioners, especially in the G20 economies, for a high-level document that reflects the way risk is managed in multinational organizations and national governments,"

> " Risk managers need to be able to identify, quantify and communicate the return on investment of an effective enterprise-wide risk management process based on ISO 31000

YuG / Shutterstock.com

> **" The guide recognises that risk has both an upside and downside**

says ISO spokesperson Sandrine Tranchard, "as well as how risk management should be incorporated into the governance and management systems of organisations." The revised guidance is expected any day now.

Implementation of the standard is not without challenges, says Russell McGuire, Practice Director, Enterprise Risk Services, at the software consultant Riskonnect.

"ISO 31000 is more of a guide than a mandate, so getting executive support may initially be harder to obtain," he says. "Risk managers need to be able to identify, quantify and communicate the return on investment of an effective enterprise-wide risk management process based on ISO 31000."

Establishing ownership of the components of risk management can also be a challenge. "From objective owners down throughout the organisation, there is often inaction without ownership," he says. "Simplified data gathering is the key,

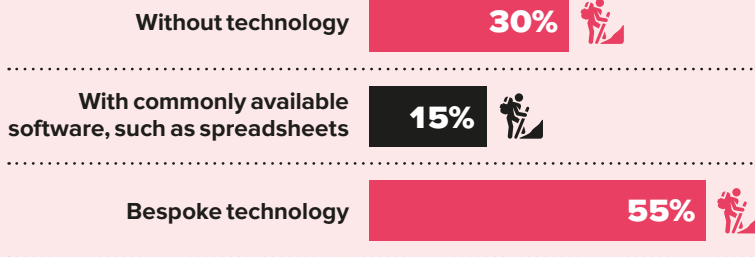followed by having the technology do the heavy lifting of data aggregation, analysis and reporting."

Implementation can also be an endless process. "Knowing where enough is enough," McGuire says. "Identifying and understanding what the end game should look like and then mapping out a process to get there is critical to success of an enterprise-wide risk management process."

Technology

While technology can help, typically a significant portion of the early work requires little or no technology. Policies and guidance need word processing at most. Depending on the intended maturity level of the enterprise-wide risk management process, the level of technology changes.

Few organisations need to achieve the pinnacle, McGuire says, and can have a very effective enterprise-wide risk management process without the

use of highly technical and expensive simulation tools. "Rather than aiming for a high risk maturity level, risk managers need to identify the right level for their organisation and then seek technology to achieve that level, if necessary," he says.

But ISO 31000 is not just for larger organisations, which is why the standard-setter has also released a guide for small-to-medium-sized businesses (SMEs) recently.

"Whilst most SMEs manage risk to a large extent, a number of SME leaders don't consider implementing formal risk management processes, believing they aren't big enough to warrant a proper risk management system or because they feel they are too busy running the company," says John Lark, the author of the handbook.

Other related standards that risk managers should also be aware of include ISO Guide 73:2009, *Risk management – Vocabulary*, which complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk. ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*, which focuses on risk assessment. And ISO/IEC 31010:2009, which focuses on risk assessment concepts, processes and the selection of risk assessment techniques.

Whatever stage risk managers have reached on their journey to implementing an enterprise-wise risk management process, the revised standard is likely to keep existing challenges in place. ISO 31000 looks set to remain the remain the industry benchmark for years to come. 🅴🆁

Directory

Insurance claims handling and risk management software

JC Applications Development Ltd is a market leader in the development and implementation of highly effective Risk Management and Claims Processing software. With over 25 years experience and a strong presence in both the Public and Commercial Sectors, our entire team is focused on ensuring that our risk management and claims management solutions are richly functional, cost effective, fit-for-purpose and with great support. We provide scalable, intuitive solutions for risk management, governance, and claims management that really work.

👤 **Phil Walden**

📞 **+44 (0) 1730 712020**

✉️ **phil@jcad.co.uk**

🌐 **www.jcad.co.uk**

📍 **JC Applications Development Manor Barn, Hawkley Rd Hawkley, Liss, Hampshire GU33 6JS**

Risk management technology

Riskonnect is an independent innovator and the only global provider of enterprise-wide risk management technology solutions. Built on the world's leading cloud platform, Riskonnect breaks down silos and unites the entire organisation by providing a holistic view of risk management. Through Riskonnect RMIS, Riskonnect GRC, Riskonnect Healthcare, and Riskonnect Safety, the company provides specific and configurable solutions needed to reduce losses, control risk, and increase shareholder value. Riskonnect's growing suite of risk management applications are built on a lightning fast, secure, and reliable platform you can trust.

👤 **Ross Ellner, Director, EMEA**

📞 **+44 (0) 7714 262351**

✉️ **ross.ellner@riskonnect.com**

🌐 **www.riskonnect.com**

📍 **Riskonnect Ltd. 52 Kingsway Place Clerkenwell EC1R 0LU**

Risk management software

Magique Galileo provides flexible and fully integrated web-based solutions for enterprise risk management, policy compliance, incident management, questionnaires, issue tracking and extensive reporting. Its web interface works with PC, laptop, iPad and other smart devices, enabling the whole organisation to participate in the risk management and assurance processes.

👤 **Trevor Williams or Verna Hughes**

📞 **+44 (0) 203 753 5535**

✉️ **info@magiquegalileo.com**

🌐 **www.magiquegalileo.com**

📍 **Magique Galileo Software Level 30, The Leadenhall Building, 122 Leadenhall Street, London, EC3V 4AB**

To advertise here contact: Clementina Christopher ✉️ clementina.christopher@theirm.org 📞 +44 (0)20 7709 9808

Specialty insurance solutions

Allied World Assurance Company Holdings, AG, through its subsidiaries and brand known as Allied World, is a global provider of innovative property, casualty and specialty insurance and reinsurance solutions. With 20 offices servicing clients throughout the world we are building a global network. All of the Company's rated insurance and reinsurance subsidiaries are rated A by A.M. Best Company and S&P, and A2 by Moody's, and our Lloyd's Syndicate 2232 is rated A+ by Standard & Poor's and AA- (Very Strong) by Fitch.

👤 **Enrico Bertagna**

📞 **+44 (0) 207 220 0707**

✉ **enrico.bertagna@awac.com**

🌐 **www.awac.com**

📍 **Allied World**
19th Floor, 20 Fenchurch Street,
London, EC3M 3BY

Risk management information systems

NTT DATA Figtree Systems is a specialist software provider for risk management Information Systems. Figtree Systems is used globally for incident and OH&S management, claims management, corporate insurance and employee benefits management, fleet and asset management and enterprise risk management. By using system features such as workflow automation, document management and creation, reports and dashboards, smartphone and web-based data-capture and email notifications, users have reported increased productivity, lowered costs and improve risk management processes. Easily configurable, the system is available in the traditional client-server model as well as a Software as a Service (SaaS) model from ISO 27001 compliant datacentres.

👤 **Ayaz Merchant**

📞 **+44 (0) 20 722 09210**

✉ **ayaz.merchant@nttdata.com**

🌐 **www.figtreesystems.com**

📍 **NTT DATA Figtree Systems**
Level 3, 2 Royal Exchange,
London, EC3V 3DG
United Kingdom

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

Become a Certified Member

and demonstrate your risk management excellence with:

- Proven risk management knowledge

- Verified years of practical experience

- Commitment to personal development

Find out more at:

www.theirm.org/certification

+44 (0)207 709 4125

membership@theirm.org

irm

News

CHARITIES GETTING BETTER

The IRM's Charities Sector Interest Group (CSIG) has released a new risk maturity framework and accompanying guide: CSIG's *Risk maturity framework* and *Getting better*, respectively.

This simple framework has been designed to help charities develop a plan for improving their risk management. It sets out four levels of risk maturity (conscious, developing, proficient and expert) and summarises what this means in terms of knowledge, skills and behaviours.

If you've just got started then you might class yourself as "conscious", although in some areas you might well be "developing" or even "proficient". But think about whether you actually need to be "expert" – most of us probably don't. It's a question of matching your risk capabilities to your likely needs. But if you rate "conscious" in all aspects of risk management, then you'll probably want to make some improvements. If you don't, you're likely to find that objectives and targets are missed or not met in full, simply because senior management are diverted to deal with unplanned events.

IRM's short guide explains how you can use the framework to assess your charity's risk capability and identify where you need to improve. This will help you focus your limited resources on developing the right areas – why insist, for example, that all staff attend risk training if actually the problem is just that you haven't effectively communicated and promoted your risk policy?

SAVE THE DATE – RISK LEADERS

Don't forget to save the date for the IRM's *Risk Leaders Conference* – Thursday 24th November, London. The focus will be on resilience and keeping your business fit for the future.

Our keynote speaker is General Sir Richard Shirreff KCB, CBE a former senior British Army officer. He'll be bringing his years' of senior military experience and overlaying that into the world of risk – from the battlefield to the boardroom – it's a must-attend event. Register here: http://bit.ly/25LJsAg

Sir Richard Shirreff

IRM'S CPD GOES LIVE

Get the recognition you deserve – IRM's Continuing Professional Development (CPD) scheme is now live. The scheme is relevant and applicable to all IRM members, whether you are studying, qualified, working part time or undertaking a career break.

Ultimately CPD will help IRM members and Fellow's attain Certified Member status and keep you current and competent.

CPD will become compulsory from 1 July 2016.

IRM DELIVERS TRAINING IN JEDDAH

Richard Cross recently delivered IRM training for ALJ in Jeddah, Saudi Arabia – with lots of positive feedback.

George Michael Shaw, CRA, CIRM, Managing Director, Risk Management, ALJ said: "Over the last two years we have had almost 130 risk champions and risk professionals participate in the Fundamentals of Risk Management training. The feedback that we have received is overwhelmingly positive, especially in terms of relevance and content. We have received great feedback, and the course is in high demand within ALJ. The course content is relevant and adds a lot of value to our daily work in managing the organisations risks"

To find out more about in-house training options please contact: sanjay.himatsingani@theirm.org or call +44 (0)20 7709 4114.

Richard Cross delivered IRM training at ALJ in Jeddah, Saudi Arabia

RISK APPETITE FOR BREAKFAST

Risk appetite is an amorphous concept, according to panelists at a recent IRM/Willis Towers Watson breakfast session on the topic.

It is a phrase often used but not always in the same way even with the same organisation. Agreeing a definition for risk appetite and the level of granularity it will be managed at was expressed as critical to embedding it.

Some firms view risk appetite as the cumulative effect of the entire risk management framework. A panellist shared that instead his firm defined risk appetite at the higher level board view of the world in broad categories i.e. market, credit, operational risk and how they interact with one another. This approach ensures the board is not involved in dealing with day to day risk decisions.

The ERM in Banking and Financial Services SIG is suitable for people working in banking, or associated financial services such as asset management. The group will be focusing on the challenges in this sector. More information can be found at: www.theirm

How ready are you for diversity in your business?

Achieving a more diverse workforce is a creditable aim and has been championed by high-profile businesses. But the transition can be painful

The recent immigration crisis in Europe is a good reminder that populations in developing countries are increasingly diverse today. But that diversity is not reflected throughout the workplace. For example, in the UK more than half of FTSE 100 companies have all-white boards of directors – and women hold only about 17% of directorships in those businesses. Talking about change is topical, but achieving it throughout the full organisation can be difficult.

Companies that have trodden the diversity route recognise that it involves hard work, money and ongoing commitment from the top management team downwards. Without the support of people at all levels of the organisation, such projects are likely to be a waste of everyone's time and money.

One success story can be seen in MGM Resorts International – the global hospitality group. In 2000, it launched its diversity programme during its merger with two other businesses. The initiative has scooped a bucketful of awards. The message is everybody's voice gets heard and good ideas are acted upon.

The naffly-named Diversity Champion Workshop was and is the catalyst for the company's transformation. No matter how senior, everybody in the company has to go through the process. People get to know each other. They form employee interest groups along gender, ethnicity, faith and sexuality lines – 15 at the last count. And Terri Lanni, the late chair of the then MGM Mirage, made it a part of the

William Perugini / Shutterstock.com

> 66 Diversity programmes can be transformative, but they risk flattening out the differences they aim to accommodate

business' strategy with planning meetings, KPIs, status reports and managerial compensation packages tied to how well diversity targets were hit.

Some universities in the US, on the other hand, are struggling with the successful outcomes of their own diversity efforts. In a recent article in the *New yorker*

magazine, the writer Nathan Heller spotted what he called an "ideological incongruity" that activist students had noticed, but that had passed by most of those working in the administration of Oberlin – a higher educational establishment known for its liberal reformism.

Oberlin was among the first to regularly admit women and black students to its courses. While it supports ideas such as intersectionality – which confers authority to people on the basis of their experience from culturally marginal backgrounds in the classroom – it is at the same time grooming them for "old school entry into the liberal upper middle class." By supporting diversity, it is, in effect, helping to eradicate it. The students feel trapped by the need to be activists in a system that acknowledges their differences, without necessarily having the flexibility to properly meet their needs.

Such activism can seem to critics like consumer identity politics – the students just want to pick their identities and see them reflected in their courses. May be. But it does raise the more pressing issue of how you include diversity into an organisation in a meaningful way. Diversity programmes can be transformative, but they risk flattening out the differences they aim to accommodate.

So, the question is, how far are you willing to risk the fact that the organisation will change, even transform into something completely different? If you have achieved diversity without cultural change, perhaps you need to think about changing the culture of your diversity programme. ER

Get the Recognition You Deserve

Continuing Professional Development (CPD) is relevant and applicable to all IRM members, whether you are studying, qualified, working part time or undertaking a career break.

Being a risk professional brings with it a responsibility to maintain your competency by ensuring your technical and business knowledge and skills are relevant and up-to-date.

Maintain and enhance your knowledge and skills to complement both your current role and your future career progression.

What's in it for you?

A planned, structured approach to your own personal development will help you:

- Learn new skills and keep up-to-date with the latest trends
- Perform better in your current role
- Gain a competitive edge and improve your future employment opportunities
- Increase your self-confidence
- Enhance your professional reputation
- Achieve tangible evidence of your commitment, competence and professionalism

Ultimately CPD will help you to attain Certified Member status and keep you current and competent.

Compulsory from 1st July 2016.

Contact IRM for further details or visit:
www.theirm.org/membership/continuing-professional-development

irm

A perfect fit

IRM's team of experienced trainers deliver highly relevant, interactive and practical training to meet the needs of the risk profession globally

Tailored and bespoke training

Short courses and workshops are offered at a range of levels from new starter to senior professional covering a wide variety of topics.

As well as our popular public and off-the-shelf courses, we also offer effective and practical bespoke training. Tailored to your organisation's needs, we develop and deliver the right solution for you.

Our training incorporates organisation-specific case studies and creates a win-win for meeting both individual and organisational objectives. Our trainers will work closely with you to ensure the course's design, content and materials suit your needs.

"I just wanted to let you know that the CEO was extremely impressed by the course you ran. His exact words were "he loved the course as it stimulated lots of thoughts for him beyond the expected". Learning Consultant, Capital One.

Contact us: email: **training@theirm.org**

phone **+44 (0)20 7709 4117**

or visit **www.theirm.org**

irm