Enterprise Risk

Autumn 2017 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Grasping the nettle: public sector challenges / **Working in harmony:** getting in sync with NEDs / **Lessons from Solvency II:** thoughts from the regulator / **Extreme events:** a behavioural risk audit could help /

Adapting to change: Science and risk management have a lot in common, says NEST's chief risk officer Dan Davis

CDS

Cyber Data Solutions

Intelligent Risk Management
You can't Protect It, so **Insure It!**

You insure your Hardware; why not your critical data?

Data is an Asset

Your business-critical Data can be purchased and sold, stolen, lost, accidentally or intentionally damaged.

CDS Data Insurance protects the contents of your Hardware (your data) in the same way that your asset Insurance protects your (easily replaceable) Hardware.

Your Data is your most valuable asset. Lost data has a catastrophic, financially damaging impact whether it is stolen, subject to cyber-attack or the result of human error.

CDS Data Insurance enables your business to set the value of your data, which becomes the indemnity value in the insurance policy. If you lose your data or lose access to it, CDS will return the insured data to you or you will receive the indemnity value of the data.

80% of all **UK businesses hacked** in 2015, resulted in **13% of data being deleted** by Hackers

The potential for expensive loss and catastrophic business failure

Your company's data is highly likely to be its most valuable asset, so how can you insure against data loss when losing it could be such a catastrophe potentially causing business failure in months?

Cyber Security spending according to Gartner will exceed $81.bn in 2017 but are businesses spending their cyber security budget wisely?

90% OF DATA LOSS IS NOT CAUSED BY A CYBER-ATTACK

60% of all businesses that lose Data **will shut down within 9 months**

90% within **2 years**

Whilst Cyber Insurance provides some data protection in the event of cyber-attack, the financial coverage for this is limited and usually fails to cover, among other things Hardware failure, employee error or sabotage, etc., which represent over 90% of all data loss events.

Why is CDS Data Insurance different?

We cover ALL Risks. CDS Data Insurance is new and It offers an increasingly important, intelligent risk management solution for your business-critical data.

CDS Data Insurance enables you to identify and value your critical data via a simple intuitive online application form. You then place the data identified for insurance cover in an Insured Data Environment© (IDE) using one of our accredited BaaS Providers.

The data, once placed in the IDE is then insured and covered by the policy.

CDS partners provide outstanding data backup and recovery, managed services and risk management advice.

In the Winter publication learn more about CDS Data Insurance or if you would like to know more now, get a quote or apply for Insurance, please visit our Website or call.

Cyber Data Solutions Limited is a specialist insurance provider and owner of CDS Data Insurance© which is underwritten by Allianz, a top 5 global Underwriter.

Allianz

cdsDataInsurance.com - info@cyber-data-solutions.com or call 0207 416 6735

Cyber Data Solutions Ltd is authorised and regulated by the Financial Conduct Authority (FCA), registration number 764799, as an Authorised Representative of Genesis Special Risks Ltd, whose registration number is 311626.

Enterprise Risk

Autumn 2017

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
Clementina Christopher
clementina.christopher@theirm.org
Tel: +44 (0)20 7709 9808 Ext. 234

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

Developing ambition

Risk managers are often undervalued within their organisations. In our feature on the challenges risk professionals face in the public sector, that can be seen where departments have poor reporting lines to the chief executive officer, for example. Perhaps they are merged with other services such as internal audit.

Whatever the mechanism, the effect is the same. Risk management is sidelined. Readers of this magazine realise that without proper resources and access to management, risk management can be less effective.

But that should not be a cause for despair. It calls, instead, for renewed ambition from the head of risk and his or her team.

"The chief risk officer has to demonstrate how risk management can add value to the organisation," Samuel Kibaara says in the feature. That entails building a strong business case for risk management at the same time as refusing to be pigeon-holed as a compliance function.

Without a driving ambition to align risk management to the business' objectives and prove the function's worth by improving business processes and strategy, the success of the risk department could be compromised.

> **Without a driving ambition to align risk management to the business' objectives and prove the function's worth by improving business processes and strategy, the success of the risk department could be compromised**

Ambition is not something that is taught at business school. In fact, psychologists have done relatively little work on the subject. Some see it as the propensity to take ill-considered risks, others as a key tool for motivating positive behaviour.

Louis Cooper, writing in this issue, also urges risk managers to raise their sights. Given the changes to the corporate governance landscape in recent years, non-executive directors need to be more savvy about risk. As an expert in training non-executives, Cooper does not believe that enough risk managers put themselves forward for such roles.

The key to embarking on such a journey, he says, is to start early. Be ambitious enough to believe it is possible – then take the right steps near the beginning of your career to put you in the running.

Of course, plenty of risk managers *are* ambitious. Dan Davis, featured in our cover story, for example, was already sitting on a board as head of risk at 27 years old. Perhaps not everyone can achieve those heights so early. But what's the harm in trying?

Arthur Piper
Editor

Contents

Autumn 2017

10

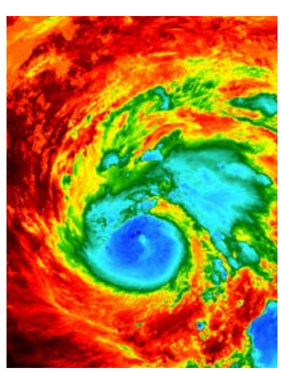
14

18

FEATURES

REGULARS

22



26

30

Do you have a Real-World Interface?

riskHive's new 'Real World Interface' for the riskHive ERM application links to and monitors any number or type of external data sources and connects them as Key Risk Indicator (KRI) inputs to warn of or trigger automatic risk response processes. From negative tweets to dipping rates to weather warnings. We've got it covered.

riskHive ERM is a secure, simple and highly configurable ERM Portfolio solution that aligns to and helps define your processes, delivers instant results, requires minimal formal training and scales-up effortlessly.

Whether you're just starting-out on your risk journey or are already expert and require more advanced capabilities the riskHive ERM solution will help ensure a successful implementation of your ERM strategy.

"We demand a return on investment for all our systems. Choosing a risk management system was no different, and we selected riskHive on the grounds that they were able to demonstrate to us that they understood exactly what we were looking for and we had the confidence that they would deliver. They have not only delivered, but continue to engage with us to enable us to drive our ERM agenda."

Rebecca Cope-Lewis DipQ MCQI CQP CIRM
ERM Director, Mitie Group PLC.

Find out more at www.realworldinterface.com
or contact us for a demonstration of riskHive

info@riskhive.com
+44 (0)1275 545874
+44 (0)781 8898997
www.riskhive.com

riskHive™
THE RISK MANAGEMENT COMPANY

A career in risk management

As Paul Hopkin steps down as IRM's technical director, he reflects on how the profession has transformed over the past forty years

Retirement is a great opportunity to reflect on the various stages of my career in risk management, which has lasted more than 40 years. These stages have occurred in parallel with significant developments in the practice of risk management. Those of you familiar with the textbook *Fundamentals of risk management* will be aware of my passion for acronyms.

In the fourth edition of the textbook, I introduced a new acronym, FOIL – fragmented, organised, influential and leading. FOIL represents increasing risk management sophistication and is a roadmap for my career over the past 40 years. And it identifies how risk management can be implemented within a company.

After a brief period teaching physics and mathematics in a secondary school in Bristol, I took a job as a government safety inspector. I specialised in health and safety in foundries in Birmingham – the industrial heartland of Britain. The regulatory approach was necessarily *fragmented* at the time, but many companies followed the same model of fragmenting their risk management systems to respond to the requirements of different regulators. Therefore, health and safety became a specialist area of risk, despite the potential for conflict with environmental, quality and production requirements.

After eight years as a safety inspector, I moved into the insurance industry at a time when a more combined approach to risk management was developing. This encouraged companies to better *organise* their risk management efforts. Often, the result was that health and safety and environmental departments combined, and closer working with the quality department was encouraged.

The aim was not just to include the specialist areas of expertise in, for example, health and safety, environmental or quality, but also to have an overall combined or organised approach to risk management that would be mutually supportive and more effective. The ultimate objective was to undertake risk management in a way that it influenced the behaviour of senior management and thereby enhanced the success of the company.

My next move was to a large PLC called BET, now part of Rentokil Initial. It was a substantial conglomerate of companies working in different sectors, including leisure, construction, transportation and security. Under the influence of a strong-minded CEO, a loss-control initiative was launched. This resulted in risk considerations *influencing* the way in which businesses operated.

The loss control initiative placed requirements on the group companies to reduce risks and, in particular, reduce the potential for inefficiency and insurance claims. This led to reduced costs, increased efficiency and added to overall success. The requirement to develop measurable loss control programs was highly influential and reduced insurance losses by 25% over a two-year period.

> **A career in risk management offers the chance to make a difference and leave a legacy**

Since leaving The Rank Group, I have seen the further development of risk management as technical director at Airmic and, more recently, at the Institute of Risk Management. Risk management is increasingly *leading* business decision making. Enhanced risk management practices are helping companies validate their business models in terms of the risks that the business model embraces.

The ultimate challenge for risk professionals still remains and that is to ensure that risk awareness guides decision-making at board level. A career in risk management offers the chance to make a difference and leave a legacy. Not many other in-house positions offer the same opportunity to explore every aspect of the business model of the company.

Paul Hopkin recently retired as IRM's technical director.

Trending

DATA

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

Full English

Businesses have heads in sand over the impact of Brexit

43%

Less than half of businesses say they have assessed Brexit risks

29%

Less than one third have made plans for leaving the EU

21%

Less than one quarter say they are willing to explore new markets

Source: ICAEW

EVEN THOUGH

8%

Less than 8% of chief finance officers expect a positive outcome

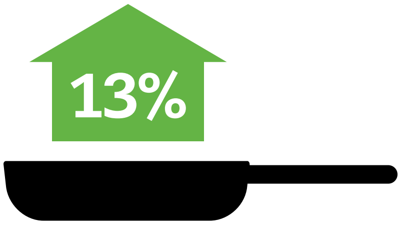
43%

And, the top worry is economic and financial uncertainty

Source: Deloitte's CFO Survey

Most trivial Brexit risk?

The price of a full English breakfast could rise by



Source: KPMG

Lack of training and skills top risk for IT security projects

Application security program implementations are an issue for almost three quarters of businesses. What challenges do you face in implementing an application security program?

41%
Lack of skilled personnel or training

16%
Little or no budget

18%
Lack of management buy-in

25%
No challenges

Source: Synopsys

Boards fail to support data law changes

General data protection regulation (GDPR) will affect pofitablity of business **62%**

IT-decision makers with board support for implementing GDPR **31%**

Source: Calligo

While other executives do not know whether GDPR affects them

40%
Number of organisations globally that believe they will be affected by GDPR

39%
The UK has the lowest level of awareness that GDPR is a compliance issue

25%
Number of US executives who understand that GDPR will affect compliance of data they hold on EU citizens

Source: 2017 Risk:Value report, commissioned by NTT Security

Adapting to change

Science and risk management have a lot in common, says NEST's chief risk officer

BY NEIL HODGE

Making the move from studying animal biology to analysing business and operational risks may seem like a fantastic leap for most people, but Dan Davis sees it as a natural step and part of his own evolutionary process.

After completing a degree in zoology at the University of Nottingham in 2006, Davis moved to London and started work at Citibank. In 2008 he took his first steps into a career in risk management when he moved to Network Rail as a risk and value analyst, working on one of London's biggest and most complex infrastructure projects – the Blackfriars Station and Bridge reconstruction – which was part of the Thameslink Programme.

In 2011 he took on his first full-time risk management role at transport and infrastructure company Thales, working on the Jubilee and Northern Line signalling upgrade project.

"I learned a lot about risk management from my time at Network Rail and Thales," says Davis. "The engineering projects I worked on were very complex, and as the work progressed new risks would emerge, and the approach to how risks were managed would need to change. It was highly fluid and we had to adapt as necessary. That

> The engineering projects I worked on were very complex, and as the work progressed new risks would emerge, and the approach to how risks were managed would need to change

experience has certainly informed the way I look at risk management and how projects are run," he says.

Easily understood

Davis joined the National Employment Savings Trust (NEST) Corporation, the organisation that acts as trustee to the government's defined contribution workplace pension scheme, in July 2012 as executive director of risk. At the age of 27, he was probably one of the youngest risk professionals to ever sit on a board. Last year, the job title – though not the role – changed to chief risk officer (CRO), because, he says, "it was more easily understood." As CRO, Davis oversees a team of 14 people spread across four risk assurance functions – compliance (which is the largest), enterprise risk, corporate technology and institutions (which looks after building maintenance and facilities). As he sits on the executive team, Davis reports directly to the chief executive, with a "dotted line" to the chair of the risk committee.

Fortuitously – or unluckily, depending on one's viewpoint – his appointment was just three months before auto-enrolment came into effect. "Talk about hitting the ground running! When I started, NEST was going through a kind of project start-up phase and was getting ready for October when auto-enrolment would begin. It was clear that the organisation wanted someone with a lot of experience of working on complex, long-term projects where plans would often need to change quickly, and this excited me from a professional point of view. The scope of NEST's work presents some unique challenges, and that's what attracted me to the organisation."

NEST is responsible for just one financial product – a defined contribution workplace pension scheme that employers can use for auto-enrolment. Set up in 2010, it is there to support the automatic enrolment programme, which came into effect the following year as part of the government's workplace pension reforms under the Pensions Act 2008. As part of the legislation, every employer in the UK must now provide access to a pension scheme for their employees, automatically enrolling eligible workers and making contributions to their pensions (though employees can decide to opt out). Companies can set up and manage their own schemes, but for those that do not want to, they can choose an established scheme – and NEST is one of them. As it was set up by the government, NEST has a public service obligation, which means that it must accept all employers that choose to use it. It reports to parliament through the Secretary of State for Work and Pensions, but it is generally independent of government in its day-to-day decisions.

NEST now has 5.3 million members and close to £2 billion worth of assets in its scheme, and acts on behalf of 400,000 employers. It continues to sign up 1,000 companies per day that want to join the scheme. NEST's success is a risk

> **Risk management needs to understand the business and the strategy that the board wants to deliver, and work out how it can help the executive achieve those aims**

in itself. "We need to ensure that we have the resources, skills and infrastructure to deal with demand. We have a public service duty to act in people's best interests, and given the sheer volume of new employers and members signing up to the scheme, we need to make sure that we continue to operate as effectively as we have done so far," says Davis.

NEST is currently funded by a loan from the Department for Work and Pensions (DWP). When the government gave NEST a public service obligation to accept all employers, it set out a funding plan that saw it initially draw on a government loan until it becomes self-funding. NEST currently owes £539 million, which is in line with the loan agreement. Projections show that within 12 years NEST will pay back the loan, standing on its own feet in 2038, when it is expected to fund its own operations through member fees rather than public money – all being well.

Payback time

Davis is philosophical about the organisation's future. "When NEST was set up I doubt anyone had a very clear idea of what the take-up would be. The fact that so many companies want to join the scheme is a testament to how well run it is and how well regarded it is. It will not rely on government money forever, and what the organisation does owe will be paid off," he says.

Due to the high-profile nature of the organisation – as well as the level of public and commercial scrutiny it is subject to – robust risk management is a priority. Davis has put in place a risk management framework that is reviewed each year to ensure it remains fit for purpose, as well as to take into account developments in industry practice. At the core of this framework is the risk management process. Each business area across NEST maintains a log of their key risks, which they review regularly, says Davis. This risk dashboard is then used to report key risks to the executive board, risk committee and NEST in its role as trustee.

Principal risks

NEST has identified several principal risks to the business. The first is that the organisation doesn't have sufficient levels of operational capacity to conduct its day-to-day operations, so ensuring there are appropriate resources and that the systems are working properly is paramount. Poor decision-making and investment implementation by the organisation's scheme and fund administration providers could also put the scheme at risk, so maintaining a strong relationship with them and having appropriate procedures in place to gain assurance on how they act on NEST's behalf is important.

People risk is another major concern for the organisation, says Davis. "If we don't recruit the right people, nurture the right organisational culture, and design and implement effective processes and systems, we could face higher operating costs, increases in errors and losses and the reputational consequences of these events," says Davis. To help prevent this, NEST undertakes an annual staff survey to gauge feeling across the workforce and take steps to address low scores and improve staff engagement. It also supports employees' professional and skills development.

Protecting member assets and data is also vital. In 2013 NEST was hit by a £1.4 million fraud when a supplier payment was diverted. No

> Organisms have to evolve in order to stay as they are. The same is true of risk

member money was touched (it was the organisation – rather than the scheme – that was affected), but it was a warning that internal controls needed to be strengthened. Davis says that information security and cyber-risk are taken very seriously, adding that the organisation's systems are independently certified to ensure compliance with ISO 27001, which is the key standard for information security management.

Another potential risk is that NEST could be adversely affected if significant legislative, regulatory or policy change occurs. "Any changes to the law, financial regulation or government policy could have an impact on the work we do and the service we provide, so we have to keep track of these developments and be prepared to respond as necessary. As with any organisation, resourcing is always an issue, so trying to look ahead and plan ahead as far as possible is important," says Davis.

Keeping it simple

Davis says that the main consideration of ensuring NEST's success is to "keep it simple". "The service that NEST offers needs to be simple to encourage companies – particularly small companies – to sign up to it, so the online service needs to be very user-friendly. We also need to use very clear wording about what the scheme does, and how it works," says Davis.

"However, the technology that enables the service is anything but simple; it is very complex and it needs to be robust and secure enough to deal with a thousand new applications per day. That's a lot of capability and it is our job to provide the board with the necessary assurance that the IT, processes and controls are fit for purpose."

Davis believes that risk management has a major part to play in delivering NEST's strategic vision. "The risk function is there to help management achieve its objectives. Risk management needs to understand the business and the strategy that the board wants to deliver, and work out how it can help the executive achieve those aims, while at the same time alerting it to the key risks that may hamper that progress."

Davis says that much of his attitude to risk management is rooted in his science background. There is a scientific concept, says Davis, called the "Red Queen" hypothesis, taken from Lewis Carroll's novel *Through the looking-glass*, where nature has to constantly change to survive. "The point is that organisms have to evolve in order to stay as they are. The same is true of risk: it does not stay the same. It can change over a period of 12 months to become more impactful, even though it is termed the same risk as before. Other factors – changes in the marketplace, regulatory issues, financial concerns – may have had an impact. So, unless you are going to conduct ongoing risk assessments, you will not be aware of the factors that are changing the nature of the key risks to the organisation," he says.

Outside of work, risk still plays a major role in Davis' extra-curricular pursuits. A keen sailor, Davis is set to take part in two legs of the Unicef Round the World Yacht Race. The first leg, which will take about a month to complete, starts in mid-September and will see him be part of a 20-man onboard team that will sail across the Atlantic from Uruguay to Cape Town. The second leg, which will last around another five weeks, will be in June next year and will involve sailing from New York to Derry and then on to the finishing point in Liverpool.

"I can't wait to give it a go, even though I have little idea what to expect. Sometimes you have to just jump in and take a risk," he says.

Neil Hodge is a freelance journalist

Grasping the nettle

Risk managers in the public sector are often underfunded and overworked. But new guidance and a push for greater clout could boost their effectiveness

BY SARAH WINT

At the same time as the UK government has been cutting costs in central and local governments, the impact of risks that do crystallise seems to be intensifying. For example, major cyberattacks earlier this year brought to a standstill several high-profile NHS hospital trusts. Not only did the healthcare providers have to get their systems back online, but they simultaneously had to deal with the mainstream and social media storm that followed.

Risk managers might believe they need to work harder to make sure all possible scenarios are covered. But they would be letting themselves in for an endless and futile task.

"If you're trying to do analysis of what can go wrong in government departments, you can get into thousands of risks," says Trevor Llanwarne, a former government actuary turned consultant. Not only that, so-called black swan events are, by their definition, unpredictable with potentially catastrophic effects. Non-executives in the industry were asking Llanwarne how it was possible that risk management departments could produce 50-page risk registers yet fail to see some of the major catastrophes that hit their organisations.

"If you're trying to do analysis of what can go wrong in government departments, you can get into thousands of risks

Resilience

An analysis of risk registers showed that they worked well for internal risks which could be managed through internal controls. But there were three other types of

Image credit: John Gomez / Shutterstock.com

risk for which this approach was unsatisfactory – external, strategic and project. There was also a particular concern about internal risks for which there could be thousands of possible, different occurrences. In practical terms, Llanwarne says, each one of those thousands of items is very unlikely to happen – but the chances of any one of those events happening is quite reasonable. Putting in place risk analyses for thousands of small items, each of which has a very low likelihood of ever materialising, is madness, he says.

Llanwarne turned the problem on its head. In relation to external risk, he believes departments should focus on resilience and what gets impacted no matter what the cause. There are only a few types of impacts that are relevant. Typically those entail either reputation, people, infrastructure, finance or operations. "Departments should ask themselves, if something does blow up, how resilient are they to it?" he says.

Llanwarne's response has been to work with a cross-government steering group to write a new risk management framework – *Management of risk in government*. This is intended to help risk professionals in government departments – and elsewhere in the public sector – get to grips with the tsunami of threats facing their organisations. Instead of trying to identify the thousands of potential external risks that could impact on the working of government, the guidance puts resilience at the heart of risk management.

The framework categorises risks as belonging to four major, sometimes interconnected, causes: internal, external, strategic and those that derive from major projects (see box, *Management of risk in government*). The guidance advises risk managers to produce regular reports to the board on the organisation's general approach to managing each type of risk. In addition, the reports should highlight the organisation's most significant risks and what

“ Risk managers in public bodies are all too often not given direct reporting lines to the CEO or executive board

MANAGEMENT OF RISK IN GOVERNMENT

Type of risk	Features and approaches	Examples
Internal	These are risks over which the organisation has some control, for example risks that can be managed through internal controls and mitigating actions. This often involves traditional risk management, such as risk registers, controls and assurance.	• Fraud • Health & safety • Capacity & capability • Data security • Delivery partners
External	This focuses on big external events/perils and then considers how to make the organisation more resilient to such events, in part because of the difficulties of assessing likelihood. A tried-and-tested approach to managing external risks is through considering the impact those external events could have on infrastructure, finance, people, operations and reputation.	• Economic downturn • Terrorist attacks • Extreme weather • Cyber attacks
Strategic	This third element concerns the organisation's raison d'etre and key objectives, identifying the principal risks to the achievement of those within a set time frame. For some, this could be the lifetime of a parliament. Risks in this area would be accompanied by regularly monitoring and adjusting interventions, as necessary. Forward-looking charts are often helpful here.	• Immediate impact risks to the organisation's ability to continue operating, eg loss of customer data; or • Slow-burning risks that grow and eventually prevent delivery of objectives, eg staff turnover
Major projects	Major projects form such a critical part of the plans for many government bodies. Experience suggests that one or two critical projects for that organisation should be considered at board level in their own right. The key is to only report to board level on the two or three that really matter. This should be via whatever tools, techniques and reporting are appropriate for each. These risks will be specific to the major project in question and could involve:	• Shifting requirements • Slippage in delivery time frames • Failure to deliver

> The chief risk officer must build a strong business case for risk management and overcome the challenge of simply adopting a compliance-model approach

is being done to address them.

"This approach builds on the successful new framework championed by the Financial Reporting Council for the private sector," says Llanwarne, "and can lead to a comprehensive management of an organisation's risks."

Reporting lines

The framework should be helpful where the relationship between risk managers, executives and non-executives is robust. But that is not always the case in the public sector.

"Risk managers in public bodies are all too often not given direct reporting lines to the CEO or executive board," says Marie-Gemma Dequae, who works with risk management in the public sector in Belgium and the Netherlands and is advising the Federation of European Risk Management Association (FERMA). "Without direct reporting lines, it is difficult to convince top management of the benefits of risk management."

So, how can this be overcome? Dequae says while it is a difficult issue to resolve quickly, risk managers can start by making sure that their work is directly targeted towards the improved performance of their organisations. They need to get themselves invited to attend management and strategic committees so that they know what is happening throughout the entity.

"Risk managers have to build their reputation and become visible in an organisation so that people think of them when they have a problem," she says.

That also involves overcoming the kind of silo thinking – where departments act as isolated parts of the business – that has built up in many organisations. "Risk managers need to develop a more collaborative way of bringing people together in order to show that there is a better way of working on risk issues," she says. Some risk professionals may find that uncomfortable at first, but she urges them to get out of their comfort zone to listen and consult with colleagues in order to help them resolve their problems.

Working through scenarios can be a great icebreaker. “Risk managers really have to leave their office and talk to people and try to convince them to consider scenarios and work together for the benefit of the organisation,” she says. Heads of risk should ensure that their staff are well trained in communication and interpersonal skills from day one.

Structural issues

“If decision makers within the public sector do not appreciate risk management, they will continue to treat it as a peripheral function and view it through the same lens as internal audit,” says Samuel Kibaara, a former senior risk officer at Kenya Power and now a director at Pinebridge Training and Consulting. He is frustrated with the practice within many organisations in East Africa where little distinction is made between risk management and internal audit.

“Some risk managers have doubled up as internal audit managers and that puts the brakes on risk management implementation,” he says. “They have not been given the proper clout to enable them to be part and parcel of strategic decision making within the organisation.”

Kibaara says the problem is serious because, without proper reporting on enterprise-wide risk management, top management will fail to appreciate the benefits a dedicated risk function can bring. For risk management to focus on compliance is not the answer.

“The chief risk officer has to demonstrate how risk management can add value to the organisation,” he says. “He or she must build a strong business case for risk management and overcome the challenge of simply adopting a compliance-model approach.”

Kibaara feels that better training for risk managers is needed to raise standards. Most risk managers come from an accounting or audit background and require training on how to implement and organise a risk management function within an organisation. Training in technical issues needs to be balanced with courses that boost soft skills – interviewing, listening, presenting and running workshops. Staying ahead on strategic risks such as cyber security, climate change and big data is also important and helps bring the department to the attention of senior management. But risk managers also need to be up to speed on the strategy and future plans of their own organisations so they can talk knowledgably with top management.

It is a tough ask, especially since the public sector in East Africa is generally perceived as being slow on the uptake concerning any new knowledge. Coupled with a correspondingly slow pace of organisational change, risk managers can struggle to take the necessary steps to improve their situation.

Kenyan code

On the plus side, the public sector in East Africa is growing, and it is a driver for growth in the risk management profession, says Kibaara. In addition, Kenya’s *Corporate governance practices code* of 2015 is beginning to bite. It requires all directors of state corporations to go through training, which includes aspects of risk management. This means that risk management is now being viewed more seriously, he says.

Kibaara says risk managers should push while the door is opening by creating more opportunities for executives to hear about risk management.

“At every monthly executive meeting, there will always be a risk issue that is affecting the organisation at that point in time,” he says. “The risk manager needs to package that from the point of view of what the risk perspective is and what opportunities can be derived from it.”

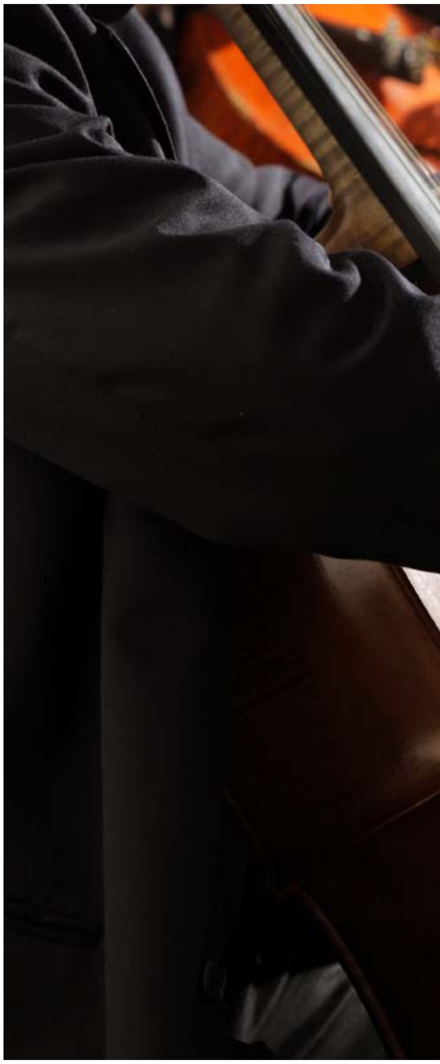
He says that initially it may look like risk managers are trying to be in on everything. “But the tide will change and management and the board will start insisting that they need risk management input in every project or opportunity,” he says. And when that day comes, risk managers will be ready.

Sarah Wint is a staff writer and editor

Above: Nairobi the capital city of Kenya, East Africa, where the public sector is driving growth in risk management

> **Risk managers have to build their reputation and become visible in an organisation so that people think of them when they have a problem**

Working in harmony



Learning how to work well with non-executive directors could help to improve the performance of the business and provide valuable career lessons to aspiring risk managers

BY LOUIS COOPER

The role of the non-executive director (NED) is well defined by the Financial Reporting Council as part of one of the essential principles in the UK Corporate Governance Code: "Non-executive directors should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible."

The NED role is therefore typically defined by the key pillars of governance, strategy, finance and risk. Risk management should be one of a NED's specialist subjects and one that they are comfortable in providing insight into and direction on. In reality, this is not always the case, and some boards of directors may be organised on the basis of individual NEDs having responsibility for certain areas of corporate activity, rather than being an expert in all of the key areas.

> NEDs can work with risk professionals to help shape their organisation's approach to managing risk

NEDs in action

The day-to-day role of the NED is both challenging and critical. But only being part-time in the business, it can

be difficult to understand fully all of the issues and to feel an integral part of the organisation. If you just attend board meetings, you can feel a bit of an outsider. NEDs do rely heavily on executive management to provide accurate and relevant information, and there are examples where NEDs might feel that the information they receive is selective and watered down – more later.

The input of NEDs may also depend on the life cycle of the organisation and whether an organisation is in steady-state, expansion or crisis mode. In a steady-state environment, the board generally will adopt a passive-monitoring approach. However, more proactive and direct intervention may be needed when an organisation is growing rapidly or if it is having to respond to challenging internal or external circumstances.

NEDs and risk

NEDs are appointed based on their knowledge and experience. They should bring to the board a range of different perspectives and provide an independent, broader view drawing on their previous roles and responsibilities. The ability to benchmark the organisation's approach to certain situations acts as a positive challenge to executive management's thinking.

The risk agenda may also be considered in a similar way, and a NED's approach to certain key risk drivers can help guide and shape good practice. In particular, questions can be asked to explore the response to a number of topical risk concepts (see *Key risk questions*).

All of these areas are further developed in the IRM training course *Risk in the boardroom*. They help to position risk management as a strategic activity and, by sharing their insight, NEDs can work with risk professionals to help shape their organisation's approach to managing risk.

Working together

NEDs and risk managers should be working to promote and progress the same risk agenda, but interaction may be confined to contact through attendance at risk and/or audit committee meetings – depending on the size, complexity and governance structures of the organisation. NEDs will be reliant on the reports and information presented at such meetings. The committees and the board itself will have a particular attitude to dealing with risk reports and how they are used in decision-making processes.

The type, quality and frequency

of information received is central to the committee and board's ability to fulfil its governance role. Risk reports prepared by risk managers may be summarised and condensed by the executive team or may need to be reformatted based on board paper preferences. For example, words and narrative may be preferred to diagrams and charts, or vice versa. Other areas to consider might be whether the organisation is measuring the right things (key risk indicators). How dynamic is the organisation's approach to risk – has it just become routine? Is there an issue with the volume of data to sift through and interpret? Are senior managers seeking to supply information that clearly supports a particular narrative? And are NEDs taking an accepting, passive approach to the information presented, rather than using it as a mechanism to explore options and question management?

Risk managers need to be on the front foot and tailor their reports to different stakeholder needs. Stakeholders might include the board, various committees, NEDs, regulators, and audit and compliance teams. The use of technology to support the reporting and monitoring process can also reach a tipping point with the move from flat spreadsheet lists to more data-rich relationship databases that enable trend analysis techniques and provide the opportunity to run pre-defined reports at the touch of a button.

Lines of communication need to be two-way. Typically, information flows up the line, but often there is little feedback or understanding of how risk information has been used and decisions made. Much will depend on who attends board and committee meetings to present reports and who, if anyone, sponsors risk and performs the role of chief risk officer in name or deed. Those organisations that take risk seriously will also introduce a degree of value measurement of risk management itself, which as well as promoting the value of the work undertaken may in turn enable a cycle of continuous improvement.

KEY RISK QUESTIONS

- **Risk maturity:** What is our level of maturity? When did we last review our current v future state position? Are we on a cycle of continuous improvement?
- **Risk culture:** What is the risk culture of the organisation? How does this compare to the overall organisation culture?
- **Risk appetite:** Have we got a clear articulation of our appetite for risk across all areas of the organisation? How do we as a board communicate and reinforce this?
- **Risk opportunity:** How do we balance the negative threats with the positive opportunities we need to grasp? Have we utilised simple strategy techniques such as SWOT analysis?
- **Reputation risk:** How do we cope with a crisis situation? How do we make sure that things do not spiral out of control?
- **Extended enterprise risk:** Have we mapped our extended enterprise risk position to consider any sensitivities and threats in our strategic and operational supply chain?

> A NED's ability to benchmark the organisation's approach to certain situations acts as a positive challenge to executive management's thinking

A friend in need

The loneliness of the NED is a theme that serves to emphasise how some NEDs can feel. While all directors, both executive and non-executive, are considered as one in legal terms and should come together as a team, the nature of the role if done properly can be tough. While being the independent voice, NEDs do need to have a support network in the organisation. In order to foster this, they also need to have greater visibility and be seen to operate outside of the boardroom –walking the floor is a recognised feature of keeping in tune with the business and in understanding how it ticks.

NEDs also need to keep their own continuing professional development and technical training up to date. This area often lacks any structure or formality as NEDs are left to their own devices. Establishing ongoing contact with the risk function can help NEDs to update their knowledge and skills; while keeping current, they can also help to identify emerging risks and focus on the areas that may take the organisation away from achieving its objectives.

The problem a lot of NEDs face is the amount of time they put into the role – contracted hours are often less than those required to do the job, especially where internal and external expectations are much higher and the thickness of board-packs has expanded threefold. A degree of personal investment of time is required, and spending time with the risk professional can provide a broader understanding of critical business issues which have a direct impact on delivering the strategy – one of the other main responsibilities of the NED. Conversely, this interaction may also help the risk professional in terms of reassessing and plotting their own career progression.

The risk professional as aspirant NED

Boardroom diversity continues to be a hot topic, especially from an age, experience and new-skills perspective. More younger executives should be given the opportunity to take on external NED roles at an earlier stage, and

SIX STEPS ON THE ROAD TO BECOMING A NED

1. **Start early, set your objectives and make a plan.** What are your strengths and weaknesses? Plug any gaps with extra training or education. Look at the Essential training courses offered to aspiring NEDs by the Non-Executive Directors' Association

2. **Start with small steps.** There are a range of NED-related roles in a variety of organisations such as schools, charities and sports bodies. Consider what your interests are and where you can gain some useful initial experience in a non-threatening environment

3. **Re-write your CV.** Look at your CV in the light of taking on a board-level role. You will need to revamp and reshape the document to sell your value. It will be a very different CV to your current employment model and may help in highlighting gaps and development areas

4. **Get your current employer to sponsor you.** Look to get on the ladder early and ask your employer to support you – it will help your development and bring new ideas back into the organisation. A number of organisations are building this into their talent programmes

5. **Raise your level of networking.** NEDs must network, network and network. The trick to finding out about the right opportunities – and which ones are realistic – is to adopt a methodical approach about who can help you. Think about who you can approach to ask for help, especially reactivating past contacts and thinking more broadly about new ones

6. **Find a mentor. Talk to a NED in your organisation.** They might be able to help or know where to get some advice and find the right person for you.

risk professionals are well qualified to do this. The mantra from the 2016-17 Non-Executive Director Awards was that "the need to populate British boardrooms with able, diverse and enthusiastic NEDs is more important than ever".

Risk professionals can respond positively to this statement and have a head start on a number of other professionals, given risk is a key element of the NED role (see *Six steps on the road to becoming a NED*). The skills and attributes of a risk person align well with the requirements of being a NED (strategy-led, financially literate, enquiring mind, good communicator and listener). Risk professionals should be stepping up to the plate to perform NED roles – to date they have not been encouraged to do so and often lack confidence, hiding their light under a bushel.

Louis Cooper is the chief executive officer (part-time) of the Non-Executive Directors' Association, a freelance risk consultant and a member of the IRM's Innovation Special Interest Group. For more information on being a NED, contact Louis via: louis.cooper@nedaglobal.com.

> Risk managers need to be on the front foot and tailor their reports to different stakeholder needs

Learning lessons from Solvency II

There are lessons to learn for insurers in implementing Solvency II, as the European Insurance and Occupational Pensions Authority (EIOPA) discovered when it undertook the first analysis of progress since the regulations started

BY GABRIEL BERNARDINO

The application of Solvency II to insurers from January 1, 2016, signalled a shift in the assessment of solvency, moving to a preventive and risk-based approach. While Solvency II introduced new requirements relating to capital management and disclosure, it also established governance and risk management as a central pillar of the framework.

Historically, studies of insurance failures have shown that the primary causes of failure have been as much about poor management and inappropriate risk decisions as they have been about inadequate capitalisation. This demonstrates that in risk management, *management* is just as important as *risk* and makes the risk management function one of the most important functions in insurance governance systems.

Solvency II requires all insurance and reinsurance companies to have an effective system of governance – including risk management – in place, which is proportional to the nature, scale and complexity of the business.

> **Board members should possess risk management skills and sound risk management procedures**

> The risk management function is one of the most important functions in insurance governance systems

Risk and the board

An effective risk management function is one that assists the board and other functions in the operation of the risk management system, monitors the risk management system and the risk profile, reports on risk exposures and advises the board, and identifies and assesses emerging risks.

With Solvency II, companies are expected to adopt the necessary changes in their organisational structure, so that the risk management function can effectively comply with its tasks, with operational independence and with direct access to the board. In particular, the risk management function needs to be sufficiently resourced and staffed by professionals with the right level of risk management skills. Similarly, board members should possess risk management skills and sound risk management procedures, integrated into a comprehensive framework with proper documentation in place.

ORSA – making sense of risk

In addition to the greater focus on the overall risk management function and the capacity of board members to integrate risk into their strategic decisions, Solvency II also calls for a more forward-looking approach to risk management. This means that insurance companies must also consider any future developments that might have an impact on their business, such as business expansion plans. The *Own risk and solvency assessment* (ORSA) is a powerful risk management tool that sets out the principles of forward-looking self-assessment of risk management and solvency for insurers.

ORSA encourages a more holistic view of risk, both quantitative and qualitative, and favours a more in-depth look at the whole business, rather than focusing solely on financial risk.

While ORSA acts as an internal assessment process within the undertaking and is therefore embedded in the organisation's strategic decision-making process, it also acts as a supervisory tool for national supervisory authorities, since insurers must keep supervisory authorities informed of the results of ORSAs.

EIOPA's role

One of the most important strategic objectives of EIOPA is to achieve consistent supervisory practices, and EIOPA monitors the implementation of Solvency II with particular attention to the governance system, including risk management.

To foster a higher level of conduct of supervision, EIOPA has developed a supervisory handbook of good supervisory practices related to Solvency II, with chapters covering the roles and responsibilities of board

EIOPA expects board members to use the ORSA results in their strategic decision-making process to enhance the overall risk management of undertakings

members and key functions, as well as ORSA governance.

EIOPA has also conducted an analysis on the implementation of ORSA based on the supervisory assessments conducted by national supervisory authorities. This analysis provides a first insight into national experiences with the supervisory assessment of ORSA and points to areas for further improvement.

State of play

EIOPA's analysis shows that while insurance and reinsurance companies are making good progress in implementation, there is scope for further improvements.

Most undertakings have made good progress in implementing ORSA processes and policy. In particular, during the last few years, the vast majority of insurers have established well-functioning internal processes that allow the right people to be involved in and take responsibility for the conduct of ORSA.

EIOPA has seen, however, that small insurance businesses tend to face more challenges in implementing and applying ORSA processes. This encourages them to further elaborate on ORSA processes including their ORSA policy and the quality of data used in assessments.

Room for improvement

In its analysis of ORSA implementation, EIOPA has observed a number of areas for improvement, notably the need for a greater involvement of the administrative, management or supervisory bodies. In this regard, EIOPA encourages insurers to improve the involvement of their administrative, management or supervisory bodies in the ORSA process. Board members are expected to follow the top-down approach and to play an active role in the ORSA assessment. EIOPA expects board members to use the ORSA results in their strategic decision-making process to enhance the overall risk management of undertakings.

There is also scope to further expand risk assessment. According to ORSA requirements, undertakings should assess all current or potential material risks, including those that are not quantifiable. The findings show that risk assessments do not always include all potential risks and, in many cases, the assessments are not linked to the business model and strategic management actions of the undertaking. Therefore, EIOPA calls upon insurers to widen the scope of their risk assessment and to deepen the risk analysis.

EIOPA's analysis indicates that there is an overreliance on the standard formula by undertakings. In addition, the assessment of the significance of the degree to which risk profiles deviate from the assumptions underlying the solvency capital requirement under the standard formula should be further improved. EIOPA expects all organisations to perform an assessment of their specific risk

> **Effective governance, like risk management, is not a tick-box exercise; instead good governance is one of the best tools to enable sound business practices**

profile when calculating their overall solvency needs, taking into account the proportionality principle.

Finally, there is scope to improve the quality of stress testing including reverse stress tests and scenarios used in the ORSA assessments. The stress criteria used should enable insurers to evaluate appropriately in a forward-looking perspective the potential risks they and their business may be exposed to and the required solvency in order to manage such risks. EIOPA encourages undertaking to further improve the quality of stress testing.

While recognising the steps taken by insurance and reinsurance companies in implementing ORSA, further improvements will help to better embed this risk management tool into business strategy.

Good for business

Risk management and, in particular, ORSA are essential elements of good governance. An effective governance system encompasses more than risk management to provide for a holistic approach to sound and prudent management of business. Solvency II promotes sound and robust behaviour to manage and reduce risks through well-defined governance systems. EIOPA has identified a number of characteristics that contribute to an effective and proportionate governance system.

These include an adequate and transparent organisational structure with a clear allocation and appropriate segregation of responsibilities, with written policies in place – including in relation to risk management. In addition, there should be at least four established key functions that are independent from each other and with a clear segregation of responsibilities. There should be contingency plans in place for the appointment of board members and key function holders. Finally, if any key tasks or functions are outsourced, there should be no negative impact on either the governance system or operational risks.

Effective governance, like risk management, is not a tick-box exercise; instead good governance is one of the best tools to enable sound business practices.

Benefit for consumers

In many cases, developing and implementing an appropriate and effective governance system, including risk management, will require a cultural change, starting at the top. This cannot be achieved overnight, and the role of senior management and board members is central to its success. An organisation's board needs to set, communicate and enforce a risk culture that consistently influences, directs and aligns with the strategy and objectives of the business.

The right approach to risk management should also reflect well with the consumers. Solvency II aims to ensure a uniform and enhanced level of protection for policyholders across the European Union, and a more robust system should give policyholders greater confidence in insurers and their products.

To conclude, risk management is an essential function for business planning and strategic decision-making. Solvency II and, in particular, ORSA are powerful tools to help companies taking a holistic approach to risk which, in the longer term, can only serve to benefit consumers and policyholders.

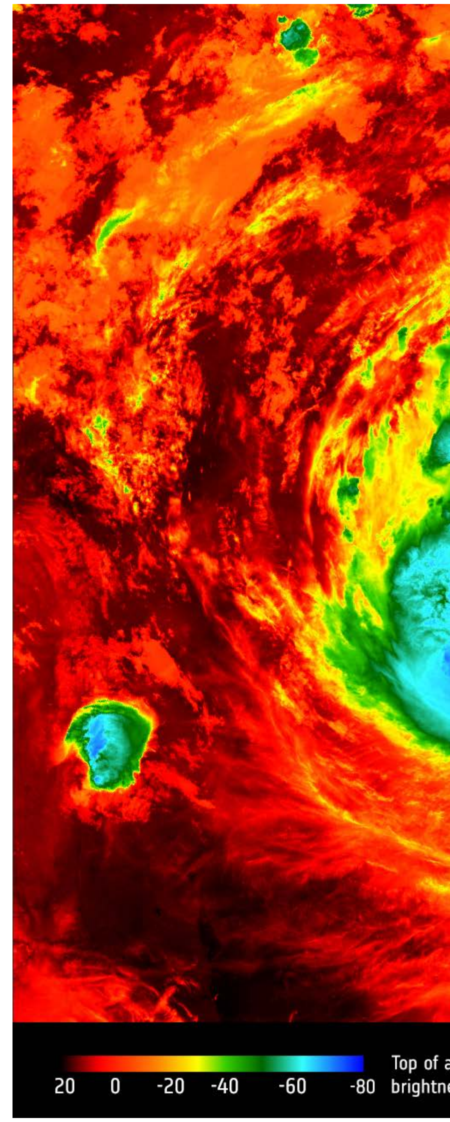
Gabriel Bernardino, chairman of the European Insurance and Occupational Pensions Authority (EIOPA)

> **EIOPA calls upon insurers to widen the scope of their risk assessment and to deepen the risk analysis**

Preparing for extreme events

Organisations tend to underprepare for disasters. A behavioural risk audit could help people get ready for the worst

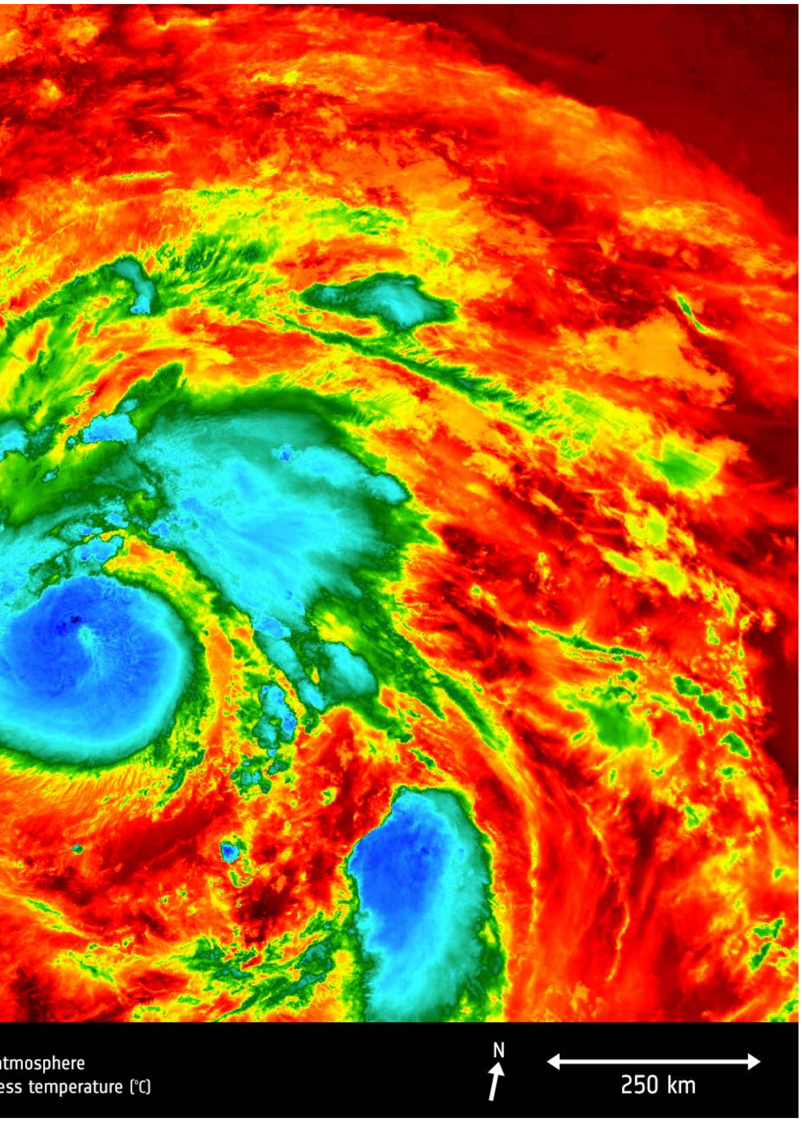
BY HOWARD KUNREUTHER



Hurricane Harvey, which has devastated Houston, Texas, highlights again the challenges we face when dealing with low-probability, high-consequence events. Houston had never experienced any severe flooding, so it is natural that residents assumed that they would not be subject to any severe damage. It is thus not surprising that, according to estimates by the Federal Emergency Management Agency, only 15 per cent of the victims of Hurricane Harvey had purchased flood insurance even though it is not very expensive.

> **A behavioural audit can nudge and encourage individuals to undertake preparedness measures for disasters before they occur**

In our book, *The ostrich paradox: why we underprepare for disasters*, Robert Meyer and I outline six decision-making biases that cause individuals, communities, organisations and institutions to underinvest in protection against low-probability, high-consequence events. These biases are myopia (we have a hard time thinking much beyond tomorrow); optimism (the tendency to believe that the disaster will not happen to us); amnesia (the tendency to forget too quickly the lessons of recent disasters such as Hurricanes Sandy and Katrina); inertia (the tendency to do nothing if we are unsure of the best action to take);



Left: Satellite image of Hurricane Harvey.
Above: Water coming over the road in Kemah during Hurricane Harvey.

> Biases cause individuals, communities, organisations and institutions to underinvest in protection against low-probability, high-consequence events

simplification (the tendency to selectively attend to limited data that supports our preferences); and herding (the tendency to imitate others).

Nudge

We propose a behavioural audit that recognises the above biases and uses them to nudge and encourage individuals to undertake preparedness measures for disasters before they occur.

There are several ways to incentivise those at risk to take action now. One is to stretch time horizons. Rather than indicating that the chance of a severe hurricane next year is a 1-in-100, experts could reframe their estimate as a greater than 1-in-4 chance that there will be at least one such hurricane in the next 25 years. The same probability is presented over a longer time period. This reframing may help overcome the myopia and optimism biases.

Give short-term incentives. For example, provide a long-term loan to property owners to spread the cost of a loss-reduction measure over time. If the mitigation measure is cost-effective and insurance premiums reflect risk, then the annual cost of the loan will be less than the savings in insurance costs for the safer structure. Tying the loan and insurance to the property and/or the mortgage rather than the individual will address the amnesia bias, as safety measures in place will be a constant reminder.

Reframing

Use default options. For example, insurance premiums could be automatically included in a homeowner's mortgage or taxes. Individuals would be able to opt out if they did not want coverage. However, the need to spend time and energy to cancel a policy may lead them to keep insurance due to the inertia bias.

Another strategy could be that insurers consider offering homeowners multi-year insurance policies, thus freeing them from the need to make an annual decision about renewal. For example, flood policies would be written for three- to five-year terms that would carry an annual premium that would remain stable for the length of the contract. Such an insurance policy would address the simplification bias. Rather than homeowners having to deliberate each year about whether they should renew, or worry if they

8TH ANNUAL RISK LEADERS CONFERENCE

This year's Annual Risk Leaders Conference will focus on how corporate and individual behaviour affects the ability of organisations to manage their risks, particularly in the context of the widespread political and technological changes that have been rapidly evolving across the world.

The theme, *there is no more "business as usual"*, will be explored by a number of eminent business and risk leaders. In addition to Wharton School's professor Howard Kunreuther, speakers include:

PROFESSOR MERVYN E KING
Professor King led the committee that produced the *King report on corporate governance*, widely regarded as one of the most advanced in the world, for The Institute of Directors in Southern Africa.

IAN BARLOW
Ian Barlow was a partner at KPMG and now holds non-executive director roles across the public and private sectors, including as lead non-executive director at Her Majesty's Revenue & Customs.

TREVOR LLANWARNE
Trevor Llanwarne was a government actuary working in the fields of pensions and insurance across the civil service, education, the NHS, the armed forces, the police and the judiciary.

CAROLINE WEHRLE
Caroline is global risk and compliance director at Diageo, and a director at Aster Group UK. She has held various director positions across audit, finance and risk functions.

Sign up today: https://www.theirm.org/events/risk-leaders-2017.aspx

Image credit: Shutterstock.com

Above: An aerial view of Houston showing the extent of flooding caused by Hurricane Harvey. Houston emergency services with cars across the flooded street in Houston, Texas.

are covered should a flood occur, the coverage would be automatic for the length of the contract.

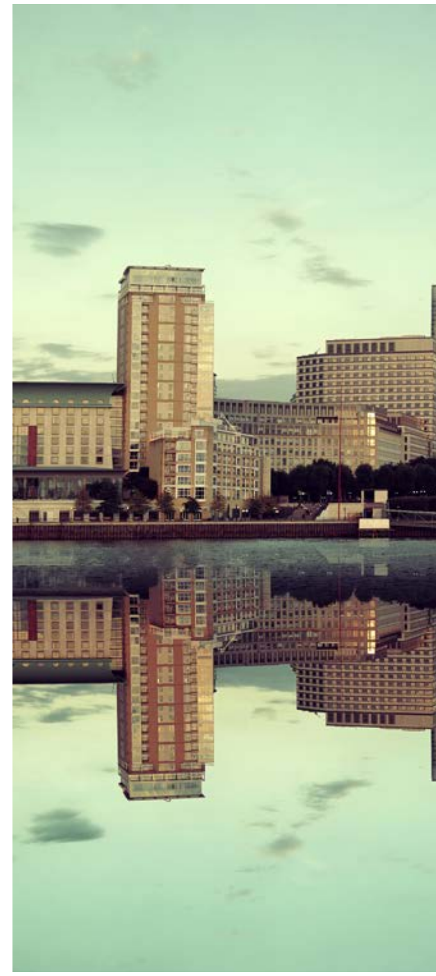
Finally, seals of approval can be effective. The most cost-effective means of making communities safer from hazards may be through social norms that directly address the herding bias. If residents in flood-prone areas see all of their neighbours making investments in loss-prevention measures and buying insurance, they are likely to follow suit. The Insurance Institute for Home Building and Safety has awarded seals of approval to homes that meet or exceed building code standards. The hope is that such marks of excellence would not only increase the property value of the home but also be seen as signs of status by others – nudging them to undertake improvements.

We need to recognise that when making decisions, our biases are part of our cognitive DNA. While we may not be able to alter our internal wiring, we may be able to improve preparedness by recognising these biases and designing strategies that anticipate and deal with them.

Howard Kunreuther is the James G Dinan professor; professor of decision sciences and public policy at the Wharton School; and co-director of the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania. He will be speaking at IRM's 8th Annual Risk Leaders Conference, *No more business as usual*, November 23, 2017. Book now: https://www.theirm.org/events/risk-leaders-2017.aspx

> Our biases are part of our cognitive DNA

Demonstrating excellence



IRM has responded to the past decade's changes within the financial services industry by revamping its sector-specific qualification

BY ARTHUR PIPER

It is a decade since the financial crisis hit the world in 2007. Key banks and financial institutions went bust or were privatised, interest rates plummeted and governments around the world have been printing money to keep the global economy afloat. Not surprisingly, regulators in the UK, Europe and the US have played a key role in examining what went wrong and revamping their regimes to make the financial system more resilient.

Those working in the financial sector are living not only in a different world of compliance but also in an industry where technology has transformed both the services that financial institutions can offer and what customers now demand. These pressures have encouraged financial organisations to look increasingly to their risk functions to develop enterprise-wide risk management and to help ensure that their strategies in the digital marketplace are fit for the challenges they face in a dynamic and unpredictable market.

> **We have revised our syllabus placing a sharp focus on the importance of strategy, culture, behaviour and competence**

Never a dull moment

As Iain Wright, chief risk officer of Old Mutual Wealth, told *Enterprise Risk* magazine in June, "Part of the thing about working in the risk function of a financial services organisation is that it's not a dull place to be."

IRM has responded to those trends in the sector by refreshing and renewing its International Certificate in Financial Services Risk Management.

COURSE OVERVIEW

MODULE 1

Principles of risk and risk management in financial services

This module introduces the principles and concepts of risk management in financial services, leading to an examination of how to classify risks in a financial services environment and the approaches that are used to identify, assess and treat them.

- Recognise the origins and key concepts of risk management
- Understand the regulatory environment in financial services
- Understand the main sources of risk within banks and insurers.

MODULE 2

Practice of risk management in financial services

This module explores the impact of the business environment on risk management in the banking and insurance sectors. Learn how corporate governance influences risk architecture, culture, appetite and tolerance.

- Case studies, including post-financial crisis
- Explore the impact of the wider business environment
- Study the Three lines of defence governance model
- Apply risk management frameworks.

IRM QUALIFICATIONS

The International Certificate in Enterprise Risk Management is the ideal qualification for anyone looking for a solid foundation in the theory and practice of effective risk management.

Taking just six to nine months to complete, the certificate is a distance learning study programme that is internationally recognised and relevant to all sectors.

For 30 years, IRM's International Diploma in Enterprise Risk Management has been the global choice of qualification with risk professionals and their employers.

This post-graduate-level qualification has been developed by internationally recognised academics and industry practitioners to provide you with the knowledge and skills to manage risk and maximise opportunities in any organisation.

Learn more: https://www.theirm.org/qualifications.aspx

Socrates Coudounaris, who has been overseeing the changes to the qualification, explains: "We have overhauled the International Certificate in Financial Services Risk Management to reflect international regulatory developments such as Basel III and Solvency II. These regulatory regimes require that companies and their staff have a broader understanding of risk management."

He says the certificate is designed specifically to meet the demands of the financial services sector from a banking and insurance perspective in light of these changes.

Strategic focus

"The post-crash environment has seen regulators, investors and business partners make increasing demands on financial services organisations to demonstrate that they have top-class risk management in place at an integrated, enterprise level," he says. "We have revised our syllabus placing a sharp focus on the importance of strategy, culture, behaviour and competence in relation to risk, and concepts like risk appetite, risk maturity, conduct risk and decision making have to be integrated into the business."

The highly regarded degree-level qualification provides a comprehensive, structured and practical understanding of risk management, covering the latest thinking and regulatory developments in the financial services industry (see *Course overview*). The International Certificate in Financial Services Risk Management is an internationally recognised supported distance learning study programme, which takes six to nine months to complete.

"The certificate gives risk professionals a distinct career advantage and employers the confidence that their experts can deploy a range of practical tools and techniques," says Coudounaris.

The IRM offers a wide range of risk management qualifications and training. It helps members develop their risk management skills and knowledge that can be applied immediately. Studying with IRM also demonstrates credibility with employers and enhances the knowledge of both individuals and risk management teams. ER

Find out more about IRM qualifications and training: www.theirm.org/fsquals

Lessons from failure

Attendees at a recent event held jointly by IRM and The Geological Society heard how Network Rail uses risk management to manage railway assets. By Tim Laverye and Tim Lulham

The suspended railway at Dawlish and the remediation works completed by AMCO's Orange Army will, for many people, be forever associated with the storm events of February 2014. However, not two miles south of this location an equally challenging problem for Network Rail occurred in the form of a large-scale complex slope failure of the Teignmouth sea cliffs, resulting in approximately 15,000m^3 of debris material slipping down and causing the line to close.

Short-term intervention works were immediately implemented to remove the failed mass from the cliff face, enabling the residual risks associated with the earthwork failure to be managed in planned possessions of the line. This allowed the safe running of trains to start again in time for Easter Weekend, April 4, 2014.

The latest flooding at Cowley Bridge Junction, approximately 1.5 miles north of Exeter, occurred in 2016. In this instance, the railway was closed for 48 hours. However, a flooding event in 2012 caused the railway line to be closed for three weeks. Historically, flooding has occurred at this location since 1866 as a result of two culverts passing beneath the Taunton–Exeter main line and the Barnstaple branch line becoming overwhelmed with floodwater.

Although catastrophic, several lessons have been learnt from the events at Teignmouth and Cowley Bridge Junction, which have enabled Network Rail to establish a more mature approach to risks associated with infrastructure failures.

First, subsequent studies of both the Teignmouth sea cliffs and Cowley Bridge Junction have shown that the sites are known areas of historic asset weakness. The failure of these assets has provided Network Rail with more information about the types of failure modes and the trigger mechanisms which may have caused them. With this information Network Rail has been able to manage future risks arising from both sections of infrastructure. Through adopting a tiered approach to risk, via enterprise risk management, Network Rail can more efficiently manage risks arising from the assets at all levels of the business.

Second, the future improved resilience of both sections of railway infrastructure has been recognised and developed. The UK Climate Projections 2009 calculations indicate adverse weather events will increase in frequency throughout the 21st century. Therefore, resilience

Above: Teignmouth Sea Cliffs.

management of targeted susceptible assets is critical to ensure the long-term safety and performance of the operational railway.

Third, closer collaboration and engagement has been established between Network Rail and key stakeholders, including the Environment Agency, train operating companies and freight operating companies. More integrated working with the Environment Agency has allowed the potential flooding of key assets, such as Cowley Bridge Junction, to be forecast earlier and allowed operational mitigation measures to be deployed in a more timely manner. In turn, this has allowed Network Rail to better inform train and freight operating companies of any potential disruption.

Fourth, Network Rail has recognised that better use of technology, particularly remote condition monitoring, can assist monitoring of susceptible assets and when making operational decisions.

Finally, mitigation measures, such as temporary barriers and temporary speed restrictions, have been deployed at key locations which are susceptible to geo-environmental hazards, to ensure there is minimal or no disruption to the railway network.

Tim Laverye is route asset manager (Geotechnics) and Tim Lulham is route risk co-ordinator at Network Rail Western Route.

Deliver success in today's complex operating environment

4C STRATEGIES

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.

Dr Aarti Anhal Gooden
+44 (0)20 3795 2350
aarti.anhalgooden@4cstrategies.com
www.4cstrategies.com
4C Strategies
20 St Dunstan's Hill
London
EC3R 8HL

Enterprise risk management and risk analysis software

riskHive Software Solutions

Since 1999, riskHive have been an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Low maintenance, highly-configurable and cloud-based, the riskHive Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Contact us today for your free 10-day trial of our ERM or Analytic software solutions. The ERM application, settings and data are easily transportable to your own IT infrastructure if desired.

Ian Baker
+44 (0) 1275 542 839
ian.baker@riskhive.com
www.riskhive.com
riskHive Software Services Ltd.
Dilkush, Farlers End
Bristol
BS48 4PG

Leaders in Forensic Investigation

Hawkins
Leaders in forensic investigation

Hawkins, established in 1980, provides specialist forensic root cause analysis and expert witness services to the insurance, loss adjusting, risk management and legal professions. The company has offices in the United Kingdom, Dubai, Hong Kong and Singapore. All offices are staffed by highly experienced forensic scientists and engineers from a wide range of disciplines.

Graeme Drysdale
+44 (0) 1223 420400
enquiries@hawkins.biz
www.hawkins.biz
Miller House
120 Cambridge Science Park
Milton Road, Cambridge
CB4 0FZ

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, insurance and safety technology solutions

Ventiv Technology is the preeminent provider of global risk, insurance, and safety technology solutions. Working in partnership with our clients to understand their challenges and key business objectives, our solutions adapt to your precise needs and evolve with you. Providing a central platform to work across your company and functions to eliminate silos and help embed risk management. Delivered with Ventiv's extensive risk management and technology experience to provide unsurpassed client value and operational excellence. Winner of 2016 IRM Risk Management Solution of the Year.

Angus Rhodes
+44 (0) 7808 905877
angus.rhodes@ventivtech.com
www.ventivtech.com
Ventiv Technology
30 Eastcheap
London
EC3M 4PL

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

Directory

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
Birchin Court
20 Birchin Lane
London, EC3V 9DU

Risk management software

Origami Risk is the industry's #1 Risk Management Information System (RMIS) as ranked by the 2016 RMIS Review. Founded by industry veterans committed to bringing new ideas and advanced features to the RMIS market, Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage Total Cost of Risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com.

Neil Scotcher
+44 (0) 7775 758655
nscotcher@origamirisk.com
www.origamirisk.com
Origami Risk
4th Floor, Victoria House
Victoria Road
Chelmsford, CM1 1JR

Risk management software

Xactium is a cloud based Risk Management software vendor that is changing the way regulated organisations evaluate and manage their risk. Our aim is to enable risk and compliance managers to transform the value of risk management within their organisation, through the use of modern, agile and collaborative software. Our risk management platform ensures that organisations such the FCA, Direct Line Group, HS2 and HomeServe can stay up to date and respond rapidly to both business and regulatory change.

Rob Stephens
+44 (0) 114 2505 315
rob.stephens@xactium.com
www.xactium.com
Xactium House
28 Kenwood Park Road
Sheffield
S7 1NF

A say on pay

Will recent reforms to reporting on pay diminish the power of shareholders?

From June 2018, UK companies are going to have to publish more detail on the differences in pay between those at the top of the company and those at the bottom. Under the new rules, announced in August this year, about 900 publicly listed companies will have to disclose the pay ratio between bosses and workers in their annual reports and accounts.

Reaction has been typically partisan. The Trades Union Congress, for example, said that the raft of corporate governance reforms which was meant to increase the influence of workers within business has been drastically watered down. For example, the original proposal to mandate worker representation on corporate boards has been dropped.

Instead, businesses will need to ensure that staff can either nominate a director, create an employee advisory council, or assign a non-executive director to represent the workforce. This requirement is to be implemented through the UK Corporate Governance Code, which operates on a comply or explain basis. Companies that don't bother just need to explain why not.

While executive pay levels have fallen recently, the historical picture shows a steady disparity between those at the top and those at the bottom of companies. Businesses are fond of saying that they need to pay top rates to attract the most talented executives in a competitive global market. Twenty years ago, chief executives made about £45 for each £1 earned on the shop floor. Today, the boss earns £129 per every £1 a worker earns, according to research group the High Pay Centre.

Image credit: Shutterstock.com

> While executive pay levels have fallen recently, the historical picture shows a steady disparity between those at the top and those at the bottom of companies

The bigger picture, though, is not exclusively about pay. Over the past 20 years, the shareholder model of capitalism has strengthened despite counter-movements that argue companies have a responsibility to a broad range of stakeholders. In the UK, the shareholder model is written into law so that directors have a duty to act in the best interest of their investors. How they pay workers is their own business.

Privately, many at the top of the largest financial consulting firms believe that the shareholder model has run its course. They argue it promotes risks associated with short-termism to the detriment of communities, environments, and workers. The expansion and emphasis on non-financial reporting initiatives that have seen businesses widen the extent of their public disclosure in areas such as board diversity and pollution all support this trend.

But others worry that, without radical change, the shareholder model will continue to reassert itself by other means. With constant investor pressure, the government's pay ratio reforms could force executives to embrace the letter rather than the spirit of the new rules.

For example, rather than cutting executive pay or increasing the salaries of their workers, companies may look at other ways of reducing the ratio. That could mean outsourcing jobs or increasing automation. The former has been one of the stories of the last 20 years; the latter most likely will be a major story of the next ten.

Risk managers have slowly been moving to look more holistically at the threats that could derail their businesses' strategies. Reputation risk arising from a wide range of issues now ranks as one of the top five executive worries – largely because it can destroy shareholder value. The power of a range of communities outside of corporations has been massively amplified by social media. Only time will tell whether those stakeholders will assert themselves over the shareholders who have called the shots during the past 20 years.