

Enterprise Risk

Summer 2020 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Purposeful resilience: beyond survival/ **Tilt to green:** adjusting to climate change / **Spotlight on assurance:** internal audit's new code/ **Blurred lines:** governance's fuzzy practices / **Chasing the ideal:** safety management



IRM survey: risk managers are playing a vital role supporting their organisations during the global crisis

International Certificate in Enterprise Risk Management

Advance your career with the global benchmark qualification in Enterprise Risk Management



About the International Certificate

The International Certificate in Enterprise Risk Management (ERM) is the industry-standard qualification for anyone looking for a solid foundation in the theory and practice of effective risk management. The certificate explores elements of the risk management process and explains how organisational culture and appetite for risk may affect the implementation of such processes.

With the growing uncertainty of current global events, our qualification provides the understanding, tools and techniques needed to help risk practitioners stay up-to-date with the best practices required to effectively manage and mitigate risks. Resilience, risk and recovery are all covered in our globally recognised qualification, which is studied via supported distance learning and takes as little as five months to complete.

What our students say



Sachin Singh IRMCert

Business Continuity Manager, Abu Dhabi Motorsports Management

"The qualification validates my understanding of risk management. The certificate exposed me to a methodological structure on analysis and treating risk. It has also helped to improved my own standing in the industry as a risk management expert, being able to use risk status reporting to the board as a result of what I have learnt."



Cynthia Nakowa IRMCert

Risk Officer, Equity Bank, Uganda

"With the IRM's International Certificate in ERM, you will be given risk management knowledge right from the basic principles, various risk management standards and essentially having an extensive understanding of ERM. It will definitely grant you the first step to eventually becoming a Chief Risk Officer in any organisation."

Find out more at:

www.theirm.org/erm-mag

Resilience, risk and recovery



Developing risk professionals

Editor

Arthur Piper

Produced by

Smith de Wint

Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

Sponsorship and Advertising Sales Manager

Redactive Media

IRMSales@redactive.co.uk
Tel: +44(0)20 7324 2753

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

ISSN 2397-8848

About the IRM

The IRM is the leading professional
body for Enterprise Risk Management
(ERM). We drive excellence in managing
risk to ensure organisations are ready for
the opportunities and threats of the future.

We do this by providing internationally
recognised qualifications and training,
publishing research and guidance, and
setting professional standards.

For over 30 years our qualifications have
been the global choice of qualification for
risk professionals and their employers. We
are a not-for-profit body, with members
working in all industries, in all risk disciplines
and in all sectors around the world.

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

Copyright © 2020 Institute of Risk
Management. All rights reserved.
Reproduction without written permission
is strictly forbidden. The views of outside
contributors are not necessarily the views
of IRM, its editor or its staff.



Developing risk professionals



Editorial



Notes on a crisis

Not many people were thinking seriously about the coronavirus in December last year. The UK news and risk agenda had bigger fish to fry than another virus threat. Brexit dominated boardroom risk discussions and, in some quarters, the term “existential threat to the economy” was currency about our future relationship with the European Union.

Even in early January, the World Health Organization did not recommend travellers to China take any safety precautions. Chinese authorities reported 41 cases and one death from what they then called Novel Coronavirus.

A mere six weeks later, the virus had reached 50 countries including the UK, and the tragic wave of deaths mounted higher and higher.

How was it that so many governments and organisations had failed to either consider the risks of or prepare for a global pandemic? It had been repeatedly flagged up by the World Economic Forum and others as a high-impact risk event – not highly likely, but possible. Risk professionals in just over half of UK businesses had considered the effects of a global pandemic (or something similar) on their organisations, according to IRM’s research (see *Risk management in the global crisis*, pages 10-13). Unaccountably, 20 per cent of those that had considered these risks did nothing.



Risk professionals in just over half of UK businesses had considered the effects of a global pandemic

When Carolyn Williams, IRM’s director of corporate relations, and I discussed this problem she described it as a noise and signal issue. The noise – Brexit say – drowned out the weaker signal of a global pandemic. The world had seen two recent viral outbreaks: SARS and MERS. But they never reached Europe and never made it onto busy boardroom agendas for long.

I agree that many risk managers suffer from noise overload. But perhaps it also reveals a lack of understanding about what a high-impact risk actually means. As we talked, we wondered how many organisations had credible plans for operating without the internet, or without other parts of the nation’s critical infrastructure, for a period of time.

But in over 20 years of reporting in this area, I have repeatedly heard it said that boards are too busy to deal with complex risk issues. While the situation has improved a little, perhaps that is another critical high-impact, high-probability risk that now needs urgent redress.

Arthur Piper

Editor

CEO pens open letter to company directors, appealing for change



COVID-19 has exposed the traditional governance and risk management process as defective. But there is a better way

..... BY ANTHONY STEVENS

I get it. I am asking you to read this in the midst of a period of immense global upheaval. But this is the moment to campaign for change. In 2020, companies are being forced to consider business risk like never before, so why not shift the paradigm while we're at it? COVID-19 caught many boards dazed and shocked. Why?

Risk and compliance activities have historically been treated as nothing more than guesswork, shackled with outdated admin. As a result, there is almost never a clear consensus on what needs to be done about genuinely managing risk. This mindset puts boards at risk of being dangerously disconnected from reality.

Evolve

.....
In a world fraught with “unknown unknowns”, comprehensive risk management at all levels is critical. Tedious workshops and confusing admin simply have to go. We must evolve. Not just for the effective governance of our companies but for the people we are charged with protecting, both within our organisations and those whose customer information and money we are trusted with.

Addressing business risks can be a confronting experience. Nevertheless, many more of them are headed our way.

Recently, when we published our latest *Top 10 Global Business Risks*, boardrooms lit up with discussions as cyber incidents reached number one. We were also tackling climate change and actioning impending modern slavery compliance. Weeks later, COVID-19 exposed the traditional governance and risk management process for what it really is: defective.

Take heart, it is the traditional risk review process that is letting you down, and you are not alone.

Critical issues

.....
Over the past year, our team learnt three critical things from our discussions with hundreds of leaders about the effectiveness of traditional risk identification, assessment and review by boards:

1. The most important aspect of risk management is the discussion you have with your colleagues and the related consensus. The people closest to the “action” are

not being appropriately consulted.

2. It is critical to get input from your team and as broadly as possible to allow for individual and collective perspectives on the likelihood and impact of risks.

3. With the increasing breadth of risks, using expertly defined risk libraries is critical to identifying the “unknown unknowns”.

4. Historically, there has been no easy-to-use, team-based tech solution available to support these objectives.



The most important aspect of risk management is the discussion you have with your colleagues and the related consensus

.....
Companies need effective governance and risk management, and their company directors and senior management on board to achieve it. The vision should be for a more secure world, where ethics, standards, regulations and morals are baked into digital transformation. Our governments, enterprises and service providers alike must demonstrate that they are effectively managing risk, achieving acceptable levels of compliance and, most importantly, protecting sensitive information and delivering reliable services.

Together, we can focus our business efforts on what will have the greatest benefit to global citizens. ☺



.....
Anthony Stevens is the CEO and co-founder of 6clicks, a Melbourne-based technology business helping companies automate vital risk assessment, compliance and ISMS processes.

The company's free mobile app 6clicks Risk Review for Teams was launched in 2020, enabling stakeholders globally to identify and assess risk at a team and organisational level quickly and easily, generating a powerful risk matrix in a matter of clicks: <https://6clicks.io/>



10

FEATURES

10 Risk management in the global crisis

Risk managers have served their organisations well during the global pandemic, but there is still much to do over the coming months and years

14 Purposeful resilience

Risk managers can play a vital role in creating resilience that has purpose in their organisations

20 Tilt to green

For some, the global pandemic underlines the importance of acting quickly to avoid the worst impacts of another major pending worldwide catastrophe – climate change

24 Spotlight on assurance

The coronavirus has exposed cracks in some corporate governance structures. A new code of practice for internal auditors aims to boost the role of independent assurance in corporate Britain

28 Blurred lines

The three lines of defence model of corporate governance is meant to establish clear lines of responsibility on risk, assurance and control. In practice, that clarity is often blurred

30 Chasing the ideal

Organisations have been using the International Safety Rating System in one form or another for 40 years to improve their operational risk management. There have been important lessons along the way

REGULARS

07 IRM Viewpoint

Like many organisations, IRM has swiftly adapted the way it works to deal with the current crisis

08 Trending

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

35 IRM Focus

While it has been a difficult couple of months, IRM's interest groups have successfully served members online

36 Directory

In need of insurance services, risk management software and solutions, or training? Look no further than our listings

38 Toffler

Executives are beginning to wonder if high-rise office blocks will become a thing of the past, yet homeworking brings its own risks



14



20



24



28



30

IRM's New Virtual Training Courses

With over 30 years' experience delivering industry-leading training courses



IRM is now able to offer our industry leading training courses online, with the global pandemic causing disruptions and uncertainty surrounding face-to-face training delivery we want to be able to support and successfully train risk practitioners whatever level you're at.

The IRM has restructured the learning so it's accessible online and also introduced new content - keep an eye on our website for new courses.

Training courses include:

- > Fundamentals of Risk Management
- > Risk in the Boardroom
- > **NEW** Managing Third Party and Supply Chain Risk Management
- > **NEW** Enterprise Risk and Resilience e-Learning

Benefits of IRM training:



Practical &
interactive training



Industry expert
trainers

CPD

CPD &
accreditation



Find out more at:

www.theirm.org/training-mag



Developing risk professionals

Resilience, risk and recovery – our theme going forward



Like many organisations, IRM has swiftly adapted the way it works to deal with the current crisis

Just a few months ago, pandemic was, maybe, an entry in a risk register, up in the corner with the other high-impact, low-probability risks. Then it happened, and the effects of the COVID-19 epidemic and its economic consequences are being experienced by individuals and organisations around the world.

IRM has, along with all other organisations, been forced to move swiftly, change and innovate to support our customers, members and students. IRM's 25 staff normally commute to and work in a small office in the City of London, alongside our dedicated training facilities. In a normal month, scores of delegates from around the world would be joining us in London for training courses. Our member groups would be networking at various locations, our business development staff visiting our contacts around the world.

More resilient

In line with UK government requirements, the entire staff of IRM shifted to working from home from mid-March. We had already changed our ways of working in response to the emerging digital world: many systems are in the cloud, much communication is not paper-based, and study materials and support for students are online. All these made us more resilient.




IRM has, along with all other organisations, been forced to move swiftly, change and innovate to support our customers, members and students

Our first thought was for our students, preparing to take their exams this year. As our examinations are studied on a distance learning basis, there was no immediate disruption to their studies. However,

students have to attend in person to take exams, and it was looking increasingly likely that access to examination centres worldwide would be disrupted. Within a few weeks we had worked with our specialist third-party examination providers to ensure that student certificate exams can be smoothly deferred to a future session and a new, remote assessment method is put in place for the diploma exams. Enrolment for new students for all our qualifications has continued as normal all through the disruption – there has probably never been a better time to study risk management.

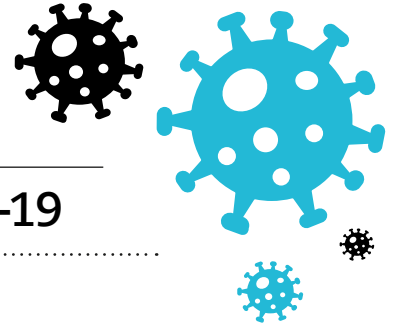
Videoconferencing

Face-to-face training was an early casualty of the lockdown. However, it was evident that there was still an appetite for risk management training, perhaps with people deciding to use their additional free time to upskill. We swiftly scheduled our most popular course, "Fundamentals of risk management", to a videoconference format using the same expert trainers with adapted material and activities. It quickly sold out, and more are scheduled. Feedback told us that this new format had improved accessibility of the course for people who may not have been able to travel to London. Similarly, our member groups, board and committees have been switching to webinars, and we have seen wider inclusivity with people being able to join in from around the world. We will be looking to retain these benefits as we settle into new ways of working.

With 8,000 members globally, our membership renewal exercise each year is a major task, which this year is being done entirely via email (so do check with us if you haven't received yours). Not only does this avoid us sending paper renewal documentation to empty offices, but it is also a step to a greener way of operating. We will certainly be taking these lessons we have learnt through this experience into account when looking at our future plans to ensure that IRM can be a more sustainable organisation in the new digital era. 

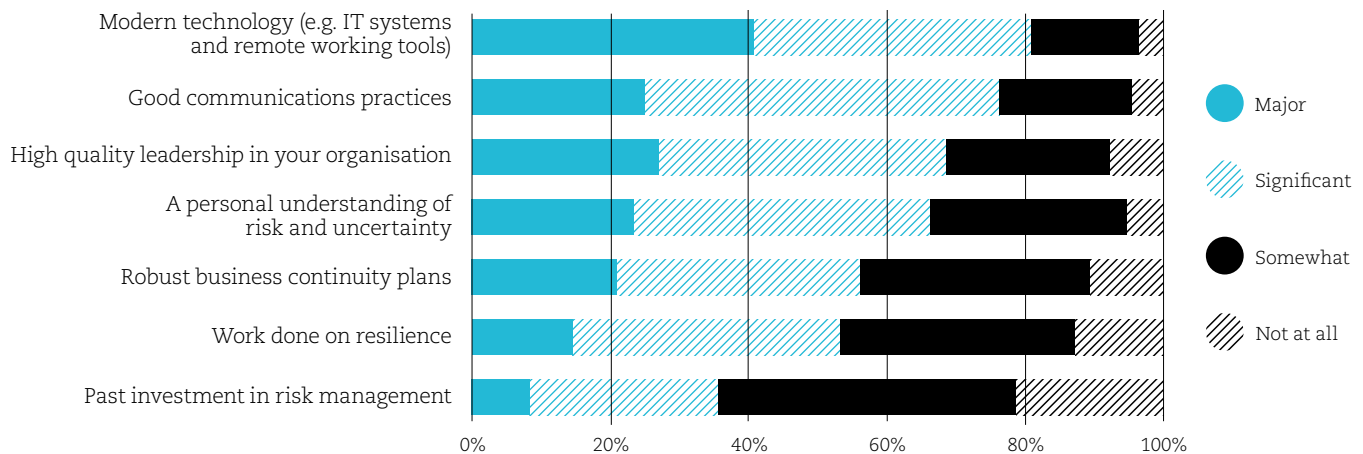
 Carolyn Williams is IRM Director of Corporate Relations

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



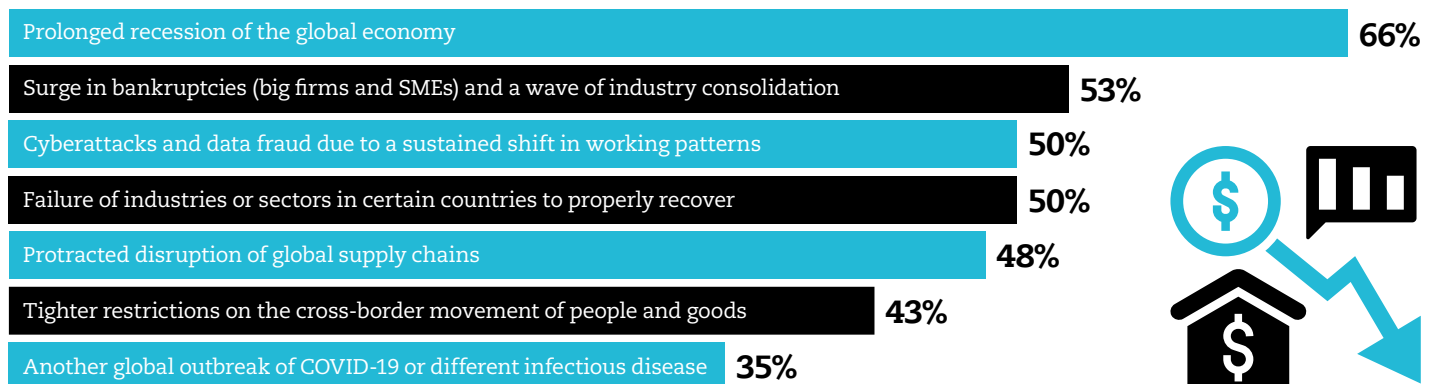
Technology helps risk professionals in Covid-19

From the point of view of the support that the risk function gives the business, what factors have helped your response?



Source: IRM COVID-19 pandemic global risk management response

Recession tops business risk in post-Covid19 landscape



Source: World Economic Forum: COVID-19 risks outlook: a preliminary mapping and Its Implications

Why digital transformation fails



Why it went wrong



41%

Lack of skills or insufficient training



40%

Interoperability with legacy tech



33%

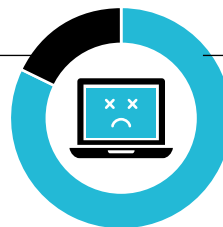
Underinvestment/under-prioritisation

How it went wrong



18%

Failure to adopt (initiative was launched across the firm, but poorly understood and adopted by employees, vendors/suppliers/partners and customers)



82%

Failure to launch (could not get initiative launched across the firm)

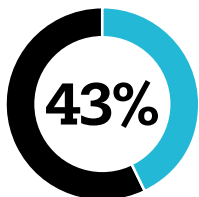


Source: BDO Building tomorrow's business – how the middle market is tackling disruption today

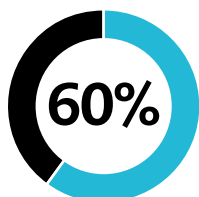
Third party risk neglect



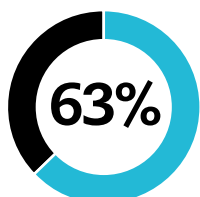
With an average of nearly 10,000 third-party relationships to deal with, many organisations are not completing full third-party due diligence at either onboarding or ongoing monitoring stages



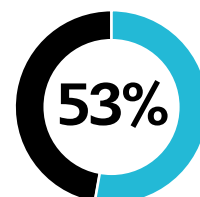
of third parties are not subject to due diligence checks



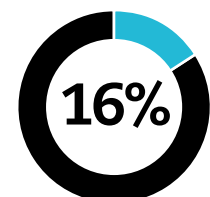
of businesses are not fully monitoring third parties for ongoing risks



of organisations agree that the economic climate is encouraging businesses to take regulatory risks in order to win new business



of businesses say that they would report a third-party breach internally



of businesses say that they would report a third-party breach externally

Source: Refinitiv: The real risks: hidden threats within third-party relationships

Risk management in the global crisis

Risk managers have served their organisations well during the global pandemic, but there is still much to do over the coming months and years

..... BY ARTHUR PIPER

Risk managers have played a vital role at most organisations during the current pandemic, according to IRM's most recent survey – *COVID-19 pandemic global risk management response*. Of the 1,000 risk professionals taking part, 98 per cent said they were providing risk advice related to crisis decision-making – suggesting that most risk staff had not been furloughed or moved onto other projects.

Crisis management has also been holding up well for 82 per cent of organisations. One in four respondents said they were “very satisfied” that their plans had worked well, with just over half (57 per cent) saying that problems had not prevented them working more or less to expectations.

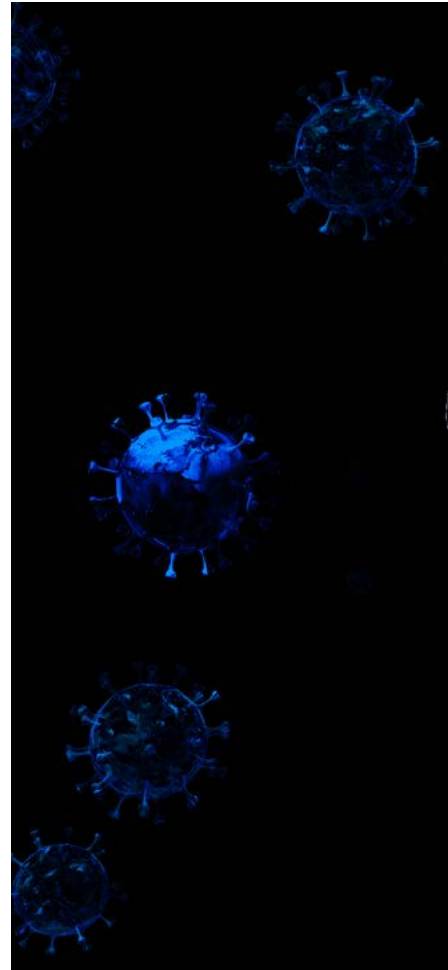
“It appears that our community is fully engaged with the pandemic response, with 98 per cent still at work and appropriately distanced – dealing with current issues and preparing for the future,” IRM chair Iain Wright, CMIRM, says. “Good technology, good communications and good leadership have been rightly highlighted as the key positive factors in maintaining operations.”

Resilience

.....
“The survey shows that resilience is going to be a key issue for businesses going forward – the ability not just to survive, but to bounce back better,” Carolyn Williams, IRM's corporate relations director, says. “If you



The future seems to be coming earlier in some areas
.....





Good technology, good communications and good leadership have been rightly highlighted as the key positive factors in maintaining operations

UK during 2019 made them better prepared than they may otherwise have been. “We have benefited from not being complacent about reviewing potential global risks to our organisation on a routine basis, which I believe put us in a strong position to respond,” said one respondent. “Also, Brexit preparation with, for example, supply chain reviews has supported our response.”

Others said that natural disasters, geopolitical risk, people issues and climate change are being neglected too much by organisations. “For the future we expect to see a sharper focus on resilience and on strategic risk management,” Wright said. “These topics have been around for some time, but this period of crisis will focus attention on ensuring organisations have the people and skills to raise their game to what will be required in ‘the new normal.’”

The world of work could be one such area. Social distancing measures are likely to remain in place for months to come. “When staff do return to the office, they will need to find new ways of working that are consistent with social distancing requirements and may be faced with staff who are reluctant to return to work,” said Dr Jimi Hinchliffe, chair of IOR, in *IRM’s COVID-19 global risk management response: resilience, risk and recovery*, which provides insights from a range of sectors and countries. “There will need to be more collaboration, robust governance and careful management of concentration risks, including third party suppliers.”

After

The picture could look bleak for some organisations and businesses as the world enters into an expected

look at the news, there are some organisations achieving changes to their digital offerings, the way they use premises and how staff work that may have taken years otherwise. The future seems to be coming earlier in some areas.”

Not all organisations were well prepared though. Almost one third (32 per cent) said they had not considered a pandemic or something similar from a risk management perspective. More worryingly, of those who had, a significant minority (20 per cent) had taken no action (see *If you had previously considered a global pandemic, or similar, what actions do you take?*).

“For a risk community this lack of attention is high, given that it has been continuously flagged up by high-profile groups such as the World Economic Forum and the Cambridge Centre for Risk Studies,” Williams says. “It’s a weak-signal issue – the signal has been drowned out with all the other noise that has been going on. It shows that low-probability

and high-impact risks do not have enough time at board level; people pull it back to what they are familiar with and what they can control.”

She says that emerging risk management needs to become part of organisations’ DNA so that they are more prepared to deal with what look like far-off risks – solar storms or the collapse of critical infrastructure – by ensuring the enterprise is able to deal with threats that involve fundamental changes to the way they need to operate.

Impacts

So far, the major impacts of the pandemic have included rapid changes to the way people work, delays in projects and recruitment, and, for some, the opportunity to enhance their reputational standing (see *Has your organisation experienced the following short-term impacts?*).

Anecdotally, a few organisations said that political unrest in the

recession. “The landscape is likely to involve more competition, a reduction in services and changes in societal trends,” according to IRM’s Charity Special Interest Group (SIG) – comments that could apply to many sectors. “Those that survive will need support from funders to continue in what will be an economically challenging environment, which may well lead to the scaling back of strategic ambitions.”

Second-order risks have also been crystallising. In the UK health sector, for example, one emerging area of risk already receiving attention is the number of people who may become seriously ill as a result of delayed treatment or identification of non-COVID-19 conditions during the current crisis, according to IRM’s Health and Care SIG. There are concerns over the capacity of the health and care system to provide the treatment required, especially in the event of further waves of COVID-19.

Risk management

In the IRM survey, 94 per cent of respondents believed that the experience of COVID-19 has strengthened the case for risk management. Alexander Larsen, CFIRM, chair of IRM’s Energy SIG, agrees: “Risk managers are important now, more than ever, and need to step up to the plate and show their value in helping organisations survive and thrive into the future.”

In practical terms, that means risk managers need to be considered a critical part of decision-making, providing management with up-to-date risk information in order to improve the quality of its decisions. That may include identifying key risk indicators specific to the current crisis that should be monitored closely over the coming months. In addition, quantitative risk analysis should be conducted where possible in order to support decision-making, he says.

“It is important to understand that organisations need to prepare for recovery too and risk managers also play a vital part in supporting the strategic planning process (whether it be diversification, re-invention or cost cutting) by running scenario workshops, identifying risks to any proposed



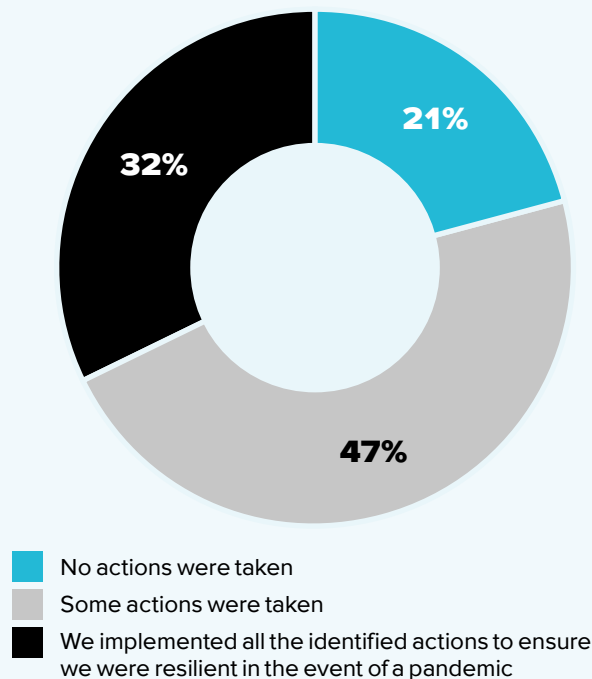
Those that survive will need support from funders to continue in what will be an economically challenging environment, which may well lead to the scaling back of strategic ambitions

strategies and undertaking risk analysis of those strategies (providing an indication of likely deviations from the plan),” he says. “Risk managers can even set key opportunity indicators to provide management with the optimal time for purchasing, starting up projects or entering new territories, something that management rarely receive from a risk management department and may help in changing perceptions from that of risk management as the bearers of bad news, to a more positive view.”

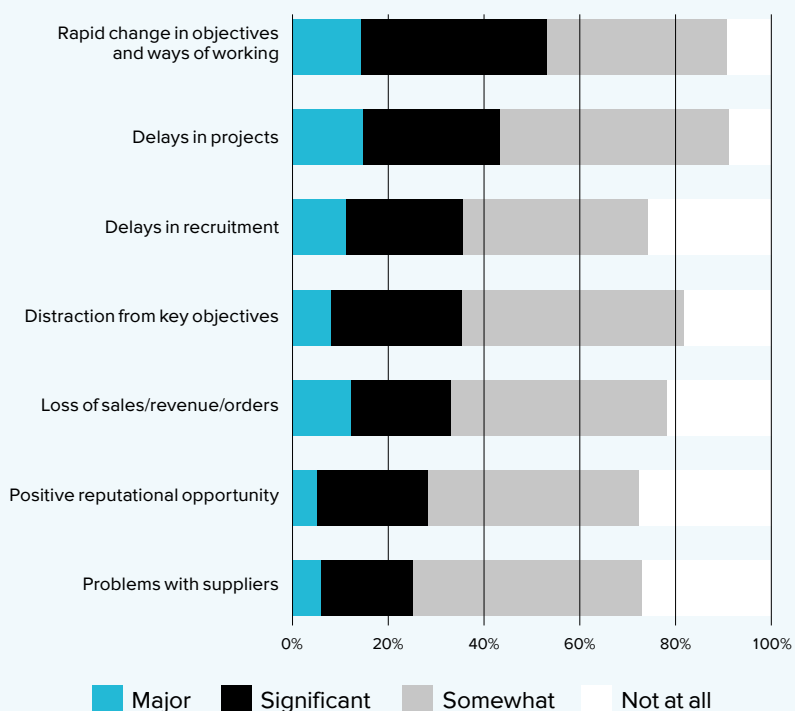
Some risk managers may need to brush up their skills and knowledge.

“It is critical for risk managers to also equip themselves with skills in the area of disaster management and business continuity management,” says Zanele Makhubu, CMIRM, chair of IRM’s South Africa Regional Interest Group (RIG) and a director of enterprise risk management and business continuity in the public sector. “The outbreak has made risk assessment a prominent skill and most sought-after in assisting in mitigating the virus. In our country risk managers are called to lead in advising business and government in terms of risk assessment and business continuity management.”

IF YOU HAD PREVIOUSLY CONSIDERED A GLOBAL PANDEMIC, OR SIMILAR, WHAT ACTIONS DID YOU TAKE?



HAS YOUR ORGANISATION EXPERIENCED THE FOLLOWING SHORT TERM IMPACTS?



LEARNING THE LESSONS

- Alterations to resilience plans and the testing of them. This includes preventative measures and the capabilities in people, processes, technology and culture
- A greater understanding of the dependencies around third parties and the sensitivities in relation to resilience strategies. This includes a clear understanding of key business activities and accurately identifying the key risks and mitigation strategies
- The need to ensure there are effective frameworks to identify risks, set minimum expectations for controls and plan for critical systems and processes failing eventually
- The importance of maintaining adequate liquidity and having diversified portfolios
- An understanding of the importance of front-office activities, and the ability to quickly adapt to protect assets, employees and customers, ensuring there is a good balance between automation and manual activities
- The need for highly skilled people with diverse specialisms and professional qualifications that bring pragmatic approaches to solutions

Source: IIRM Financial Services SIG; Maria Singende, IIRMCert, risk manager at Barclays Bank; and Keith Webb, director of consulting, business risk at Xcina Consulting

“It is critical for risk managers to also equip themselves with skills in the area of disaster management and business continuity management

Lessons and reflections

The challenges faced by every sector and in every country demonstrate there are lessons to be learnt (see *Learning the lessons*). It is important to learn lessons now so that organisations are better prepared for critical business risks arising in the future.

“The question to be asked is how did so many of us not see this coming, yet over the years, the World Economic Forum has listed the spread of infectious disease as one of the risks in the global risks heat map,” Dorothy Maseke,

CMIRM, chair of IIRM’s East Africa RIG, says. “The survey shows that many did not foresee the impacts that such a pandemic would bring. It should not come as a shock if in the coming years the environmental and climate change risks that have been long researched, documented and spoken about manifest just as this pandemic has. This is a lesson for the future.”

IRM would like to thank all of those who took the time to contribute to the survey and share their views in our research report at such a busy time.

Purposeful resilience

Risk managers can play a vital role in creating resilience that has purpose in their organisations

.....BY GARETH BYATT



The need for organisations to demonstrate purposeful resilience is as important as ever in today's world. We all know that the COVID-19 pandemic has had a huge impact around the world. Many businesses continue to face extremely difficult challenges and tough choices, and much has been observed over the past few months about the way that businesses, large and small, across all sectors have had to adapt to changes forced upon them as a result of COVID-19.

The impacts of these changes will continue to be felt for a long time. COVID-19 has been an enormous challenge to deal with, yet the need to have good organisational resilience was already paramount. Change has been speeding up for years, through shifts such as advances in new technology and digitisation, the need to implement action towards sustainability for matters such as climate change and tackling poverty and corruption, and the need to ensure our eco-systems and supply chains operate well. COVID-19 has accelerated many of these changes.

As businesses and the partners they work with up and down their value chains continue to adapt to their changing environment, examples of innovation and resilience abound. Sometimes they come from creative



Just as a tree bends and flexes in the wind, organisations, together with the partners they work with, need to bend and flex to adapt to change



desperation (which we have seen in the midst of the COVID-19 pandemic), sometimes by learning from what's missing or is not working and correcting problems quickly.

This piece does not go into specific resilience principles and mechanisms such as high resilience organisations rather, it highlights some key points and features of purposeful resilience that can be applied to any organisation, regardless of its nature and size. Even so, demonstrating purposeful resilience is not easy. In the midst of competing goals and scarce resources to manage, how can we turn stated ambitions and ideals into practical actions that work?

Starting points

A starting point for understanding your organisational resilience is to look at your organisational

structure (see *Key business factors*). What linkages do you have to the customers and suppliers you work with, and what type of flexibility is built into these structures?

Just as a tree bends and flexes in the wind, organisations, together with the partners they work with, need to bend and flex to adapt to change. Rigidity slows you down, and it will hinder your response to disruption and uncertainty. Even with robust plans in place to deal with disruption, if they are not aligned to a flexible structure and an ability to change when you need to deal with things in unexpected ways, they will not be truly effective when you need them.

An important foundation-level consideration for your organisational resilience, therefore, is to ensure you have the right type of flexibility and adaptability in your structure, and your eco-system, so that you



Demonstrating purposeful resilience is not easy

.....



Manufacturers, large and small, have quickly retooled production lines to make ventilators; retailers have changed their production lines to make healthcare PPE

can be nimble and responsive when you need to be. This isn't always easy. It requires the right balance between control and agility.

Practical tools and techniques that we use for risk management can be applied to managing resilience (see *Tools to aid resilience management*). Thinking through resilience risks, in an unbiased way and with diverse thinking welcomed, is a valuable and important part of understanding our state of resilience, and whether we are focusing the right amount of effort on what's critical.

International guidelines on resilience and business continuity exist from the ISO. ISO 22300 and the accompanying standards 22301, 22313, 22316 plus ISO/TS (Technical Standards) 22317, 22318, 22330 offer good guidance and link to other related standards such as ISO/IEC 27001. These standards adhere to a Plan-Do-Check-Act

(PDCA) model, which is good general management practice.

Having purpose

A fundamental element to organisational resilience, for businesses of all sizes, is being able to demonstrate purpose in times of need.

We have seen many excellent examples of businesses demonstrating societal purpose as they have responded to COVID-19 – while appreciating that many businesses and sectors have been hit extremely hard by the economic impact of the pandemic. Pharmaceutical and medical businesses have donated PPE and switched their focus to work together on developing a vaccine for the novel coronavirus responsible for COVID-19; various manufacturers, large and small, have quickly retooled production lines

to make ventilators; retailers have changed their production lines to make healthcare PPE; breweries have adapted their production lines to make hand sanitiser; a small pizzeria in Chicago adapts its ovens to make face masks for healthcare workers.

These are just a handful of examples of businesses being able to quickly adapt and to demonstrate purposeful resilience for society's pressing needs. I could have listed many more. The principle of purpose applies to any type of unwanted event and disruption – whether it is a public health matter, a major flood, an earthquake, a major cyberattack, terrorism, major operational breakages or a major

disruption to the supply chain.

When you have thought through your resilience approach, and planned and practised how to respond to fast-changing circumstances, you give yourself time to see valuable and critical insights to being purposeful when the disruption occurs.

Remember that in order for this to work, your organisational design has to be flexible – it has to allow teams to work together quickly and in concert, with purpose being at the centre.

An example of purposeful resilience is with sustainability. The elements of sustainability, which are encapsulated in the United Nations Sustainable Development Goals (the SDGs) require and demand resilience.



Risk managers can be the glue for teams right across our organisations

KEY BUSINESS FACTORS

- 1** Businesses exist in an eco-system that is more dynamic and interconnected than ever before – which represents threats and opportunities;
- 2** The velocity of overall change and the dynamism of risk is increasing, and it will continue to increase – for example, through new technology and the digitisation of commerce, and the compound effect of eco-system linkages having ever faster effects. Are you seeing and anticipating change on your radar?
- 3** Sudden, major changes can occur at any time. To emerge stronger from them, we need to be ready to adapt, together with the parties that we work with. We will not succeed in isolation;
- 4** While we cannot plan everything that we would do in the face of a sudden and unanticipated change, by adopting a mindset of purposeful resilience and using good tools and techniques to help us plan our actions, we can adapt and demonstrate true purpose, with the partners we work with, up and down our value chain, and the communities we serve.

TOOLS TO AID RESILIENCE MANAGEMENT

Scenario analysis: By looking at a broad range of scenarios (and not dismissing those that you may think of as outliers) in an unbiased way, you can ask yourself what your resilience to change will be, and you can stress-test your ability to respond and review whether you have the right “plan Bs and Cs” in place. Scenario analysis is most effective when you think broadly about plausible possibilities and apply them to your context.

Stakeholder mapping: Mapping stakeholders in your eco-system and understanding the practicalities of resilience in this map can show you where you may have weaknesses. Such weaknesses may be two or three links down the chain. Which suppliers and contractors you work with are critical? And are appropriate resilience plans in place with them and perhaps other options in case circumstances change?

“What if?” decision trees: You might not call options analysis by this name, but in plotting different paths of how events and decisions could take shape and your ability to respond, you may find yourself using decision trees in some form.

Bow-tie analysis: In certain circumstances, practical bow-tie analysis can be a useful way to look at specific resilience threats, and the controls that should be implemented to deal with them. For example, if you have an extended denial of access to your premises, what specific controls do you need to have in place to continue operating as close to normal as possible?

Business impact analysis (BIA): BIA is a technique in most risk managers' toolbox. It can be aided by good scenario analysis. To make a BIA valuable and practical, you need to connect it to your operations, and to provide them with immediate value by thinking through resilience measures to critical operations (which starts with knowing what really is critical). Then link it up seamlessly with resilience and continuity plans. Don't leave it “orphaned and separate”.

Business continuity plans: Business continuity plans have to be practical. They should be informed by a good risk assessment and BIA. How people work together to respond to disruption is key. You don't want things to fall through gaps between teams.



KEY QUESTIONS FOR RISK MANAGERS

- 1** Does your organisation currently have activities underway, in some shape and form, to look at your resilience?
A: If so, are you involved in these activities? If not, find out how you can help.
.....
- 2** Is organisational resilience part of/connected to your risk framework/management system?
.....
- 3** Can you articulate case studies, within your business or from outside, of how resilience has added value? Storytelling is always a valuable way to generate interest.
.....
- 4** Can you review your top business risks (for example, those in your business plan) with scenario analysis to stress-test your resilience? Is your organisational structure adaptable enough to respond quickly and effectively?
.....
- 5** Are there certain teams/functions that you can/should assist sooner than others? For example, teams such as supply chain, HR, finance, sustainability, tax and treasury. Can you help them with policy redesign and identification of new skills required for new and better processes, for example?
.....
- 6** Is organisational resilience linked to your appetite for risk – and is this appetite changing due to the impacts of COVID-19? For example, is your appetite for resilience in your supply chain changing?

From aspects such as playing our part towards increasing affordable and clean energy (SDG #7), helping to eradicate poverty (SDG #1) or tackling climate change (SDG #13), purposeful resilience impacts, and is impacted by, them all.

Rather than resilience practices being a stand-alone activity, or something that requires a large implementation project to put in place, you should be able to design and implement continuous purposeful resilience as part of regular operations, and through regular in-built testing be prepared to respond when you need to. To achieve this, you need to keep your resilience activities completely in line with the context of what you do (which can change, of course), and you need to keep them efficient and effective.

Play a part

One of the great features about the role of a risk manager is that, given the span we usually have, we can be the glue for teams right across our organisations. Risk managers can work with leaders and teams in all parts of the business in a number of ways (see


Key questions for risk managers).

Risk managers, if they are not already involved in efforts towards purposeful organisational resilience, should be well placed to involve themselves in such efforts – if there is a will to do so.

If we want to “be the glue that binds teams together”, getting involved in organisational resilience provides us with another way to demonstrate the value of that glue.

Many tools and techniques that we apply to identifying, assessing and managing risk lend themselves to purposeful organisational resilience – together with other management techniques that we can add to our toolkit.

Focusing on purposeful organisational resilience may mean that you have to reassign or change your priorities, which may require a discussion with management to ensure it is appropriate. If the appetite is there, risk teams can play a valuable role in ensuring they contribute to successful and purposeful resilience. 📌

 Gareth Byatt is an independent risk consultant and is IRM's APAC representative.

International Certificate in Financial Services Risk Management

*Advance your career with the
global benchmark qualification in
Financial Services Risk Management*



About the International Certificate

The International Certificate in Financial Services Risk Management will help develop your skills and expertise with practical and immediately applicable knowledge. The qualification has been developed for anyone working in the financial services sector, who is looking for a solid foundation in the theory and practice of effective risk management.

As the global pandemic causes uncertainty for the future, risk managers need to be at the forefront of effectively managing and mitigating risks. Our qualification has been updated in response to international regulatory developments such as Basel III and Solvency II, with resilience, risk and recovery being covered to ensure risk practitioners stay up-to-date. The qualification is studied via supported distance learning and takes as little as five months to complete.

What our students say



Audrey Onsomu IRMCert
Audit and Assurance Supervisor, PwC, USA

“My IRM Risk Management in Financial Services qualification is a treasure. Having the opportunity to study risk and understand why it is so important especially in the financial services arena is one of the wisest investments I have made so far. My qualification has helped firm up the experience I’ve gained over the last six years.”



Johnny Kollin IRMCert
Vice President, Wholesale Credit Sanctioning, Barclays, UAE

“The certificate is a great way for professionals to learn the foundations of risk and for seasoned professionals to broaden and deepen their existing knowledge, staying abreast with recent developments and networking with fellow risk professionals in other industries, to exchange ideas and challenges.”

Find out more at:

www.theirm.org/fs-mag

Resilience, risk and recovery



Tilt to green

For some, the global pandemic underlines the importance of acting quickly to avoid the worst impacts of another major pending worldwide catastrophe – climate change

..... BY MARTIN MASSEY

While the COVID-19 crisis is rightly taking all our attention now, we must not lose focus of the need to address climate change, a catastrophe risk management problem on a planetary scale. As risk managers there is an expectation from key stakeholders including regulators that existing risk management frameworks will need to address risks from climate change and therefore organisations will need to enhance their frameworks and risk maturity from identifying to reporting climate change risks to boards in supporting strategic decision-making. This is both a major challenge and big opportunity for risk managers.

Climate change is unlike any other environmental problem and any other public policy problem and is underpinned by a combination of four unique issues: global, long-term, potentially irreversible and uncertain. Yet the COVID-19 pandemic provides us with an indication of what a fully fledged climate crisis could entail. Experts have been warning about these threats for years and indicate that the world at large is generally ill-prepared to deal with either. What has been encouraging is how scientists and health professionals have been collaborating and reinventing how they work. Integration of scientific knowledge into risk management is also crucial to building resilience to climate risk.

The impact of climate change also poses a financial



Risk managers, through collaboration with a range of stakeholders, will need to play an increasing role in supporting organisations in identifying, assessing and managing climate-related risk and opportunities



stability risk to the global financial system, and as such, various national and international and industry bodies driven by the Financial Stability Board representing the G20 countries are working together to achieve long-term regulatory alignment. Although it is easy to feel overwhelmed by the complexity of the problem, there are a range of solutions including the need to replace fossil fuels with cleaner, renewable energy like wind and solar power.

During the coronavirus crisis there has been discussion of a “tilt to green” in future investments. Organisations that are front-runners that adjust to future structural changes and put sustainability at the heart of their strategies more rapidly will be able to reap the potential benefits that it will bring. They will include enhanced brand image, employee engagement, innovation, new sources of revenue, enhanced relationships with stakeholders and operational resilience.

Risk managers, through collaboration with a range of stakeholders, will need to play an increasing role in supporting organisations in identifying, assessing and managing climate-related risk and opportunities and integrating them within existing Enterprise Risk Management (ERM) frameworks. This integration of emerging risk information and analysis will provide a number of benefits including an improved risk appetite framework and risk mitigation strategies across most areas of an organisation’s risk profile.

Drivers

There are now a number of key drivers of change and expectations that organisations must address, with the most relevant being new international and national legislation and regulation, and a voluntary disclosure approach led by the Task Force on Climate-related Financial Disclosures (TCFD). Other major



It is important that risk managers integrate climate change within their existing emerging risk management framework and processes

drivers include increasing public concerns and pressure from lobbying, activists and investors. The main driver is the Paris Agreement, an agreement within the United Nations Framework Convention on Climate Change (UNFCCC) with long-term goals to keep the increase in global average temperature to well below 2C above pre-industrial levels, and to pursue efforts to limit the increase to 1.5C. This translates to cutting emissions significantly year-on-year to reach net-zero CO2 emissions by 2050. The key question is how we put in place the difficult steps under the agreed global action plan.

TCFD provides expectations for organisations and has structured its recommendations around four pillars, namely governance, strategy, risk management and metrics and targets. The recommendations provide clear guidance for risk managers and boards. Under strategy, it includes the need to “describe the climate-related risks and opportunities the organisation has identified over the short, medium and long-term”.

ERM integration

In the world of radical uncertainty that we are currently in, the role of the risk manager is clear: to translate the complexity and deliver the information to meet the board's needs in a summarised way so they can make informed decisions. It is important that risk managers integrate climate change within their existing emerging risk management framework and processes with agreed ownership and accountability for managing the risk across the risk profile. There are a few existing tools that will be of particular use in identifying and managing climate change, such as bow-tie analysis and horizon scanning.

For example, horizon scanning is an important tool particularly to identify external climate-related shifts across different time horizons such as government policy changes on carbon taxes and new disruptive technologies. Horizon scanning is a formal process to help to explore what the future might look like to understand the uncertainties better and to analyse whether the organisation is adequately prepared for potential



Firms will need to give consideration as to whether they wish to embed climate change across existing credit, market and operational risk committees or if they would benefit from a single consolidated governance body dedicated to the risk

threats and opportunities.

Seeking out information outside the organisation such as using PESTLE analysis is critical to gain insights for global trends such as climate change. One of the main benefits is to build consensus among a range of stakeholders about the future threats and opportunities and how to tackle or profit from them. Boards need input from risk professionals on the financial risks from climate change and help addressing and overseeing these risks within the firm's overall business strategy and risk appetite. The integration

into the risk appetite framework and supporting metrics will be of particular importance, for example metrics that include the science-based targets to reduce emissions.

All of the above needs to be underpinned by a clear governance structure. This is particularly important for a risk such as climate change that cuts across all traditional risk categories. While the incorporation of climate change within the software framework is of some help in this context, firms will need to give consideration as to whether they wish to embed

NEW RISK TAXONOMY

A new climate risk taxonomy developed by the Financial Stability Board is now being adopted by stakeholders including regulators, providing a clear delineation of physical, transition and liability risks.

Physical risks include direct damage to assets and indirect impacts from supply chain disruption. It is important to recognise that physical risks can be event-driven (acute) or longer-term shifts (chronic). The most important and notable impacts have been the increase in storms and floods which, in the last decade, have been responsible for 75 per cent of all global insured catastrophe losses, according to data from Munich Re. The intensity and frequency of wildfires, often driven by drought, are also becoming an increasing concern particularly for Australia and California, and in Europe.

Transition risks relate to financial risks as a consequence of transitioning to a lower-carbon or “green” economy. These risks arise from two related transformations, namely in regulatory policy such as carbon taxes and technology and market disruption that will include innovation in renewable energy. Transition risks are developing as governments support and subsidise low-carbon industries and regulate and tax high-carbon ones.

Liability risks stem from the potential for litigation if entities and boards do not adequately consider or respond to the impacts of climate change. This may include the potential breaching of directors' duties. In February 2020, plans for a third runway at Heathrow airport were ruled illegal by the UK Court of Appeal. This was the first in the world to be based on the Paris Agreement and may have an impact both in the UK and globally by inspiring challenges against other high-carbon projects.

climate change across existing credit, market and operational risk committees or if they would benefit from a single consolidated governance body dedicated to the risk.

In terms of risk solutions, organisations will need to consider a range of risk migration and opportunity strategies. For example, the agricultural sector will need to think about innovative risk-transfer solutions for shifts in temperature and other climate perils. The insurance industry is innovating and has been developing parametric insurance solutions through the use of platforms that draw on remote sensing and weather and climate data from national agencies.

Stress and scenario testing

Stress and scenario testing (SST) acts as a key link in taking the output from the emerging risk process and helping both to assess the quantitative impact on the firm and enabling executive management to consider how they might respond, in advance of an event happening, so that organisational knowledge is built up within an organisation to improve its resilience in times of crisis.


Both the TCFD and regulators such as the Prudential Regulation Authority have made clear that scenario analysis should be conducted to understand the strategic implications of climate-related risks

and opportunities. Scenario analysis evaluates a range of hypothetical outcomes by considering a variety of alternative plausible future states (scenarios) under a given set of assumptions and constraints.

The PRA's discussion paper *The 2021 biennial exploratory scenario on the financial risks from climate change*, published in December 2019, provides some good guidance on the approaches required over a 30-year future time horizon. It gives details of discrete climate scenarios aligned to the Paris Agreement and variables for consideration. Physical risks examples cited include regional sea-level increases and changes in storm patterns, and transition variables include a pathway for the carbon price.


Firms can also supplement this information with more policy-specific recommendations to build their understanding. For UK-based firms, the Committee on Climate Change's May 2019 paper *Net zero – the UK's contribution to stopping global warming* and the Green Taskforce's July 2019 *Green Finance Strategy* offer useful insights into likely transition pathways. There are also some good threat-specific methodologies and modelling tools available – for instance, in flood risk and investment portfolio risk.

Risk managers can therefore play a vital role in driving the scenario selection and design decisions to

assess future scenarios in a rapidly changing world. In a COVID-19 world, we are already seeing positive shifts that could assist in addressing these challenges. These include behavioural changes in people as we decide to fly less, repatriation of supply chains, more understanding of the importance of resilience, greater appetite from governments and organisations to tackle risks, economic incentives to accelerate new sustainable infrastructure and greater global co-operation. 

 **Martin Massey** has 30 years of experience in risk management for some of the leading global insurance and risk consulting firms such as Swiss Re, Aon, AIG and Marsh. He is now a freelance consultant and co-authored IRM's horizon-scanning practitioners guide. His MBA dissertation was "Hedging weather risk from temperature volatility". Massey is chairman of IRM's Climate Change Special Interest Group (SIG). Its goal in 2020 is to produce a practitioner's guide on climate change for risk managers and present the findings and recommendations at the IRM's Risk Leaders Conference in November 2020. The main theme of the guide will be to address how risk managers can embed climate change within their existing ERM frameworks. For more information, contact: martin.massey@hotmail.co.uk



 **Organisations will need to consider a range of risk migration and opportunity strategies**

Spotlight on assurance

The coronavirus has exposed cracks in some corporate governance structures. A new code of practice for internal auditors aims to boost the role of independent assurance in corporate Britain

..... BY GAVIN HAYES

In an increasingly uncertain world, and with businesses exposed to a level of adverse risk not seen since the 2008 financial crisis, boards should be turning to strong, effective and well-resourced internal audit functions to get independent assurance that their risks are being managed and mitigated effectively. The Chartered Institute of Internal Auditors' new *Internal Audit Code of Practice* provides the framework and practical guidance to underpin this critical work.

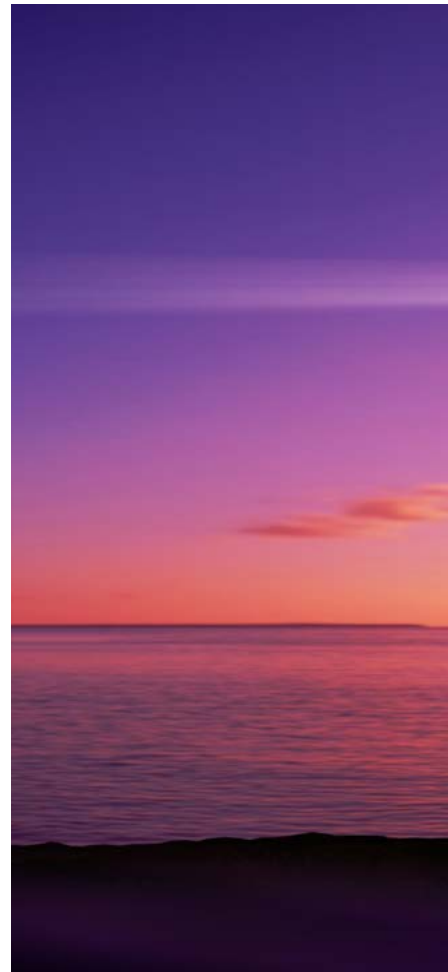
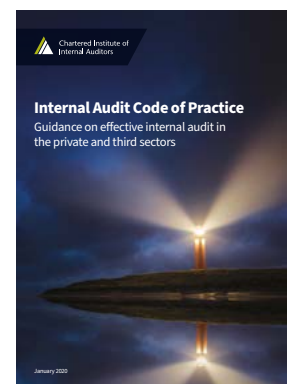
The advent of the coronavirus crisis means that the need for effective internal audit has never been greater. The current global pandemic has exacerbated a plethora of adverse risks to business. Examples include cashflow and liquidity problems, an increase in cyberattacks and fraud, serious health and safety threats, as well as putting immense pressure on supply chains caused by demands from consumers for perceived essential products such as hand sanitiser. This means that now more than ever, businesses must make sure they have robust and effective governance, risk management and internal control processes in place.

Yet even before this crisis emerged, there had for some time been a far greater focus on the need for businesses to manage and mitigate their risks more effectively. There has been a greater demand for independent assurance and calls for stronger corporate governance. The catalyst has of course been a myriad of corporate



The advent of the coronavirus crisis means that the need for effective internal audit has never been greater

.....





failures, many of which have been linked to governance, internal control and audit deficiencies. Most notably Carillion, but before that BHS, as well as more recently the sad demise of Patisserie Valerie and Thomas Cook.

New internal audit code

Much of the focus in the debate that has ensued has been on how to improve external audit. Yet in improving governance, risk and control processes, internal audit also has a pivotal role to play, working in partnership with risk management, compliance and finance as part of the wider corporate governance and audit framework.

This is why, to respond to calls for stronger corporate governance, in January this year the Chartered Institute of Internal Auditors published its new Internal Audit Code of Practice. The Code aims to boost the skills, scope and status of internal audit functions, thereby increasing

internal audit's effectiveness and raising the bar across the profession. It builds on the Institute's vital work in developing a similar Code for financial services, following the 2008 financial crisis, which has been a great success at elevating the internal audit profession. The objective for the new Code is to achieve similar results for internal audit operating in the private and third sectors.

Critically, the new Code secured the backing of influential supporters, including Sir Jon Thompson, the chief executive of the Financial Reporting Council, and Sir Donald Brydon CBE, who led the government's independent review into the quality and effectiveness of audit. It has also been backed by the chief executives of all the main accountancy bodies including The Association of Chartered Certified Accountants (ACCA), Chartered Institute of Management Accountants (CIMA), Institute of Chartered Accountants in England and Wales



Where the internal audit and risk functions are fully combined, the board and the audit committee will also need to ensure that the internal audit role is not undermined



Internal audit should assess not only the process followed by the organisation's first and second lines of defence but also the quality of its work
.....

(ICAEW) and Institute of Chartered Accountants of Scotland (ICAS).

The Code aims to kick-start a debate and discussion about the role and position of internal audit within organisations starting with senior management and the board. As part of these conversations, careful thought and consideration will need to be given to how internal audit interacts, engages and collaborates appropriately with other control functions in the pursuit of good corporate governance. Probably one of the most important to get right is the interaction and relationship with risk management.

Interaction with risk management

One issue that is particularly pertinent and is addressed in the new Code is how internal audit maintains its independence and objectivity, where the head of internal audit also takes on responsibility for some of the control functions, most commonly that of risk management. The big issue here is that, while within financial services there is separation between the second and third lines of defence, outside of financial services there is often not the same degree of

separation, and it is common for there to be a head of internal audit and risk.

Ensuring that internal audit provides independent and objective assurance on risk management and risk control is vital for risk to be managed effectively. However, combining risk and internal audit activities raises issues about the objectivity of internal audit's assurance on risk management. Boards and the audit committee will need to address these issues if the two in any way overlap.

Where separate internal audit and risk teams are managed by a joint head of internal audit and risk, there needs to be a mechanism, appropriate to the organisation, to ensure the audit committee and senior management are getting separate, clear and objective messages from each function.

In cases where internal audit is asked to give advice or assistance on risk management, for example as part of its consultancy role, safeguards are needed to ensure that boards are still receiving the objective assurance on risk that they require. Where the internal audit and risk functions are fully combined (for example in smaller organisations, those that are less risk mature or whose risks



are low level and not complex), the board and the audit committee will also need to ensure that the internal audit role is not undermined.

Pragmatic

To address these issues, the Code offers clear, sensible and pragmatic guidance under Section D “Interaction with risk management, compliance and finance”. In this section, the Code makes clear that the objectivity and independence of internal audit is strongest if it is neither responsible, nor part of, the “control” functions and that separation is preferred. However, because the purpose and skills of internal audit are complementary to that of the “control” functions, the guidance acknowledges that in some cases, the head of internal audit may be assigned responsibility for some “control” functions, citing the common example of a head of internal audit and risk.

The Code states that where such circumstances exist, these additional responsibilities should not undermine the head of internal audit’s ability to give appropriate attention to their internal audit responsibilities, do not impair their independence from management, are appropriately documented in the internal audit charter, and that where a head of internal audit is not able to make an objective assessment of the effectiveness of the additional functions they are responsible for, it may then be desirable to commission an external assessment instead.

The key purpose of this guidance is to ensure there are safeguards in place to protect the independence and objectivity of internal audit, something which is of fundamental importance to the integrity of internal audit.

Revised scope and status

One of the other key focus areas of the new Code is on internal audit’s scope, ensuring that there is no aspect of the business which internal audit should be restricted from examining. Here the Code makes clear that internal audit should assess not only the process followed by the organisation’s first and second lines of defence but also the quality of its work.

This includes areas such as examining the setting of and adherence to the risks the organisation is willing to accept, i.e. the risk appetite, along with the risk and control culture of the organisation. In some organisations inevitably this broadening of scope could result in internal audit examining the work of risk management in more depth and in more detail than it has previously done. This recommendation has the potential to further enhance the relationship between internal audit and risk management and improve the quality of work of both functions.

As well as expanding the scope of internal audit, the Code also seeks to raise its status and standing within organisations. Internal audit cannot do its job properly unless it has the appropriate standing,



As a consequence of the Code, it is expected that more heads of internal audit (and indeed heads of internal audit and risk) will be elevated to a role equivalent to executive management level in the not-so-distant future

access and authority to challenge the executive. It should have the right to attend and observe executive committee meetings, coupled with a primary reporting line to the audit committee chair and ideally a secondary reporting line to the chief executive officer. As a consequence of the Code, it is expected that more heads of internal audit (and indeed heads of internal audit and risk) will be elevated to a role equivalent to executive management level in the not-so-distant future.


In total the new Code makes 38 recommendations on what good-practice internal audit looks like. Although the Code itself and its recommendations are not mandatory, and instead intended as best-practice guidance for organisations to apply appropriately and proportionately, we nonetheless have confidence that the Code will be successful and contribute to better corporate governance.


Levelling up

The latest research examining the implementation and impact of our Financial Services Code, presented in a recently published report called *Stepping up*, found half of all heads of internal audit working in financial services now have a rank equivalent to executive management such as chief finance officer, up from 19 per cent when the Financial Services Code was introduced in 2013. The report also found that 96 per cent of internal audit functions now have an unrestricted scope, up from 90 per cent in 2013.

Based on this evidence, we therefore believe that the new Internal Audit Code of Practice will play a significant role in increasing the scope, skills and status of internal audit, thereby improving

the effectiveness of governance, risk management and internal controls.

The purpose of the Code is to equip internal audit to work with their organisation’s sustainability challenges now and in the future. The coronavirus crisis is a challenge of epic proportions; it is wreaking havoc on the global economy and creating a significant number of new business-critical risks for organisations to grapple with. So, now more than ever, internal audit needs to step up and play its part in helping organisations to navigate the crisis. 

 **Gavin Hayes is head of policy and external affairs at the Chartered Institute of Internal Auditors and led the secretariat that supported the Internal Audit Code of Practice steering committee.**

The Internal Audit Code of Practice can be downloaded here: bit.ly/36gsNbq

Blurred lines

The three lines of defence model of corporate governance is meant to establish clear lines of responsibility on risk, assurance and control.

In practice, that clarity is often blurred

..... BY KIM SOIN, ELINA VAROUTSA AND LYNDA TAYLOR



It is perhaps unsurprising that different financial services organisations interpret the three lines of defence model of corporate governance differently. Our research in the sector – interviews with 19 financial services professionals (nine in the first line and ten in the second) – supports this view.

It emerged that for many in the front line, the risk management practices were already there before the introduction of the model in their institutions, but it was the labelling that was new. Some interviewees observed that the first line did not really think of themselves as the first line; they just got on with what they had to do.

But a number of interviewees used the terms fluid and messy when discussing interpretations of the framework. They expressed concerns about how to manage risk taking while maintaining the balance between commercial direction and independent risk management in the first line. Maintaining independence of the risk function in the first line was a challenge, and a part of that was the asymmetry of knowledge between the first and second lines.

First and second lines

The interface between the first and second lines of defence was where key issues played out over effectiveness of the three lines of defence model and, therefore, risk



The interface between the first and second lines of defence was where key issues played out over effectiveness of the three lines of defence model and, therefore, risk management





These more collaborative relationships result in healthy tensions between the first and second lines

management decision-making, controlling behaviour and enabling organisations to meet their objectives.

Our findings suggest more integration between risk management systems and performance measurement systems. In terms of control, communications are more closely monitored. And while performance targets are common, it is now more usual for incentives in the form of financial rewards (i.e. bonuses) to be capped. The limits placed on the payment of bonuses are linked to an expectation that employees need to appreciate organisational risk frameworks and appetite (e.g. enforcement of credit limits) as well as the new regulatory environment.

Our interviewees suggest it is more common for rewards to be negative in an attempt to avoid the damage associated with risk management failure. Deferred compensation enables banks to control aggressive risk-taking behaviour. But it also encourages action in the interests of the whole institution rather than just the individual. There is also indication of “claw-back” of bonuses, so claw-back can be invoked by the bank to recoup financial losses. Our findings suggest it is now much more difficult for individuals to reap the financial rewards of errors resulting from aggressive risk taking.

We observe positive changes to the dynamics of the two lines and how risk management is perceived. However, in light of the current global pandemic, it is imperative that we interrogate how robust existing risk management systems in the financial sector actually are. 

 **Dr Kim Soin**, director of research students, University of Winchester. **Dr Elina Varoutsas**, assistant professor of accounting, Cardiff Business School. **Dr Lynda Taylor**, assistant professor of accounting, Nottingham University Business School.

management. We found instances of both collaboration and conflict. While collaborative engagement may be key to the effective operation of the three lines model, an imbalance of power can lead to tensions and conflict between the first and second lines of defence. Part of this power was attributable to the view of the front line as the “revenue-generating people” of the organisation.

However, we also found that in many cases the views and activities of risk managers are considered equally important to those of the revenue-generating functions (i.e. the front line) and that there were consequences if the risk management function was ignored.

These more collaborative relationships result in healthy tensions between the first and second lines, as it is becoming more common to challenge the views of those in the front line. Some banks were focused on creating small, agile, inter-functional teams but

while maintaining the independence of the risk function. Our findings show the empowerment of front-line professionals, as they are encouraged to take greater ownership of their risk management responsibilities.

Appetite and incentives

Although the industry is not homogenous in terms of risk aggression, there is a change in the risk culture – across the sector – that enabled the development of a stronger risk management environment. And while there are documented power and knowledge gaps between the first and second lines of defence, we found that risk professionals have experienced increased awareness and acceptance. Many of our interviewees across both lines acknowledge the role of the risk manager as a business partner.

Management control systems can help to strengthen risk management by supporting

Chasing the ideal

Organisations have been using the International Safety Rating System in one form or another for 40 years to improve their operational risk management. There have been important lessons along the way

..... BY MARK BOULT AND MARK FISHER

In 1978 Frank Bird and George Germain published the first edition of the International Safety Rating System (ISRS®). It was the output of collaboration with organisations and individuals across a range of industries to determine the “ideal” safety management system. The ambition was for organisations to use ISRS to assess their performance against this ideal so as to identify improvement opportunities and track their performance in an objective repeatable manner.

Over 40 years on, DNV GL published the ninth edition of ISRS (now called the *International Sustainability Rating System*) in 2019. This edition continues a tradition of keeping ISRS current by reflecting the best practices you would expect to see in an “ideal” management system today and has expanded to cover a range of operational risks: occupational health, occupational safety, environment, quality, security, sustainability, process safety, energy, asset integrity and knowledge. It aligns with the 2018 ISO 31000 and COSO’s 2017 “Enterprise Risk Management – integrated framework”. Following the ISO 31000 process, these practices run from context and risk identification through to risk treatment with monitoring and review providing feedback for improvement, and with consultation and communication,



The ambition was for organisations to use ISRS to assess their performance against this ideal so as to identify improvement opportunities

.....



Those implementing risk controls often find it difficult to interpret what they receive

.....

detailed sufficiently; it is unclear what the controls are to do and how effective they need to be (i.e. their function and performance requirements). Additionally, treatment improvement actions (typically to enhance an existing or add a new control) can be unclear about the specifics of what is required, where it is required and why it is required. Clearly if the risk control strategy, including the specific controls and improvement actions, are well defined, then communicating and implementing them will be easier and they are more likely to result in effective management of the risk. If they are poor, the reverse will be the case.

The analytical stage (I, A, E and S) in the risk process is typically led by risk specialists. Managing live risk controls and implementing improvement actions tends to be by those undertaking the operational activities. For controls to be effectively implemented, these people need to understand the risk treatment strategy, including why the controls are needed and what performance is expected of them. Clear communication is therefore required between the analytical stage and the implementation and is a handover activity. For many organisations, this is a challenge as the analytical phase is delivered by a smaller group of people with risk competence, whereas implementing the controls is done by the wider organisation where risk competence may not be so well embedded. We have found that those implementing risk controls often find it difficult to interpret what they receive. This may be due to the form it is received in and/or the language used. Thus, implementors may not understand what has been communicated, what they have to do, why it is needed and, critically, why it is important.

The analyst's viewpoint on controls is typically different to that

and recording and reporting, enabling and supporting the process.

We have found that the risk treatment step in the risk process is the one where greatest improvement is sought, followed by the monitoring and review activities. This situation was reflected in the output of more than 80 attendees from our workshop at the 2019 IRM Risk Leader's Conference. The core risk loop at the heart of ISRS9 (see ISRS9 *core risk loop (extended process)* and *Risk Leader's workshop attendees' sentiment on where improvement is needed (by ISRS core risk loop steps)*) therefore provides more resolution in these areas where experience suggests organisations need greater focus. It explicitly expands and links these areas in a loop to help people postulate questions like, what controls are needed and how effective do they need to be?

(which we term a control strategy), how should we hand the control strategy over to be implemented and made operational? (which we term communication), and so on.

Risk treatment steps

.....

From our experience, the risk treatment area is seen by a significant number of organisations as needing improvement. This often because, although risk treatments are commonly identified through the risk process and quite frequently have an owner assigned to them, the chosen risk control strategies are often not sufficiently formalised and regularly miss the big-picture context. This results in the specific control arrangements being inadequate (not delivering the desired overall risk performance). The individual treatment controls are often not

of the business and operational personnel. The analysts are interested in the effectiveness of controls (as they are looking for the risk to be managed to an acceptable level); business personnel are wanting to make sure the controls are in place and working as they should (i.e. they are focused on the controls condition and are not thinking about the controls effectiveness in managing risk).

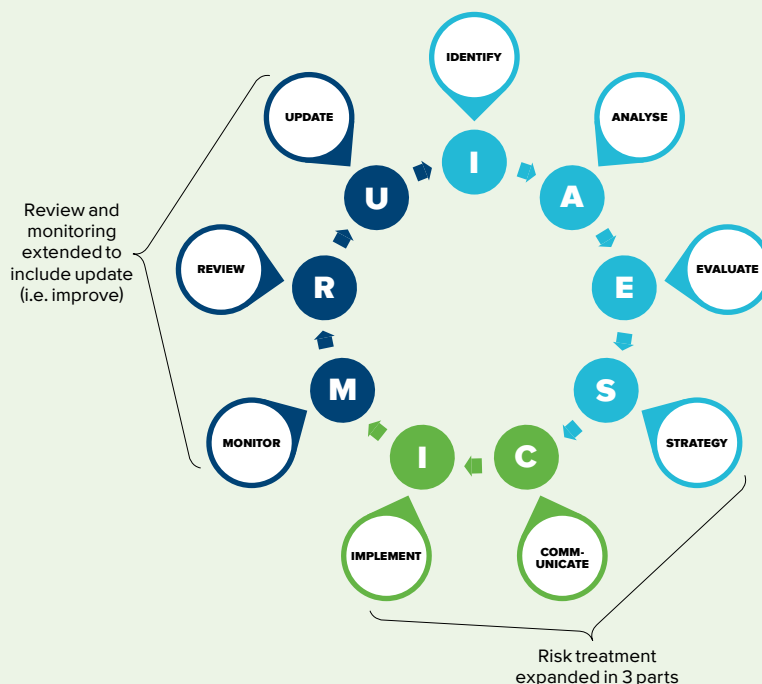
If the communication is addressed well, then implementing the risk controls and improvement actions will be easier and more likely to result in effective management of the risk. If done poorly, the reverse will be the case.

Monitoring and review

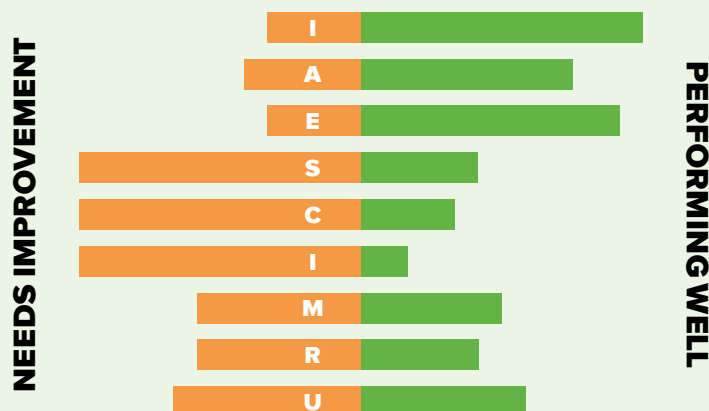
We are seeing a significant number of organisations are looking to improve their monitoring and review so it drives improved risk management. There are several factors driving this. First, some businesses or operations are recognising that they do not have a clear view of the condition of their most critical controls (monitoring). They realise that this can result in a higher risk exposure than desired, poor operational decisions and consequently a greater loss rate (number and/or severity of undesired events).

Second, failing to assess (review) the risk performance means the overall effectiveness of risk management is not known and there will be no improvement actions and, hence, no improvement when needed. This covers the need to review the holistic performance and the performance of critical controls. A holistic review may include, for example, recording, trending and analysing loss events to understand if your controls are managing/ reducing the risk to the desired level, or if improved treatment is needed. The occurrence of some events is, however, rare, so trending is not always practical. Especially for these events, reviewing the performance of the most important and critical controls should take place. This can be achieved by analysing, for example, the results of exercises (for emergency response or business continuity), inspection records for failures and repairs to physical

ISRS9 CORE RISK LOOP



ISRS9 CORE RISK LOOP (EXPANDED RISK PROCESS)



Risk Leader's workshop attendees' sentiment on where improvement is needed (by ISRS core risk loop steps)



A significant number of organisations are looking to improve their monitoring and review so it drives improved risk management

CASE STUDY – POWER GENERATION; AGEING WORKFORCE RESULTING IN LOSS OF KNOWLEDGE ON CONTROLS

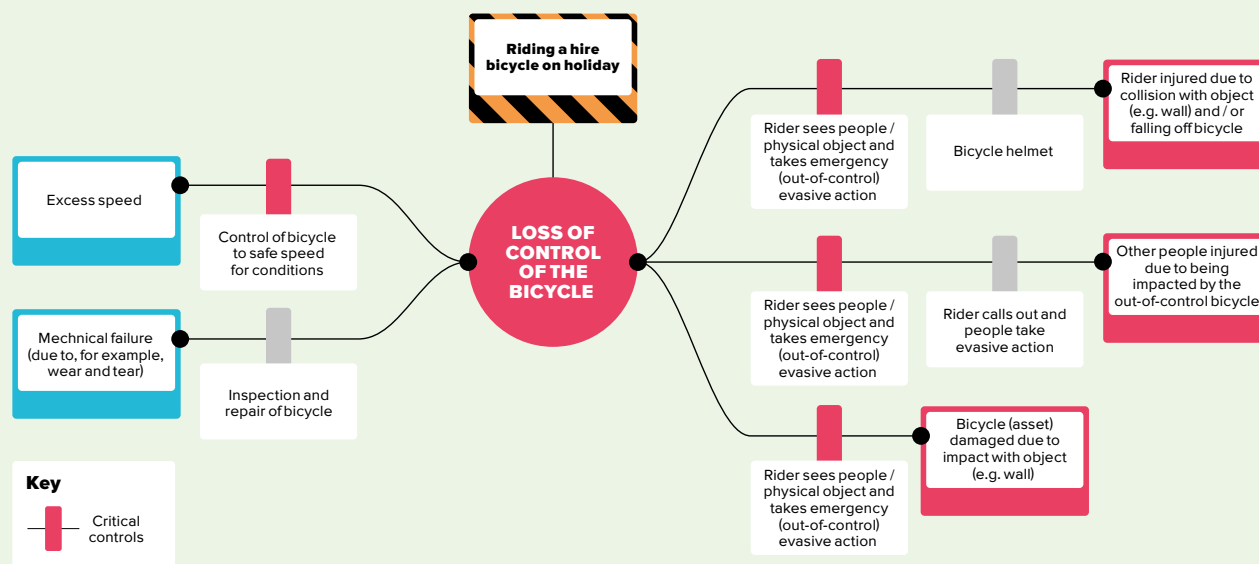
Their challenge

The organisation had an ageing workforce, and as a result was experiencing a high turnover of personnel taking retirement. They could see that they were also experiencing loss of knowledge and skills, particularly in relation to the workforce's knowledge on what were key controls and why they were there.

Response

To (re)create the knowledge in their changed workforce, the organisation used a core group of personnel to identify their key sources of risk and how they were currently controlling them. These were recorded in bow ties. They then developed a communication programme using the bow tie. This visual tool built the workforce's understanding on their key risks and hence the critical (and other) controls they had, why they were needed and what their role was in delivering control and/or in making sure controls were in a good condition.

Subsequently the organisation went on to use the bow ties as the basis for a control assurance processes (essentially scenario-based assurance) to provide ongoing monitoring of the critical barriers.



Above: Illustration of a bow tie to show how it can help communication of controls in a simple-to-understand graphical image.

Pull approaches that incentivise implementors to take ownership of the risk management process and ask for the analytical support to deliver success are more successful

controls, the frequency with which controls are called upon (is this more or less than expected) and back logs in addressing audit findings or maintenance of critical controls.

A key aspect of monitoring and review is to address the “so what?” question. Being able to clearly

explain why an undesirable trend or performance weakness is of concern, and what should be done about it, ensures management focus and organisational engagement. This means a clear line of sight between the measure and the risk be considered. While this is often

easily done with lagging indicators, it is much harder with leading ones. In addition, performance indicators need to be backed by objective audit and assessment programmes to deliver robust assurance of performance.

Democratising risk management

Risk management is generally accepted as the most effective manner of delivering sustainable business performance. The challenge is implementation. Overcoming this challenge is often cultural rather than procedural. Our experience suggests that engagement of the implementors

CASE STUDY – GAS DISTRIBUTION; CONTROL PERFORMANCE INDICATORS

Their challenge

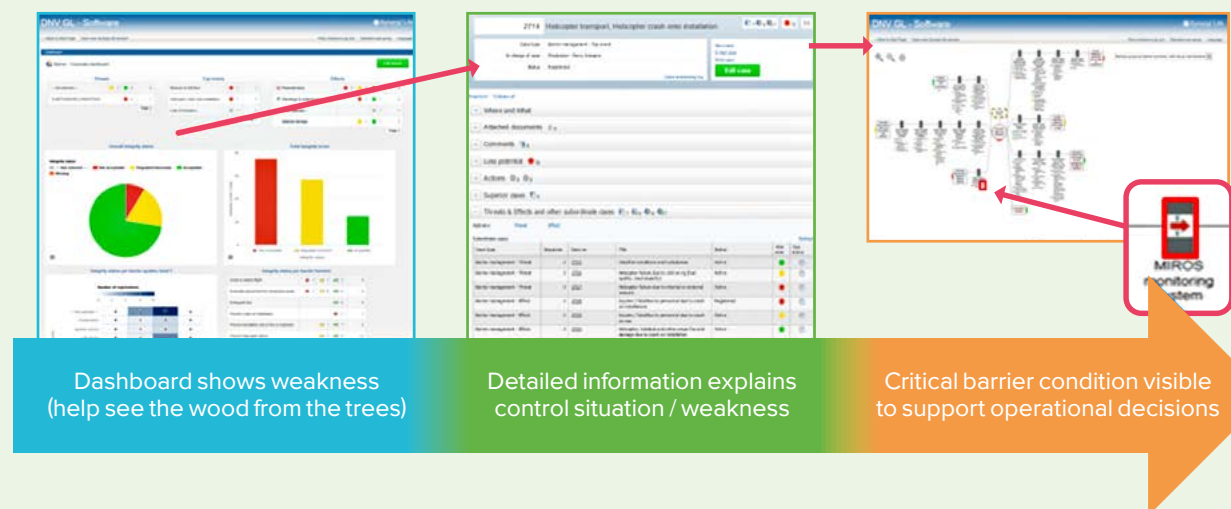
The organisation did not have a set of indicators to be able to demonstrate that their controls were working successfully. As such, they did not have a means for providing assurance to senior management that they were in control of their operational risk.

Response

Focusing on the key operational risk events, critical controls were identified and understood/detailed. From this, performance indicators for the controls were developed to provide an indication on the condition/status of the controls and the adequacy of what maintains their performance. These were run for a period and then revised to gain better assurance for both senior management and operations.

Multiple sites use the indicators to report their performance in a consistent manner, allowing tracking and management action to be taken.

The concepts explained in the case studies are evolving to improve monitoring and review, and hence improvement/update. Organisations are looking to operate “live control dashboards” that allow those responsible for business and operational activities to understand the status and condition of their risk controls. From this they can make operational risk decisions as well as identify and implement both corrective and improvement actions in a timely manner.





Above: Live control dashboards supporting operational decisions and fast response/improvement.

“A key aspect of monitoring and review is to address the “so what?” question

with the risk management process is key. The traditional process of pushing information to the implementors for action has largely proven to be problematic, resulting in difficulties in maintaining sustainable performance. Much more successful have been pull approaches that incentivise implementors to take ownership of the risk management process and ask for the analytical support to deliver success – the case studies illustrate two such mechanisms.

Democratising risk management – getting engagement from the few to the many – is a more effective and sustainable approach to implementing risk management. Assurance, using tools like ISRS, allows a big-

picture view of the effectiveness of risk management processes, and the extent of engagement of the organisation in delivering success. If that view is generated independently and is benchmarked against industry peers and examples of best practice, it tends to have more weight and stimulate better management decision-making. Ultimately it is about all levels of the organisation being able to confidently demonstrate that they are in control of risk. 

 Mark Boulton (CFIRM) and Mark Fisher are directors at DNV GL consultancy. The workshop took place at IRM's 10th Risk Leaders Conference in London in November 2019.



Reach a global audience

While it has been a difficult couple of months, IRM's interest groups have successfully adapted to serve members online, says Rahat Latif

When I took on the role of chair of IRM's Interest Group Committee last year, I sought to obtain the views of all the interest groups about what areas they'd like to see IRM improve or enhance.

Two areas which got a particularly high vote were better sharing of live events via webinars to a global audience, and more collaboration between the interest groups.

One consequence from the current restriction on movement and social contact has been that it has forced events onto online platforms and hence fulfils those wishes. It's really great to see that many of the interest groups have positively embraced this move.

Since March when social distance rules came into place, the following groups have held webinars: Qatar Regional Interest Group (RIG) on pandemic planning and building financial resilience; Innovation Special Interest Group (SIG) on innovation and another on resilience; Energy SIG on global events, pandemics and the future of oil and gas; NED and CRO SIG launch event; IOR England and Wales on COVID-19 – black swan or grey rhino?; Infrastructure RIG on sharing best practice globally; Pakistan RIG on COVID-19, crisis management and business continuity; Switzerland RIG on employee mental health.

Intimately involved

By and large, discussions on the pandemic have supported the results of IRM's recent survey in highlighting that risk managers have been intimately involved in supporting the management of the crisis, through for example scenario analysis and planning and risk-based decision-making. Beyond the crisis, organisations will be looking for their ERM teams to evolve to provide leadership on a holistic approach to risk and resilience management.

On June 11, 2020, Kingdom of Saudi Arabia and Bahrain RIG will host a webinar on business continuity and resilience; on June 29, 2020, IOR England and Wales will host a webinar on risk governance oversight – good practice and challenges.

I've been receiving very positive feedback on the webinars' effectiveness. Interest groups have


said that, while the lack of physical proximity is an obvious disadvantage, this is counterbalanced by the significant advantage of being able to attract a global audience, together with the ability to interact with them through the message, video and voting features of the webinar technology. Not only that, webinars usually have higher attendance than their "physical" counterparts. For example, the Pakistan RIG webinar I was part of recently recorded an audience of 130. The IOR England and Wales one attracted 149.



In the absence of physical meetings at this time, I would encourage all interest groups to try running webinars and to collaborate with other interest groups

Greater collaboration

The online events have also provided a great opportunity for inter-group collaboration. For example, the Climate Change SIG chair was an invited speaker at the Energy SIG webinar. Similarly, the Midlands RIG also collaborated with the Innovation SIG for their online event. Not having to travel, naturally, makes collaboration that much easier.

In the absence of physical meetings at this time, I would encourage all interest groups to try running webinars and to collaborate with other interest groups. In fact, even when things are back to normal, my guess is that given their success we will continue to see more webinars in addition to regular events. At IRM we will look into the possibility of doing both concurrently – running a regular physical event with a live global audience! 



Rahat Latif is chair of IRM Interest Groups Committee and IRM board member.

Due diligence solutions



Minimise risk by maximising the data that supports your most critical business decisions. LexisNexis is a leading provider of aggregated global content and powerful business intelligence tools. Protect your organisation from the risk of heavy fines and damage to corporate reputation by accessing the information you need on people, companies and countries. Our cost effective and

flexible product modules include: PEP, sanctions, watch list and negative news screening. Enhanced due diligence and reporting. Proactive supply-chain and third-party risk media monitoring. Outsourced due diligence, compliance and risk advisory. Content integration and data feeds (APIs) into proprietary systems.

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

Integrated Risk Management



Riskconnect is the leading integrated risk management software solution provider. Our technology empowers organisations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise. More than

900 customers across six continents use our unique

risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskconnect has more than 500 risk management experts in the Americas, Europe, and Asia. To learn more, visit www.riskconnect.com

 **Mark Holt**
 **+44 (0)7435 607 892**
 **mark.holt@riskconnect.com**
 **www.riskconnect.com**
 **8 Lloyd's Avenue**
London
EC3N 3EL

Enterprise risk management and risk analysis software



riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud based, the 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. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

 **Ian Baker or Doug Oldfield**
 **+44 (0) 1275 545874**
 **ian.baker@riskhive.com**
doug.oldfield@riskhive.com
 **www.riskhive.com**
 **riskHive Software Services Ltd.**
Dilkush, Farlers End
Bristol, BS48 4PG

Risk and audit management software solutions



Symbiant are one of the world's leading providers of Risk and Audit management software. The solution is designed for collaboration and comes as a complete suite which can be separated in to Audit or Risk sets. Symbiant is designed for non Risk / Audit specialists to use, simple and intuitive but with a lot of back end flexibility and automated functions. CIO magazine

have rated Symbiant as one of the top 20 risk solutions in the World. They have off the shelf or custom solutions to fit all budgets and requirements. Install on your own infrastructure or SaaS. 30 day free trial.

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

Risk management software



Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while 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, providing integrated solutions to the entire

insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. 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) 16179 17740
 nscotcher@origamirisk.com
 www.origamirisk.com
 30 Moorgate
London
EC2R 6PJ

Risk management software



In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and implementation of risk management. Protecht helps organisations through

deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

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

To advertise here contact: Redactive Media IRMSales@redactive.co.uk +44(0)20 7324 2753

Homeward bound

Executives are beginning to wonder if high-rise office blocks will become a thing of the past, yet homeworking brings its own risks

Number 22 Bishopsgate is a 62-storey skyscraper that will be the tallest building in the city of London when it is completed later this year. It has about half a million square feet of space and could hold 12,000 office workers.

At the moment, those people are at home. Offices throughout the city are empty as the pandemic has effectively shut white-collar workplaces in many cities throughout the world.

Jes Staley, chief executive of Barclays, is looking to implement a more decentralised approach to working in the future – which is likely to mean that, for some, homeworking becomes the norm. “I think the notion of putting 7,000 people in a building may be a thing of the past, and we will find ways to operate with more distancing over a much longer period of time,” Staley has said.

Staley seemed surprised that the £1.4 billion business could operate with around 80,000 staff working from home. But digital technologies have kept much of the middle-class population busy. Some staff have been asking whether such arrangements can stay in place after the threat of the pandemic has passed.

Co-working explosion

But homeworking can have long-term health risks. Freelancers have known this for years, which is why many choose to carry their laptops to co-working spaces. In December 2019, the Coworking Resources agency estimated that almost 1,700 new offices dedicated to this form of office space opened in 2019 alone – with London and New York dominating the market.

“The wellbeing of members is high on the list of priorities for co-working space providers, with a number of companies making it their USP,” said the firm.



Image credit: Chrispictures / Shutterstock.com

“Forcing everybody home, often around kids, in shared rooms or bedrooms and no escape socially in non-work time will be generating major mental stress


While the trend-setters may like to depict home-working spaces as light, airy and filled with aromas of coffee, the reality can be grim.

“Forcing everybody home, often around kids, in shared rooms or bedrooms and no escape socially in non-work time will be generating major mental stress,” Nick Bloom, a senior fellow at Stanford Institute for Economic Policy Research, who has researched the impact of homeworking on productivity, told the *Financial Times* recently. “This typically leads to loneliness and depression.”

The newspaper said that Bupa, a private healthcare provider, had reported that workplace psychologists were fully booked for virtual consultations – and that calls to its health and wellbeing advice line were up 300 per cent since the crisis started. It is hiring more mental health professionals as a result.

Future normal

Given the novel nature of our current lives, there is no certainty about how the pandemic will develop. If we are lucky, it will evaporate like its predecessor SARs. More likely, the virus will be around for a while. In the short-term, communication is key. Many staff have been furloughed and hear nothing from week to week, which can increase anxiety and bring on depression – both conditions associated with too much uncertainty. CIPR have issued useful guidance on how to act considerately.

Longer-term, organisations need to balance an awareness of the risks of working on site with those of working from home for longer periods. Thinking solely about bottom-line savings on expensive office space is unlikely to pay dividends for anyone. 

Supply Chain Risk Management Certificate

Identify, analyse & prevent

NEW

About the Supply Chain Risk Management Certificate (SCRM)

This qualification introduces the concepts of SCRM and equips risk practitioners with the ability to apply their risk management knowledge in a world where value is increasingly added via a supply chain. It explains how globalised outsourcing, specialisation and just-in-time production are changing the risk environments for many organisations.

It looks at how appropriate risk management tools and techniques can be applied, adapted and developed in an increasing digital context. The qualification also provides a broad understanding of SCRM principles and practices. The relevance of the qualification is explained in the context of increasingly extended organisations facing an expanded range of complex interconnected risks.

What our experts say



Robert J Trent PhD
Professor of Supply Chain Management, Lehigh University

"Far too many companies gain an appreciation of supply chain risk only after suffering directly the adverse effects of risk. This certificate provides people with the knowledge, concepts, and tools to enable them to become a valuable part of their organisation's efforts to survive and prosper in an ever changing world."



Nick Wildgoose
Independent Supply Chain Risk Consultant

"There are supply chain disruption and reputational incidents happening every day, that could have been better managed to drive value. This new qualification will help learners develop a clear understanding of supply chain risks, and the tools and technology which can help organisations stay protected."

In collaboration with

SUPPLY CHAIN RISK MANAGEMENT
CONSORTIUM™

Find out more at:

www.theirm.org/scrm-mag

Resilience, risk and recovery



Developing risk professionals

WORK WITHOUT LIMITS

Symbiant[®]

Risk, Audit and Compliance Management Software

COLLABORATE FROM ANYWHERE

For more information and a free trial visit
www.symbiant.co.uk

