

Enterprise Risk

Spring 2023 / www.enterpriseriskmag.com

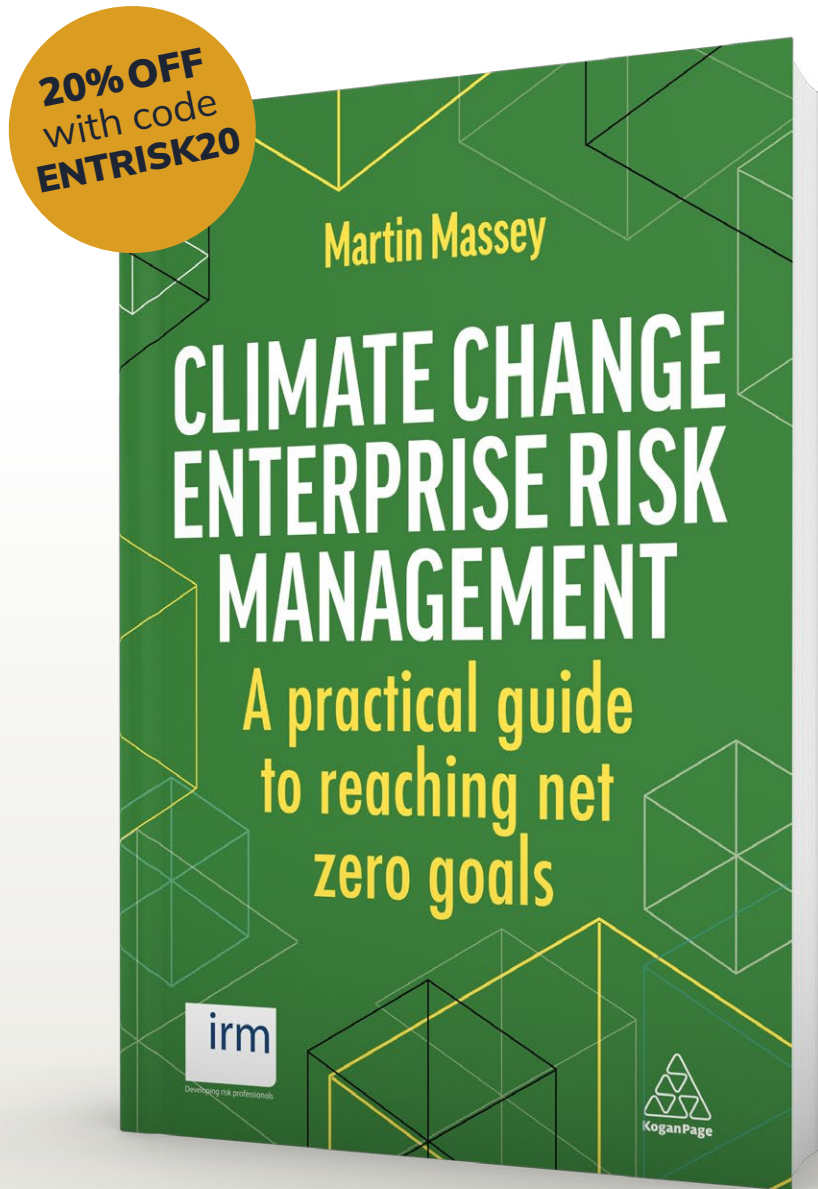
The official magazine of the Institute of Risk Management

Risk management for a new era: Mykhailo Rushkovskyi on why risk professionals need to help businesses adapt to the new reality in an age of decentralisation



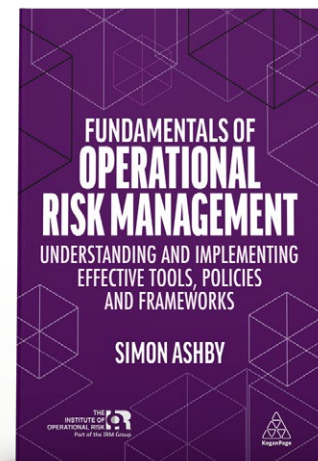
The deep learning revolution: latest AI tools explained / **Through a glass darkly:** blinded by standards and best practice / **The road ahead:** IRM's global threat predictions for 2023 / **Taking control of operational risk:** big catastrophes provide much-needed insight

Develop practical strategies to manage climate-related risks

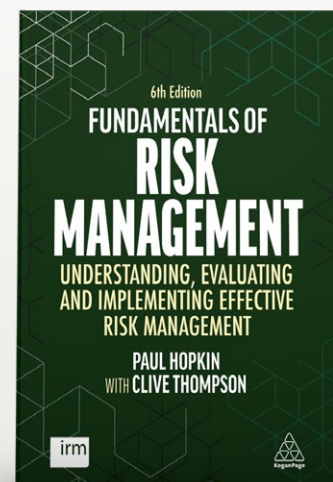


9781398608702

Also available...



9781398605022



9781398602861

SAVE 20% on all Kogan Page Risk and Compliance books at koganpage.com/Risk with code **ENTRISK20**



 @KPBUSINESSMgmt



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.

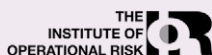
We do this by providing internationally
recognised qualifications and training,
publishing research and guidance, and
setting professional standards.

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 © 2022 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.



Curb your enthusiasm

Uncertainty has boosted the profile and role of risk managers. Not only do unexpected, large-scale risks happen more frequently than anyone could have predicted three years ago, but risk models that are overdependent on historical data seem doomed to irrelevance. Decision-making today needs solid, predictive risk management to cope with an increasingly opaque business and geopolitical landscape.

And that means applying the right risk management tools. But what are they?

While the features in this issue of *Enterprise risk* do not provide definitive answers, they do open the door for some fruitful debate. Michael Grimwade (*Taking control of operational risk*, pp 30-34), for example, shares some deep analysis into the effectiveness of operational risk in the financial services sector. Disturbingly, he found that an overwhelming number of risk managers focused their risk and control self-assessments on the wrong type of threat.

“Are you too fond of using the same tried-and-tested techniques?”

In addition, Elmar Kutsch (*Through a glass darkly*, pp 22-25) found that tried-and-tested risk management processes often become ineffective because people tend to apply them to those kinds of predictable risks that businesses generally manage well. In other words, the tools and the threats are so well suited that people can forget to look at those risks that are hard to measure and predict. The old adage “what gets measured gets done” in this context could be a recipe for disaster.

If these articles suggest a retuning of established techniques, Richard Bendall-Jones (*The deep learning revolution*, pp 16-20) offers something different. While media narratives around AI often polarise between shock and awe, Bendall-Jones gives some real-world advice about how to start applying deep learning to risk management.

Surprisingly, perhaps, the answer mirrors the conclusions of the two other features I have been discussing. To state it in oversimplified terms – make sure the risk tool and the risk area are aligned as well as possible. “Deep learning approaches work best with structured data sets looking to solve well-defined problems,” he says.

This raises important questions for risk managers about their attitudes to the tools they use. For example, are you too fond of using the same tried-and-tested techniques, or do you rush to apply your newly acquired AI program to every piece of data that you can find? Taking a fresh and dispassionate view of what is in your risk management toolbox could help.

Arthur Piper
Editor

**Supercharge
your career by
improving your
risk knowledge**



Scan me!

International Certificate in Enterprise Risk Management

Risk is part of every business, from the pandemic-to cyber threats-to supply chain disruptions. Study with the IRM to improve your career and earning potential by gaining a solid foundation in the theory and practice of effective risk management.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm



10



16



20



26



30

Features

10 Risk management for a new era

Russia's invasion of Ukraine has not just brought war to Europe, it has upended both the global energy industry and risk management practice. Mykhailo Rushkovskyi says risk professionals need to help businesses adapt to the new reality in an age of decentralisation

16 The deep learning revolution

Recent developments in artificial intelligence promise a new wave of risk management techniques and approaches. But getting the basics right is key to success

20 Through a glass darkly

The very standards and practices used to manage risks could be blinding organisations to their biggest threats

26 The road ahead

IRM risk trends 2023 maps the territory for organisations looking to navigate future uncertainties

30 Taking control of operational risk

The nature of operational risk is poorly understood, and the tools can sometimes fail to add value. But a penetrating study of the financial sector's biggest catastrophes provides some much-needed insight

REGULARS

7 IRM Viewpoint

IRM is deepening its collaboration with educational partners, launching student awards and widening participation

8 Trending

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

36 Directory

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

38 Toffler

Time management and productivity have become buzzwords of the global self-help industry – but do their methods make matters worse?

Changing perspectives on risk

Black Swans, Grey Rhinos and the growing importance of effective risk management, by Craig Adams

At the end of last year, China Banking and Insurance Regulatory Commission chairman Guo Shuqing warned that “Black Swans and Grey Rhinos were lurking”. His

comments were in reference to the growing number of financial enterprises within China that were at risk of failure, and the need to remove such “rotten apples” both quickly and efficiently for the good of the wider economy. But what exactly are Black Swans and Grey Rhinos, and more importantly, what can risk managers do about them?



create much more damaging situations. For example, many people believe that the pandemic was a Black Swan event. However, others believe it was a combination of predictable Grey Rhinos, such as poor investment in vaccine

development, a growing global population and humans’ ongoing encroachment on animal habitats.

What are the practical implications for risk managers?

In simple terms, the pandemic was perhaps more predictable than it first appeared, just like many other

said concerns ever become reality.

Technology is playing a bigger and bigger role in this process, with enterprise risk management solutions, in particular, growing significantly in popularity and adoption.

Not only do they enable organisations to view, analyse and understand all of their key risk factors in a single platform, but they also allow risk professionals to measure overall risk culture within the organisation, track changes over time and identify key challenges faced.

Doing so enables them to assess risks in more sophisticated ways, bringing a greater number of Grey Rhino issues to the fore early, where

Black Swans vs Grey Rhinos

The term Black Swan is used to describe highly unpredictable events that carry severe consequences. Natural disasters are a great example, so too are acts of terrorism and war, financial crashes and, of course, pandemics. Conversely, a Grey Rhino is a threat that is highly obvious but largely ignored, such as climate change, or the emergence of disruptive technology. Despite the fact everyone can see it coming, nothing is done until it’s generally too late.

When is a Black Swan not a Black Swan?

There’s a growing belief that Black Swans often aren’t as unpredictable as claimed. In fact, in many cases they are the culmination of multiple Grey Rhinos, which have been ignored for so long that they end up combining to





For risk managers looking to insulate their organisations against future shocks, there are numerous key lessons to be learnt

events that regularly occur within the business world. The clues were there, but they were simply ignored, and/or not pieced together effectively to reveal the bigger picture.

For risk managers looking to insulate their organisations against future shocks, there are numerous key lessons to be learnt here. From global events down to much smaller internal concerns, acknowledging the risks, understanding the risks and putting the right preventative measures in place can all have a significant positive impact should

they are less likely to be ignored until it’s too late, or worse, they morph into a Black Swan event.

For many organisations, minimising risk starts with changing their perspective on it. Only when it is seen from the correct angle can the correct actions be taken to address it. 

 **Craig Adams is managing director, EMEA, at Protecht.**
Contact at craig.adams@protechtgroup.com.

Boosting student services

IRM is deepening its collaboration with educational partners, launching student awards and widening participation

IRM is working collaboratively with a number of universities to accredit our programmes and recognise prior learning. These include Glasgow Caledonian University, Bayes Business School (formerly Cass), University of Portsmouth, DeMontfort University, University of Leicester, and University of Southampton.

The accredited programmes are predominantly master's degrees in risk management, crisis and resilience management, corporate risk and security, and insurance and risk.

Developing capabilities

On our courses, students benefit from free IRM student membership for the duration of their studies. This is a great opportunity for them to start building a professional network, develop their risk capabilities and stay up-to-date with the latest insights in professional practice.

Depending on the nature of each degree, graduates are entitled to exemptions from the first two modules or all six modules of the International Diploma in Risk Management, being awarded Certificate (IRMCert) or Graduate (GradIRM) membership, respectively.

"We recently visited IRM in London with a group of students reading for a master's in risk management," Professor Sudesh Sangray from DeMontfort University said. The presentation

brought together many strands of academic and professional learning, exemption leverage, and potential career trajectories in the field of risk: "The value-added of the interaction between students and IRM cannot be understated, and students gain an enhanced appreciation of their studies in a regional, national and global context".

Recognising talent

This November, IRM is set to launch the first university student awards, aimed at recognising the top risk management students from accredited programmes with partner HEIs. The aim is to support students' transition to practitioners, strengthen partnerships with universities and expand the diversity of ideas for thought leadership in the risk community.

The winners will be nominated by their universities and receive a free upgrade to professional membership, their first year of membership covered, one training course of their choice and mentoring from experienced members by joining the committee of a Regional or Special Interest Group.

The prizes are set out to encourage graduates to continue with their professional development journey with the Institute and help them flourish as future risk leaders.

Wider offering


Free student membership is now available to anyone studying risk


management or business and management sciences at a university or other institute of higher learning.

Historically, this offer was exclusive to risk management students. But as the profession evolves and the global business landscape remains volatile and uncertain, the type of roles undertaken by risk professionals is growing incredibly diverse. Risk management spans all business and management disciplines across all sectors globally.

We saw an opportunity to broaden the criteria and attract student members from different academic backgrounds.

The role of IRM as the leading professional body for enterprise risk management is to ensure professionals have the support to implement effective risk management from early in their careers.

This initiative aligns with IRM's strategic pillars by elevating the membership offer to students, building international collaboration and partnerships with universities and other institutes of higher learning and subsequently creating impactful global thought leadership while developing the risk leaders of tomorrow. 

 Lucas Morais, IRMCert, is IRM's student services manager.

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

Hybrid working increases data risk

Organisations struggle to comply with data rules and almost one third have seen an increase in breaches and data violations



It has increased the potential breach/attack surface

45%

Data is being shared on devices and through systems that are not sanctioned or covered within the organisation's data privacy policies

41%

It has made it more difficult for us to monitor compliance with and enforce data privacy policies

38%

It is more difficult to uphold employee training/awareness

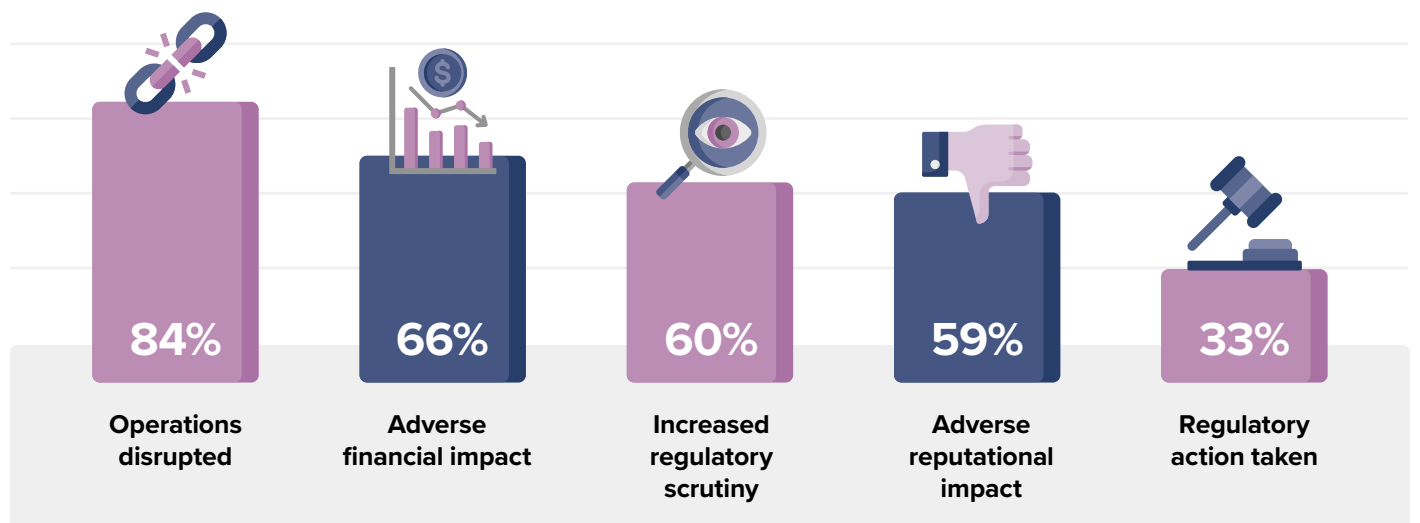
37%

We have experienced an increase in data breaches and/or violations of data privacy regulations

32%

Source: FTI Consulting, *The most valuable, vulnerable commodity: data establishes a new era of digital insights and risk management*

ERM failing on third-party risk

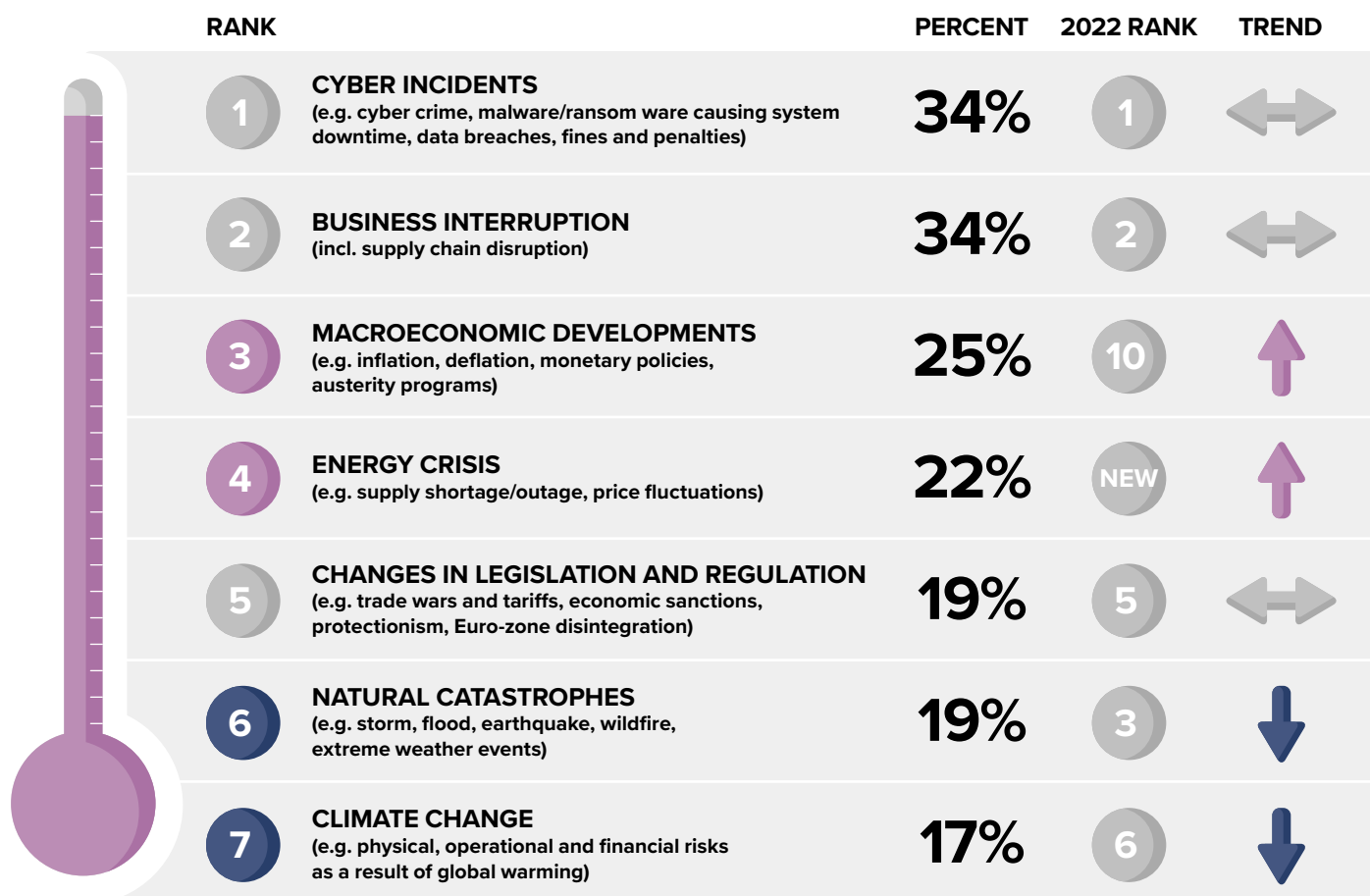


Source: Gartner executive risk committee research, 2023

Organisations reassess risk landscape



Natural catastrophe and climate change risks edged down by global turmoil

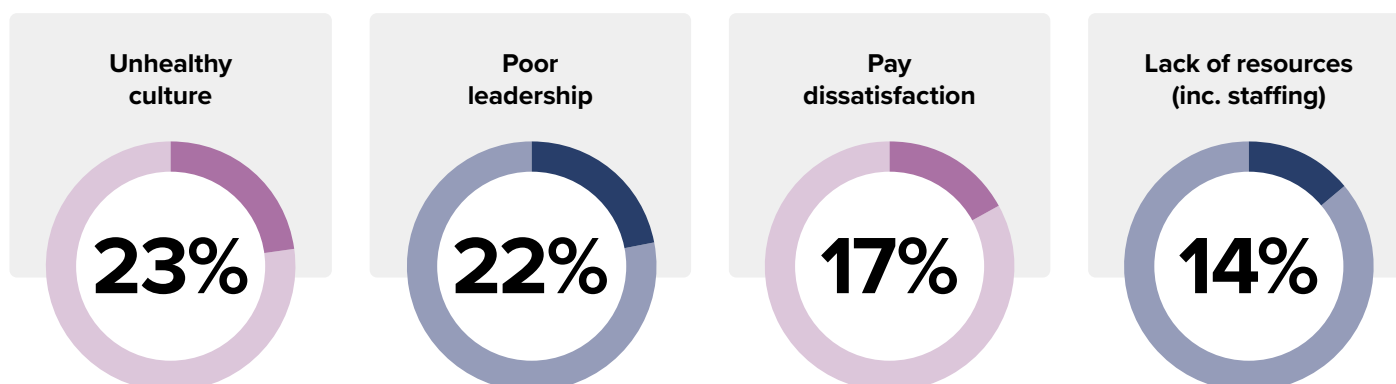


Source: Allianz Risk Barometer 2023

Four in ten seek new roles in 2023



And most leave because...



Source: New possible – what workers want 2023 survey



Risk management for a new era

BY ARTHUR PIPER

Russia's invasion of Ukraine has not just brought war to Europe, it has upended both the global energy industry and risk management practice. Mykhailo Rushkovskyi says risk professionals need to help businesses adapt to the new reality in an age of decentralisation

It may seem unbelievable now, but oil dropped to around minus \$37 a barrel back in April 2020. A mixture of low consumption during some of the worst days of the COVID-19 outbreak and a subsequent lack of storage at traditional facilities meant there was nowhere to put scheduled deliveries. The US benchmark price known as the West Texas Intermediate slumped from \$18 a barrel on Monday 20 April, dropped into single digits, before crashing through zero as producers paid customers to take the excess off their hands.

At the time of writing, crude spot price on the index is bumping along in the mid-to-high 70s – although there is some volatility

that has seen values drop lower. The Russia's war in Ukraine has not only affected prices though. Perhaps more importantly for the coming decade, it has uncovered long-standing structural problems in the global energy sector, says Mykhailo Rushkovskyi, Head of research and analysis at Kyiv Consulting, PhD researcher in risk management and founder of the Runderc, the internet portal for risk managers.

Power problems

"There is no doubt that the challenges predicted in the energy sector during the past few years have been partially realised," he says, speaking from his office in Kyiv, Ukraine – and not just

because of the war. Just before Christmas, for example, much of the US was gripped by arctic conditions that left about two million people without heat or light. Power outages throughout the region increased as people tried to keep warm at the same time as freezing conditions damaged infrastructure. The incident has not been the only extreme weather event in recent years to batter energy networks.

The problem, according to Rushkovskyi, is that centralised networks coupled with power plants powered by coal, gas, nuclear or renewable resources have little redundancy built into them. "Once you have damage to this specific power



“ It would be more rational to have decentralised systems and smart grids



Image credit: Main Directorate of the State Emergency Service of Ukraine in Kharkiv Oblast

Fire at an energy infrastructure facility after Russian shelling

grid that connects the producer and consumer, we experience blackouts on a scale of 10-15 minutes, or even days depending on the situation,” he says.

The second strand of the problem is how the energy system retains its equilibrium between suppliers and consumers. Normally, supply and demand are balanced so that ups and

system from Russia and Belarus to undergo testing before joining ENTSO-E – Europe’s equivalent. After several weeks of isolation, Ukraine managed to complete physical operations to connect its power system with the European energy network. But nationwide, power outages have continued as Russia continues to target Ukraine’s energy infrastructure.

weaknesses to natural events or man-made catastrophes,” he says. “It would be more rational to have decentralised systems and smart grids. That is what we are now doing in Ukraine – creating a parallel, independent energy production system – a more decentralised network.”

Fragmented world

In fact, it is not just war and natural catastrophes driving this change – but since the 2020 COVID-19 global lockdowns the world has become more fragmented. The emergence of China as a super-power economy and the geopolitical tensions that this event is creating have further disrupted global ties, trade and logistics. In addition, Brexit, tensions between the old and new Eastern European political allegiances and shifting power balances in the Middle East are all indicators that regionalism is on the rise in a reshaping global world.

“Do not be someone who

“ Do not be someone who is still living in 2019 – we are done with that

downs within the system can be tweaked as necessary. That works fine until there is disruption. Up until February 2022, for example, Ukraine was synchronised with Russia and Belarus in a single energy system. A few hours before the Russian invasion, NEC Ukrenergo (the country’s electricity operator) disconnected Ukraine’s power

Rushkovskyi believes that while making this move to use European energy system was essential, it leaves a faulty structure in place. Ukraine and developing countries and regions would be better served by a less monolithic, more regional approach. “If you instal power grids along a whole continent, for example, it requires a huge amount of investment with inbuilt



You can use such local, modular reactors to generate enough power for half a city and establish production absolutely independently from any national grid

is still living in 2019 – we are done with that,” he says. “The regionalisation we are facing is likely to last a minimum of ten years, but we should use this decentralisation wisely.”

That brings our conversation back to the practicalities of energy production and supply. Ukraine has been learning the hard way about the benefits of decentralisation. There are planned power outages most days, but many organisations have installed small generators – around 5 kilowatts for a coffee shop – that can make the business totally independent from the overall energy network. “Once there is a blackout, they switch on their own power generator – and you can drink your cappuccino without interruption,” he says. The locals joke that while you can sit without a light in Kyiv, you can always drink a good coffee. In fact, part-way through our call the lights do go out on our online video conference at Rushkovskyi’s end until the reserve power kicks back in around 10 seconds later.

Hybrid and decentralised

In effect, what he is suggesting is a hybrid system where customers benefit from the centralised system, but they also have the capability to be independent if they need or chose to be so. At his apartment, for example, he has built up energy storage facilities with solar panels compatibility. “Your backup plan includes independent generation and independent storage – a solution that brings the necessary level of energy supply resilience.”

He says that this approach paves the way for introducing more renewables into the energy system – but with realistic alternatives if power

outages are likely to be long and unpredictable. For example, solar panels and wind turbines (together with appropriate storage facilities) could be combined with local diesel generators so that the later can make up for any shortfalls. Small neighbourhoods could join together depending on their capabilities and needs. But when things go wrong, there would still be energy countrywide.

That does not mean that over the coming decade existing energy companies will cease to be the major suppliers of energy, but he believes that adding more diversity to the mix of sources – from renewables to nuclear is on the way. In fact, he describes himself as a supporter of nuclear power. In 2020, Ukraine was the seventh biggest generator of energy from that source in the world, with fifteen active reactors. In November 2022, the US and Ukraine announced that they would work together to build a small modular nuclear reactor in the west of the country. The pilot project aims to test whether it is possible to bring electricity to rural areas with lower-grade power grids, especially in places where it would not be cost-effective to construct a full-scale plant.

“You can use such local, modular reactors to generate enough power for half a city and establish production absolutely independently from any national grid,” he says. “That can be the basis for helping develop those regions, to move gradually to renewables with wind, solar and other biofuels. You need to provide the necessary levels of physical and IT security, but it could work not just in Ukraine but in developing countries too.”

Risk management

Rushkovskyi switches easily from the big picture to specific, practical and pragmatic solutions – he is both a risk manager and a PhD candidate at Taras Shevchenko National University of Kyiv. He was also winner of the European Risk Management Awards 2022. While he sees risk management being able to play a “super-critical” role in helping businesses transition to a more resilient energy infrastructure, he believes that many have not yet caught up with the large risk events that have shaken the certainties of a globalised world over the past three or four years.

When Russia was hit with sanctions back in 2014, he says that many European businesses were slow to cut ties with the affected suppliers. When they did begin to make the switch, instead of thinking about diversifying their supply chains to future-proof their businesses many simply looked for a single source to replace Russian gas – liquified natural gas (LNG).

“LNG makes sense,” he says, “but it is not a magic bullet. “We cannot go from one extreme to another – relying on one source for 50 per cent of our energy, to a different one at the same level.” He says it is an open question whether there is enough production capacity globally to meet Europe’s needs on such a scale – and the infrastructure investment required is huge. In fact, the potential difficulties of such a strategy were highlighted last year. Freeport LNG in Texas was supplying Europe with about 10 per cent of their supply by June 2022 when it shut down because of an explosion at the plant. The gas is only just beginning to flow again. In addition, the pandemic showed how vulnerable

supply chains could be when dock workers were furloughed or sick for months on end.

“If we see a good opportunity, the danger is that we may blindly follow it,” he says. “Every strategic shift, any big project includes risks that sit beside the opportunities, which is why it is super crucial for risk management to step in.”

Business focused

Rushkovskyi believes that risk management needs to be well-positioned in the governance structure within organisations. The old-style, second line of defence – where the function sits between line management and internal assurance – can degenerate into quarterly box-ticking exercises if organisations are not careful. While it is important to carry out such day-to-day monitoring, the responsibility for who owns risk is key, he believes.

“If the responsibility does not sit at the top level of the organisation, risk management does not work properly – this is true for international organisations, governments and enterprises alike,” he says. “No responsibility equals no results.”

The simplest way to make such responsibility stick is to link a risk to a specific financial indicator and find someone high up in the organisation who is willing and able to take it on. That can be a supervisory board, for example, or a chief financial officer – but it must be someone who is genuinely interested in and responsible for mitigating the risk and whose bonus, for instance, depends on them doing so. He makes a distinction between risk and compliance in this respect. While compliance comes from regulations, it can be back-ward looking and is generally imposed from above or outside the organisation. Responsibility, on the other hand, must come from the bottom.

“We need to start from this type of practical, bottom-up approach,” he says. “Regulation is

top down – but the real interest, the real risk owners and the people who are mitigating the risk are a few levels below; so the interest for mitigating the risk must also be there.”

Risk management 2.0

For that to work well, and here we are getting into the crux of his PhD research, risk management must speak the language of the business. It is an approach he calls Risk Management 2.0 – see, *three pillars of risk management 2.0*. It is not enough to tell a chief

and demonstrate that not dealing with the risk could derail efforts to achieve sales. In other words, the risk must pose a concrete threat to the person mitigating it.

“You always need to translate risk management language into the business’ own language,” he says. “Once you make this translation work, you have found the key to relevant risk management.”

The biggest blocker to taking this approach is usually internal corporate culture, especially when organisations are driven only by



You always need to translate risk management language into the business’ own language

sales officer, for example, that they must both hit their annual sales target and mitigate a key risk. That could create a moral hazard because the risk mitigation could simply involve ticking boxes so that the sales executive can focus most effort on hitting their sales target. Instead, the risk manager must be able to show

extremely ambitious financial goals that take too little account of risk. “Fancy goals create a sort of tunnel vision,” he says. While this may work well in the short-term, the view assumes that the past is a good measure of the future. Those who do not appreciate how far the world has moved since 2019 are likely to be hit hardest when

THREE PILLARS OF RISK MANAGEMENT 2.0

- **Pillar one:** traditional second line of defence risk management with its formal standards and practices.
- **Pillar two:** adequate insurance. If real, catastrophic risk is on the rise that cannot be mitigated, organisation should purchase tailored coverage for the businesses specific risk exposures. (The risk of not taking the bespoke route is that organisations have general insurance that does not fully mitigate potential losses and each year the premiums increase.)
- **Pillar three:** risk management becomes an internal consultant. This is something that businesses can achieve when they reach a certain level of maturity. It requires a very competent team of open-minded, curious risk professionals. Such a team can see the whole risk landscape – inside and out – and provide a service to rival large consultancies but at a fraction of the cost. “Because you are already in-house, you know precisely how recommendations can be implemented and what the likely pitfalls will be,” Rushkovskyi says.

risks inevitably hit home. A second stumbling block to achieving the benefits of risk management 2.0 are those who focus on too much detail and mire projects in processes and procedures.

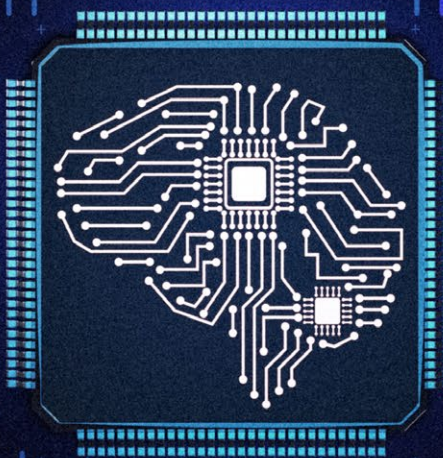
Rushkovskyi's holistic, pragmatic philosophy has come from a career working in risk – initially in reinsurance at Marsh Europe, then at Generali as a risk's underwriter – which was when he also sat for an MBA at MIB School of Management in Trieste, Italy. After a stint at Allianz, where he was employed as chief risk officer, he moved into setting up enterprise risk management at organisations where he had the freedom to start with a clean state – Naftogaz of Ukraine, the largest national oil and gas company, and then DTEK – the largest privately owned energy holding in Ukraine. He says it was then that he realised that risk management systems had to be carefully tailored to the specific needs of an organisation and communicated in a way that chimed with those responsible for mitigating it. "It was a case of learning by doing and doing by trying," he says. "When we started to see good results and understanding, I thought we could perhaps standardise our approach – which is the goal of my PhD." He has submitted the document now and it is going through the final stages of assessment at Taras Shevchenko National University of Kyiv.

While the thesis draws on the larger geopolitical and economic trends for its background, his aim is for risk professionals to take whichever parts of how work they find practical, adjust it to their enterprise and put it into action. "You should be able to run risk management through any system and end up with better operational efficiency, fewer costs and many other things," he says. "It should allow you to take a holistic view of any area of the company – not just the details, but the bigger challenges. Risk management 2.0 is as simple as that." 📄



THE deep learning revolution

BY RICHARD BENDALL-JONES



Recent developments in artificial intelligence promise a new wave of risk management techniques and approaches. But getting the basics right is key to success

In recent years, the field of artificial intelligence (AI) has seen rapid growth and development, and one of its most promising branches is deep learning. There has been a lot of press and social media coverage about the most recent chatbot, ChatGPT, and the benefits that this technology may bring to society, for example.

Deep learning is a type of machine learning that uses algorithms that can be employed to forecast a range of potential future outcomes. It is tempting to say that deep learning merely has great potential to offer significant benefits. In truth, it is already being implemented, in a practical sense, on projects and within organisations to inform decision-making and compelling action to manage risk.

Deep learning is a type of machine learning that uses neural networks, or artificial neural networks, to process and analyse data. Mimicking a biological brain, these neural networks are designed to learn from and recognise patterns in data, allowing them to make predictions and suggest decisions based on that information. In an organisational or project context, this could mean taking historical data and using the deep learning models to forecast potential future outcomes, which would then drive a discussion about what to do about it, ultimately resulting in action being taken, and the outcome feeding back into the data set.

Human interaction

You are probably already using deep learning as a part of your life.

We interact with deep learning technology in many ways, such as through voice-activated virtual assistants like Siri and Alexa. Another example can be found with Google Maps, which recently announced accuracy improvements of up to 50 per cent by deploying a new type of neural network to predict journey

often found in qualitative and quantitative risk management methods. By providing forecasts and other insights based on historical information, teams and organisations can make decisions that are freer of bias, with the aim of more quickly getting to the root of problems, or uncovering opportunities.



Mimicking a biological brain, these neural networks are designed to learn from and recognise patterns in data

outcomes. But deep learning is not only about serious stuff. The music app Spotify, for example, applies deep learning algorithms to accurately predict which songs you may enjoy based on your previous listening habits. Deep learning is already with us, and bringing benefits to how we live our lives, even though in a risk management context it is a relatively new kid on the block.

Deep learning in risk management

A fundamental element of any effective risk management strategy is to enhance and support an organisation's decision-making process. Deep learning can play a significant role in this process by providing organisations with a more efficient and accurate way to understand the range of potential outcomes, based on empirical historical data, in comparison to the subjective approaches

For example, deep learning can be applied in a fraud detection environment. By deploying a deep learning model to learn from the behaviour of transactions and actors, it can more accurately anticipate fraudulent activity and see it from further away. Similarly, insurance companies can use deep learning algorithms to analyse vast amounts of data, such as claims data and weather patterns, to better understand and predict the risk of future claims. This information can then be used to develop more accurate pricing models and to determine the most effective ways to manage risk.

From a project risk perspective, the vast wealth of project data in organisations can lead to deep learning approaches. By learning from previous project performance in a wide variety of contexts, teams and organisations can use this information to find likely sources of prolongation

“ By providing forecasts and other insights based on historical information, teams and organisations can make decisions that are freer of bias

and cost uplift and seek to mitigate them earlier than would have been identified using traditional horizon-scanning techniques. These approaches are already being adopted by a number of companies in the built environment, as a supplement or an enhancement of traditional risk identification and quantification approaches.

Quality data

Data is the foundation of deep learning algorithms. Therefore, it is essential to have high-quality data to be able to produce insights that inspire confidence, and, ultimately, value-added decision-making. So that these insights can be effective, deep learning algorithms must be trained on large and varied data sets that accurately represent the environment that they are trying to model, whether that is an organisational or a project context. Consequently, organisations must ensure that the data they use to train these algorithms is accurate, complete and up-to-date, and that it includes a broad and true representation of all relevant

factors and scenarios.

While deep learning has the potential to revolutionise risk management, it is important to recognise that there are also significant challenges to implementing this new approach. The most significant of these challenges is the change of mindset required within the environment in which the technology is being deployed. Where traditional, human-centric approaches to risk management have been applied previously, it can take effort to “let go of the reins” of the risk identification and quantification process, believe the outputs of a deep learning model and focus solely on the outputs provided and the action they foster. Similarly, innovative approaches can be misconstrued as being a panacea to solve all problems. In fact, deep learning approaches work best with structured data sets looking to solve well-defined problems.

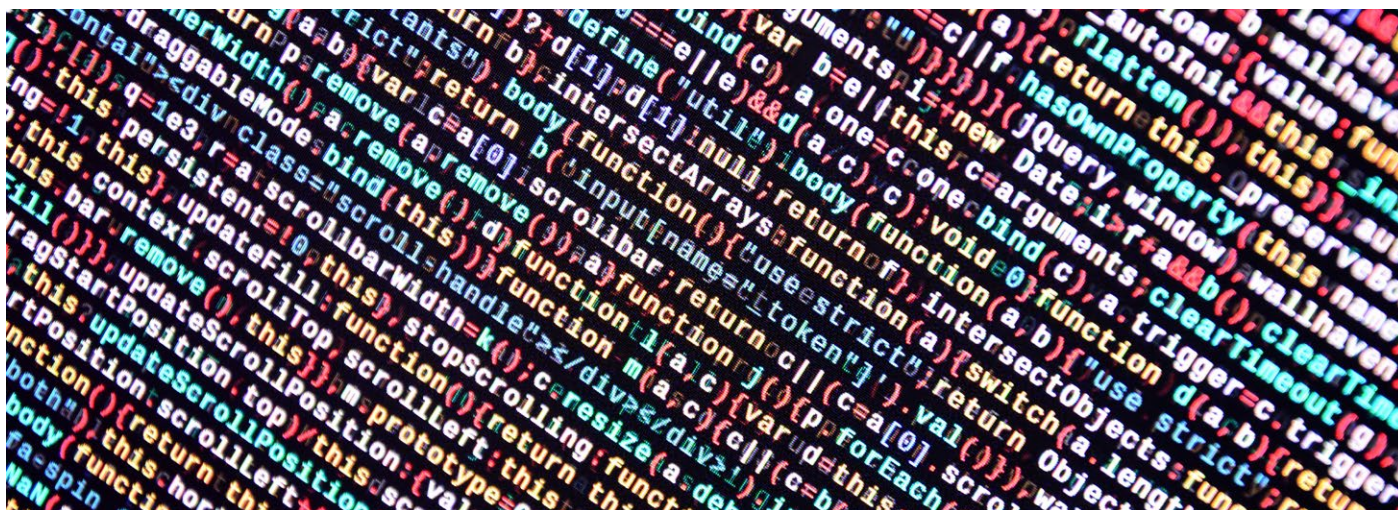
Another challenge for some organisations is the volume of data that deep learning algorithms require to be effective. Organisations must have the infrastructure in place

to store and manage this data safely and legally, and they must also have the resources to process and analyse the data in real time. As a result, approaches to deep learning, or other artificial intelligence-led approaches, will benefit from having a parallel data strategy to ensure that they can get the best out of their investment.

Benefits

Despite the challenges, the benefits of using deep learning in risk management are significant. One of the key benefits is improved accuracy and precision of forecasting, as well as identifying potential sources of risk. The depth and sophistication of deep learning models extends beyond the limits of human cognition, allowing organisations to make more informed decisions based on a broader and deeper understanding of the risks they face. If you hear about AI technologies claiming to be superhuman, this is probably why.

Another benefit of deep learning in risk management is increased efficiency of the risk process. By automating many



STARTING WITH DEEP LEARNING APPROACHES IN YOUR ORGANISATION

- **Understand the problem you need to address:** Deep learning is not a panacea. If there is a question that you think deep learning can solve, seek to address that problem in a well-defined way.
- **Invest in quality data:** The quality of the data used to train deep learning algorithms is critical to their accuracy and effectiveness. Create a data strategy to ensure that your data is accurate, complete and up-to-date.
- **Focus on data privacy and security:** The privacy and security of the data used by deep learning algorithms is paramount – think about it like the safety of your data. When using data-centric approaches, consider the governance that needs to be in place to protect against cyber threats and the unethical (and illegal) use of your data.
- **Build a deep learning culture:** In order to effectively use deep learning approaches, invest in building a data-centric culture that encourages, supports and celebrates the use of data in decision-making.
- **Consider new types of expertise:** Implementing deep learning algorithms requires a high level of technical expertise and specialised knowledge. Be prepared to invest in this expertise, whether by hiring specialists to support you in your aims or by partnering with experts in this burgeoning field.
- **Get ready to scale:** Deep learning algorithms and their application are set to get bigger and more sophisticated; get ready to have the infrastructure in place to manage this data and to process it safely and effectively.

of the more traditional, manual processes involved in risk assessment and mitigation, deep learning algorithms can reduce the time and resources needed to produce risk outputs, enabling organisations to spend this time and effort on actively managing risk and making informed decisions, reducing or terminating the impact of threats in their contexts, while maximising opportunities. Ultimately, the benefit of using deep learning is to focus teams on taking action to achieve the best organisational or project outcomes.

Influencing the future

As deep learning continues to evolve and mature, deep learning

algorithms are likely to become more sophisticated and capable of handling even larger and more complex data sets. This will allow organisations to gain deeper insights into the risks they face and see further into the future, and therefore it will help organisations and teams to make more informed decisions about how to effectively manage those risks. By adding these approaches to existing toolsets, deep learning can offer a valuable data-centric second opinion to challenge stakeholders as to any biases (conscious or unconscious) they may be harbouring.


In addition, as deep learning becomes more widely implemented, it is likely that it

“ **It is essential to have high-quality data to be able to produce insights that inspire confidence**

will become more integrated into the processes and governance of organisations. The technology, in the form of a risk professional, will hopefully become a valued seat at the table – in some instances, it already has.

And what does it mean for risk professionals? We may also start to see the requirement for knowledge of deep learning approaches, and how to integrate them with existing processes (or indeed replace them) in future job roles or specifications. In a not-too-distant future, this may be similar to how the risk profession currently considers risk framework competence, or quantitative risk assessment expertise.

Deep learning is a rapidly growing field with enormous potential to revolutionise the way organisations approach risk management. While it contains a lot of potential, we are starting to see the first practical examples of deep learning approaches helping organisations and their project teams to tackle risk proactively, taking effort out of quantification workshops and into actively mitigating risk. While innovation always comes with some challenges, the benefits are potentially huge. By challenging bias and looking at the risk landscape from an objective perspective, teams can focus on managing the things that really matter more effectively. 🌐

 **Richard Bendall-Jones,**
CFIRM, is principal risk
engineer at nPlan.

Through a glass darkly

BY ELMAR KUTSCH

The very standards and practices used to manage risks could be blinding organisations to their biggest threats

All over the world, companies and governments spend billions of dollars on what is euphemistically called risk management – gathering information about the future state and effect of their environment. Risk management is big business and becoming ever larger despite the worldwide downturn. For example, despite recent cost cutting and staff reductions, banks and broker dealers plan to increase their spending by \$100 billion a year implementing risk governance frameworks by 2025. Risk management has been at the heart of organisations and standards in programmes that are promoted globally to increase the chance of success.

In many industries, such as healthcare, aeronautics, finance or aviation, the practice of risk analysis and management is deemed critical for sound decision-making about the unknown. The prescribed tools and techniques are enshrined in several best practice risk management standards including, to mention just a few, BS 31100:2021 risk management – code of practice and guidance for the implementation (published by the British Standards Institute); PMBOK® Guide (with risk management defined as a core process, published by the Project Management Institute (PMI)); and the APM Body of Knowledge (with risk management defined as a core process, published by the Association for Project Management (APM)).

Four major stages

The principal activity of risk management can be subdivided into four major stages: planning, identification, analysis and response.

First, we can apply risk management planning to define what activities should be taken to approach project and other risks. Second, risk identification allows us to single out risks that may affect the project

materialise and how serious it will be. The resulting risk analysis is often visualised as a risk matrix (see *A typical risk matrix*). This provides a simple analysis that enables managers to focus their responses on those risks with a

“ Best practice risk management standards indirectly claim to be self-evidently effective

objectives, thereby addressing the question of what can go wrong.

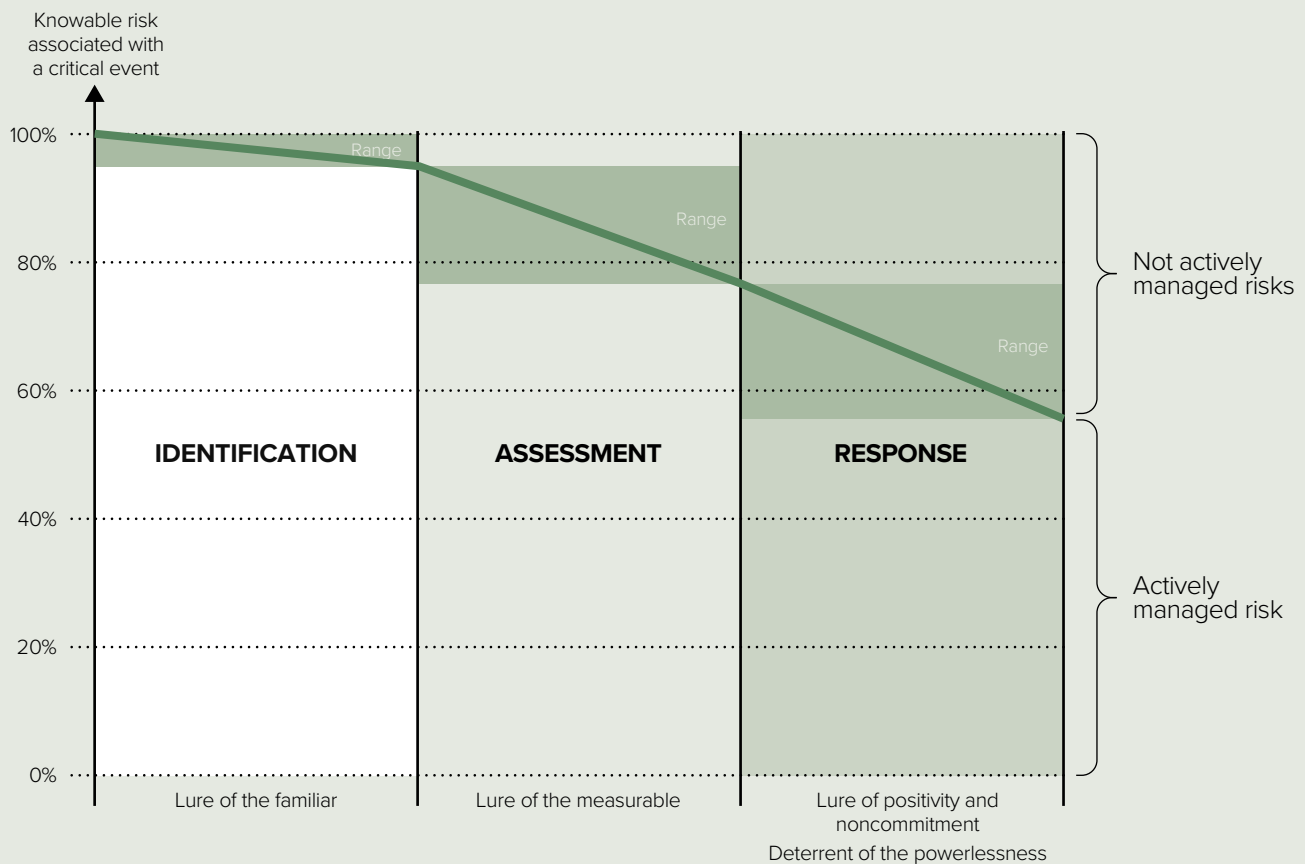
Third, by using risk analysis we evaluate quantitatively or qualitatively the likely impact of risks as well as the likelihood of occurrence – in other words, how likely it is that the threat will

high probability and high impact.

The fourth and final stage is to create a risk response – what will we do about it – that helps us to develop procedures and techniques to mitigate the defined risks. It enables organisations to keep track of these, identify new

A TYPICAL RISK MATRIX						
		IMPACT				
		Negligible	Minor	Moderate	Major	Catastrophic
LIKELIHOOD	Almost certain	Moderate	High	Extreme	Extreme	Extreme
	Likely	Moderate	High	High	Extreme	Extreme
	Possible	Low	Moderate	High	High	Extreme
	Unlikely	Low	Moderate	Moderate	High	High
	Rare	Low	Low	Low	Moderate	Moderate

EXTENT OF DISENGAGEMENT



threats during the project and implement risk response plans.

As introduced and promoted by organisations such as PMI or APM, best practice risk management standards indirectly claim to

effectively managed projects; project failure is indicative of inadequate attention to the project management procedures.”

However, research into the adoption of risk management

unmanaged by project managers in information systems projects – see *Extent of disengagement*.

On average, 44 per cent of all risks that were discovered, understood and ascertained were not actively managed. This degree of disengagement from a purportedly universally applicable process is concerning.

The reasons for disengagement from a process that is being conveyed and promoted as unmistakably right are manifold. They can be summarised as three lures and one deterrent, which are spelt out below.

The lure of the familiar

Taboos reflect a moral or cautionary restriction placed on the action to know what is inappropriate. The risk management process requires risk managers to expose threats in order to analyse and respond

“ On average, 44 per cent of all risks that were discovered, understood and ascertained were not actively managed

be self-evidently effective. In this respect, writers such as Terry Williams have argued that project management includes risk management as a core process. In an article from 2005, he writes it “is presented as a set of procedures that are self-evidently correct: following these procedures will produce

practices indicates that we not only pay inadequate attention to it but also tend to disengage from such a supposedly self-evidently correct process altogether, with some serious consequences. The extent of disengagement from probabilistic risk management shows the extent to which knowable risks were left

“ We tend to ignore difficult-to-measure risks, not because they are not useful or, indeed, have a significant probable impact, but because they are not ‘easy’ to assess

to them. However, the exposure may also create anxiety among stakeholders, and negative thoughts may therefore be suppressed. As a result, we may limit the degree to which we identify new risks to those they are familiar with, confident about and already in control of. At

the same time, we may exclude those risks from our attention that are unrecognisable to us.

The lure of the measurable

Risks are often ignored because they are deemed out of scope. Back in 1989, James Short wrote, “All too often such measures rest

upon what can easily be counted, rather than on what is meaningful to those who are at risk, ...”.

Those risks that attract more attention than others may be unusually visible, sensational and easy to imagine. Risk actors tend to focus on the better-known and readily resolvable risks, obvious

DO YOU ACTIVELY MANAGE RISKS?

How well do the following statements characterise risk management in your project/programme?

For each item, select one box only that best reflects your conclusion:

Lure of the familiar

Our focus includes risks that we have not encountered in the past

The unfamiliar attracts our attention like nothing else

We encourage cross-functional perspectives to identify risks

NOT AT ALL			TO SOME EXTENT		TO A GREAT EXTENT
1		2	3	4	5
1		2	3	4	5
1		2	3	4	5

Lure of the measurable

We question the accuracy of risks

We like to be challenged in our risk estimates

We attend to those risks that are difficult to assess

NOT AT ALL			TO SOME EXTENT		TO A GREAT EXTENT
1		2	3	4	5
1		2	3	4	5
1		2	3	4	5

Lure of optimism

We look to identify as many risks as possible

Acknowledging risks does not question our competence to plan

We are encouraged to embrace risks as an opportunity

NOT AT ALL			TO SOME EXTENT		TO A GREAT EXTENT
1		2	3	4	5
1		2	3	4	5
1		2	3	4	5

Lure of indecisiveness

Ownership of risks does not constrain our freedom to act

Making a decision now is better than doing it later

We only defer decisions to risk if more information is required

NOT AT ALL			TO SOME EXTENT		TO A GREAT EXTENT
1		2	3	4	5
1		2	3	4	5
1		2	3	4	5

Deterrent of powerlessness

We feel empowered to deal with risks

We have access to a variety of responses to manage risks

We are experienced enough to deal with the risk at hand

NOT AT ALL			TO SOME EXTENT		TO A GREAT EXTENT
1		2	3	4	5
1		2	3	4	5
1		2	3	4	5

SCORING: Add the numbers. If you score higher than 55, you are actively seeking to keep the risk gap low. If you score between 54 and 30, the danger of risks not being managed is moderate. Scores lower than 30 suggest the potential for a wider risk gap. Please question your risk management practices.

risks or those being perceived as legitimate. Hence, we tend to ignore difficult-to-measure risks, not because they are not useful or, indeed, have a significant probable impact, but because they are not “easy” to assess.

Lure of positivity and noncommitment

Due to the lack of statistical data for predicting future risks, we need to rely on subjective estimates. However, other stakeholders may not believe in the credibility of these estimates. So, during the risk identification phase, stakeholders might disagree over which risks are considered untrue or fictional. To avoid tensions that result from ambiguity, we may find that we just exclude those risks in contention from further management.

Deterrent of powerlessness

The lure of the familiar, the measurable, and positivity and noncommitment already reduce the chance for a risk to be proactively managed before it materialises. A further potential block is the deterrent of feeling powerless. Having a risk identified, analysed and associated with a response to it does not mean that that response can be enacted.

Despite having more knowledge at our disposal, we increasingly fail to pay attention to risks that ultimately matter. Instead, we tend to selectively concentrate on good-weather risks while ignoring others. This is symptomatic of an apparently universal problem – a risk gap – a gulf between what risks we should, and must, pay attention to and what risks we actually end up managing. Ultimately, we need to ask ourselves whether it is riskier to apply more of a particular process component, or refrain from doing it.

Hyper-rational

Proactive probabilistic risk management, with its assumptions of hyper-rationality, excludes many aspects of managerial

behaviour. On the one hand, some stakeholders’ preference lies in identifying, analysing and responding in advance. Other stakeholders appear to wait until risk resolves itself so to react to materialising risks only. Clive Smallman summarised the apparent emphasis of risk actors on reactive risk management: “It is hardly surprising that reactive risk management is dominant at the present time; it is, apparently, more certain and easier to manage and cost than the holistic approach.”

Does this mean that the

lure of the familiar head-on, we should venture outside our zone of familiarity and make sense of those risks we have not yet experienced. This also helps us to offset the lure of the measurable. The more we think beyond what we are familiar with, the more we appreciate that our risk measurements become increasingly guesswork, and are inexact and inaccurate. Consequently, with increasing ambiguity comes a greater unease to take a risk for granted: we are more likely to challenge the degree of positivity we associate with

“ Proactive probabilistic risk management, with its assumptions of hyper-rationality, excludes many aspects of managerial behaviour

process of probabilistic risk management is doomed, given that it only helps us to manage 56 per cent of all knowable risks actively? These numbers may well indicate that, in many cases, the process of probabilistic risk management ends up a “tick-box exercise”, with limited impact on mitigating risk. As one manager I interviewed told me: “... it becomes an administrative process and as long people feel there is a risk register somewhere and lip services paid to it on a reasonably frequent basis that they are managing risk.”

Sanity check

If you like to do a quick sanity check on your engagement with probabilistic risk management, please complete the questionnaire *Do you actively manage risks?* Suppose you find yourself caught in the act of disengaging from such a process. Could you integrate more of your thinking and doing beyond the realm of probabilistic risk management into a more holistic routine of proactively managing risks?

For example, to address the

them. Ultimately, we look at what truly constitutes a risk – and our erroneous perception of reality that has not yet materialised. The recognition of unfamiliarity, inexactness and inaccuracy, in combination with an appreciation of powerlessness, is an effective stimulant to do something about risk instead of disengaging from it.

Ultimately, it is not a question of whether or not to apply this supposedly straightforward, hyper-rational approach process. Instead, we should complement it with our tacit, at times illogical, counterintuitive but lived way of engaging with risks. ☞

i Elmar Kutsch is associate professor in risk management at the School of Management, Cranfield University. His most recent book is published by Routledge: *Organisational resilience: navigating paradoxical tensions*. IRM members can receive a 20 per cent discount on the print edition using code EFL01 by end of June.

Develop the skills to treat financial services risk

International Certificate in Financial Services Risk Management



Scan me!

Stay on top of international regulatory developments such as Solvency II and Basel III risk requirements. Study with the IRM to ensure you remain compliant and gain an understanding of how risk management impacts strategy and performance.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

The road ahead

IRM risk trends 2023 maps the territory for organisations looking to navigate future uncertainties

Uncertainty and crisis have characterised the past three years. And with no signs of normality returning, organisations need to be faster and better at identifying and mitigating risk. In such an environment, risk professionals are at a premium.

“In what seems like an increasingly fractious and changing world,” Stephen Sidebottom, IRM chair, says, “I envisage the business response to global risks evolving throughout 2023 and beyond through investment in risk management capability, assessing and evolving your risk frameworks, continuously improving data insights and building risk management skills throughout your workforce.”

Risk professionals looking



for insight and inspiration can turn to *IRM risk trends 2023*, drawing on the expertise and experience of its practitioners and experts to help with that task.

Energy and climate

While the war in Ukraine took most governments and

organisations by surprise, problems in the energy sector already existed – and were, to some extent, foreseeable.

“With respect to Europe, what has been notable is the evident lack of foresight and strategic planning when it comes to gas and electricity,” the report says, “and in developing robust and workable solutions based around renewables and alternative energy sources as sustainable means of delivering and maintaining affordable, accessible and reliable energy for industry and households.”

All of these goals are made more difficult with a potential global economic downturn on the horizon, higher interest rates and a burgeoning cost-of-living crisis.

Replacing Russian gas will not be easy. While liquified natural gas (LNG) is seen as an obvious replacement, the reality



“ I envisage the business response to global risks evolving throughout 2023 and beyond through investment in risk management capability

is complex. Countries will have to rapidly invest in new supply-chain infrastructure, which is both expensive and time-consuming. “The rapid construction of the new regasification capacities worldwide will boost the demand growth that may overrun the supply capacities and in turn drive LNG prices up,” the report adds.

The impact of this changing energy landscape is having a knock-on effect on climate change goals. Governments have needed to trade off priorities between ensuring energy supplies are affordable and secure while trying to meet net-zero global emissions targets. For example, the report notes, the scramble for new sources of energy is leading to coal plants being turned on again or expanded, for example in Germany. Governments are also looking at nuclear power initiatives, from building major new reactors to creating smaller, modular

reactors, which have faster build times and lower potential risk.

In addition, extreme weather events are becoming more frequent and severe. “Risk managers and businesses therefore need to continually review options to improve their resilience strategies including pre and post risk management controls,” the report says.

“There is an increasing range of sophisticated strategies that organisations can seek to utilise including use of new technologies such as alert systems to help reduce the impact on assets that are in high flood areas or where suppliers are susceptible to supply chain disruptions.”

But often governments fail to co-ordinate business and disaster continuity programmes. “There is a need for collaboration to develop an initiative-taking disaster risk reduction management plan agreed upon by all stakeholders from all disciplines including:

regulators, health, business, NGOs, community, civil society groups, labour stakeholders, disaster management, and business continuity,” said the report, speaking about South Africa – but expressing sentiments that apply globally.

War and cyber

The Russian invasion of Ukraine put war firmly back on the agenda. But there is also growing tension between the US and China, which adds further layers of complexity to the geopolitical landscape.

“Globally, the Chinese response to various strategic agreements is yet to be fully understood in both the military and economic sense, as well as any response to the global financial downturn,” the report says. “In the longer term, the risks associated with the financial downturn and fuel requirements and the various countries’ responses to them may well change the geopolitical and socioeconomic landscapes.”

Hackers are as active as ever with an increased possibility for additional state-backed cyber-attacks on critical infrastructure. “There is growing concern that cyber-attacks will lead to widespread business blackouts because of power grid disruption,” the report says.

Cybercrime also rose during the pandemic as hackers targeted weaknesses in organisational networks that had to cope with people working from home.

Cost-of-living and society

The cost-of-living crisis is likely to have a large impact in 2023 on business profitability. In the charity sector, for example, it affects beneficiaries, staff and the amount of money people are happy to donate. At the same time charities face an increase in demand for their services they are struggling to attract and retain staff and volunteers and raise finance to pay for their operations.

“The fundraising environment is likely to get more competitive,” the report says. “We see a

“What has been notable is the evident lack of foresight and strategic planning when it comes to gas and electricity



FIVE TOP RISKS FOR BOARDS, RISK COMMITTEES AND CHIEF RISK OFFICERS

- **Economic volatility:** High inflation and low economic growth is now certain for the foreseeable future. The important question is, when will inflation start to retreat and how will it behave in 2023 and beyond? There is also the question for the UK, when will recession hit and how bad might it be? Boards are focusing on rising expenses (increased salary costs to keep up with inflation). On a positive note, such an environment has led to higher yields which should last for a sustained period, delivering higher investment returns.
- **Societal change (people agenda):** Coming out of the pandemic into a highly volatile inflationary period will undoubtedly impact people. Boards and senior management have elevated the people agenda throughout the pandemic putting mental health and wellbeing at the forefront of their agendas. Discussions at risk committees focus on having the appropriate skillset to fulfil current and future organisational needs.
- **Geopolitical volatility:** Entering 2023 continues to see geopolitical risk as the new norm. Countries, businesses and consumers are adjusting to what it means to them locally.
- **Technological disruption:** Cyber-security and disruption to important or critical services and products remains on the agenda.
- **Environmental and Social Governance:** Boards are actively involved in the direction of travel, and the commitments being made regarding their responsibilities around ESG.

Join the Non-Executive Directors and Chief Risk Officers Group [here](#).

“ The risk professional will need to lead the development of conventional risk reporting into more mature processes

crowded market for individual giving, societal shifts in the causes that people and corporate partners want to support and tougher criteria from trusts and funding bodies.”

The cost-of-living crisis could also increase fraud risk both within organisations and from external actors. In developing countries, such as Iraq, for example, governments need to take rapid action. The report says, “The most important reason for the continuation of such activities in Iraq, for example, is the lack

of clear laws that explain these matters and act as a deterrent, as well as the lack of awareness of citizens and some employees in institutions and the lack of electronic detection systems, which has a significant impact on the spread of financial and electronic fraud operations within public and private institutions.”

In some countries, the impact of mass migration remains challenging. “Among the many risks are pressure on social welfare systems, law and order and the potential


for organised crime to expand and grow,” says the report.

Public scrutiny is also on the rise – not just in the charitable sector, but in the social-media fuelled world of public opinion and interest. As Environmental and Social Governance issues continue to create pressure from both governments and the public, organisations need to balance their strategic financial goals with ethical behaviour and transparent reporting.

“As part of meeting a wide range of stakeholder requirements, the greatest risk will be posed to those organisations which fail to demonstrate that they are being governed ethically and sustainably,” the report says. “The risk professional will need to lead the development of conventional risk reporting into more mature processes.”

Inflation is also likely to be a challenge in 2023. Not only does it affect the cost of doing business through increased wages and resources but it also intensifies an already heated war for talent as highly skilled workers can pick and choose their places of work.

In the case of insurers, all aspects of the business model and balance sheet are affected. “This can make pricing the product and estimating reserves extremely challenging, particularly if going through a hard-to-soft market cycle,” the report says. “Investment performance volatility and unrealised losses have been a feature of 2022 and are likely to continue as central banks seek to curb inflationary drivers.”

Risk professionals can play a key part in helping their organisations make timely and meaningful decisions to achieve their strategic goals. Understanding the shifting risk landscape is the first step in that journey. 

 **IRM risk trends 2023**, led by
IRM's global network of risk
practitioners and professionals

TAKING CONTROL OF operational risk

BY MICHAEL GRIMWADE

The nature of operational risk is poorly understood, and the tools can sometimes fail to add value. But a penetrating study of the financial sector's biggest catastrophes provides some much-needed insight

I first worked on operational risk management 28 years ago, more than a decade before Basel II was implemented. As operational risk management entered its fourth decade, I was struck by the extent to which the profession continued to struggle with questions over the effectiveness and efficiency of many of its core tools, which were first developed back in the 1990s. These unresolved issues included concerns over the predictive powers of key risk indicators (KRIs), the value of risk and control self-assessments (RCSAs), the subjectivity of scenario analysis and capital modelling, and the effectiveness of stress testing of operational risk for economic shocks.

Reviewing the profession's literature, conferences and training reveals that while much has been said on the subject of integrated operational risk management frameworks, these are rarely, if ever, linked to an explanation as to how the risk, which they are intended

to help manage, actually behaves. This reflects Dr Patrick McConnell's observation in 2017 that "unlike credit and market risk, operational risk is lacking in basic theory as to why, where and when operational risk losses occur". This is important as understanding how operational

data that has been systematically collected over the last two decades by either the Basel Committee ($\geq \text{€}10,000$) or the ORX loss data sharing consortium (a risk management association in the financial sector) ($\geq \text{€}20,000$) reveals that a small number of losses $\geq \text{€}10$

“ Unlike credit and market risk, operational risk is lacking in basic theory as to why, where and when operational risk losses occur

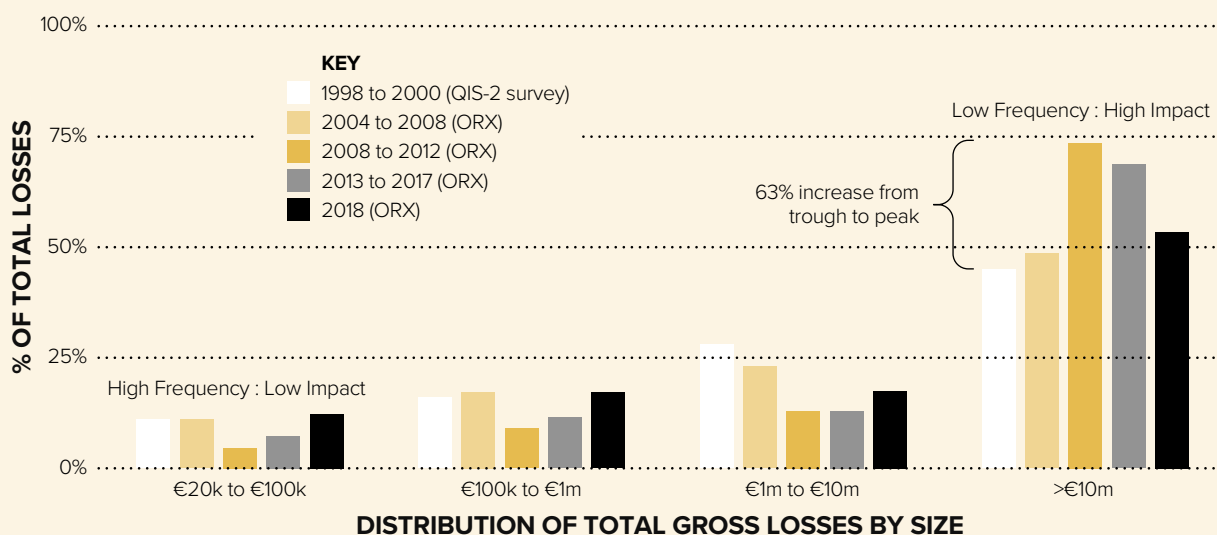
risk behaves and why has to be foundational for the development of effective risk management tools.

Operational risk losses are far from random with the Prudential Regulation Authority (PRA) describing operational risk's loss distribution as being "... unusually fat-tailed, with infrequent but very large losses ...". Reviewing loss

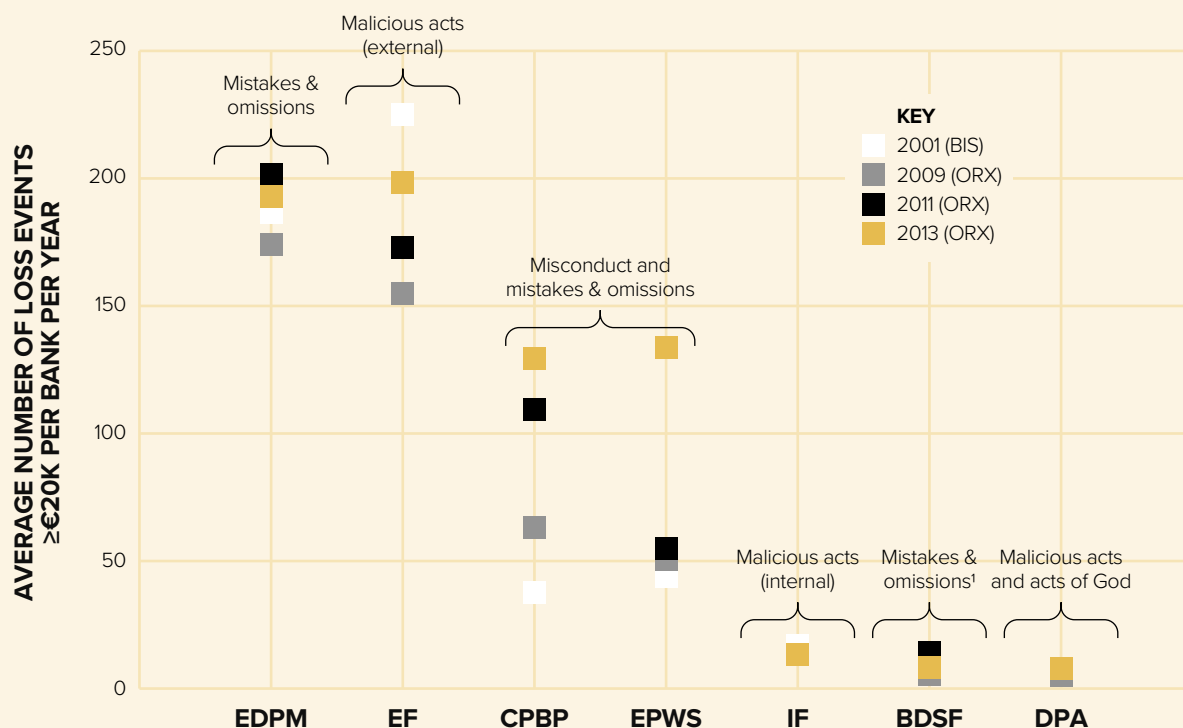
million contributed the majority of the total value of operational risk losses (see *Distribution of the value of losses by the value of individual loss events (1998 to 2018)*). The peak in the contribution of these losses $\geq \text{€}10$ million coincides with the aftermath of the global financial crisis.

In line with the PRA's observation, for the period 2010 to

DISTRIBUTION OF THE VALUE OF LOSSES BY THE VALUE OF INDIVIDUAL LOSS EVENTS (1998 TO 2018)



AVERAGE NUMBER OF LOSS EVENTS PER BANK PER YEAR FOR THE SEVEN BASEL EVENT CATEGORIES



2018, 38 extremely large losses ($\geq \$1$ billion) suffered by nine individual ORX members represented alone just over 50 per cent of the total losses suffered by ORX's members during this period, despite comprising just 0.01 per cent of the total number of loss events. These extremely large losses include mortgage-backed securities litigation, the mis-sale of payment protection insurance, inappropriate foreclosure, benchmark manipulation and anti-money laundering or sanction breaches.

Understanding the drivers behind these loss trends should help risk managers obtain more value from RCSAs.

Events and controls

While Basel II defined operational risk losses in terms of inadequacies or failures, it did not articulate their nature. The vast majority of operational risk events arise from human failings, hence a taxonomy of inadequacies or failures is dominated

by categories, such as mistakes and omissions – for example, transpositions, duplications, replication of other errors and so on; individual or systemic misconduct; and malicious acts.

Average number of loss events per bank per year for the seven Basel event categories highlights that the frequencies of five of the seven Basel event categories are really quite stable. But external fraud (EF) and clients, products and business practices (CPBP) show distinct trends. Both observations are interesting and, considering the nature of the key inadequacies or failures, help to explain these differing frequencies – such as staff members are generally honest, but they do make mistakes and omit actions at a fairly consistent rate. Hence, the most common loss events are generally execution, delivery and process management (EDPM) reflecting the combination of these human frailties and the volume of manual processing

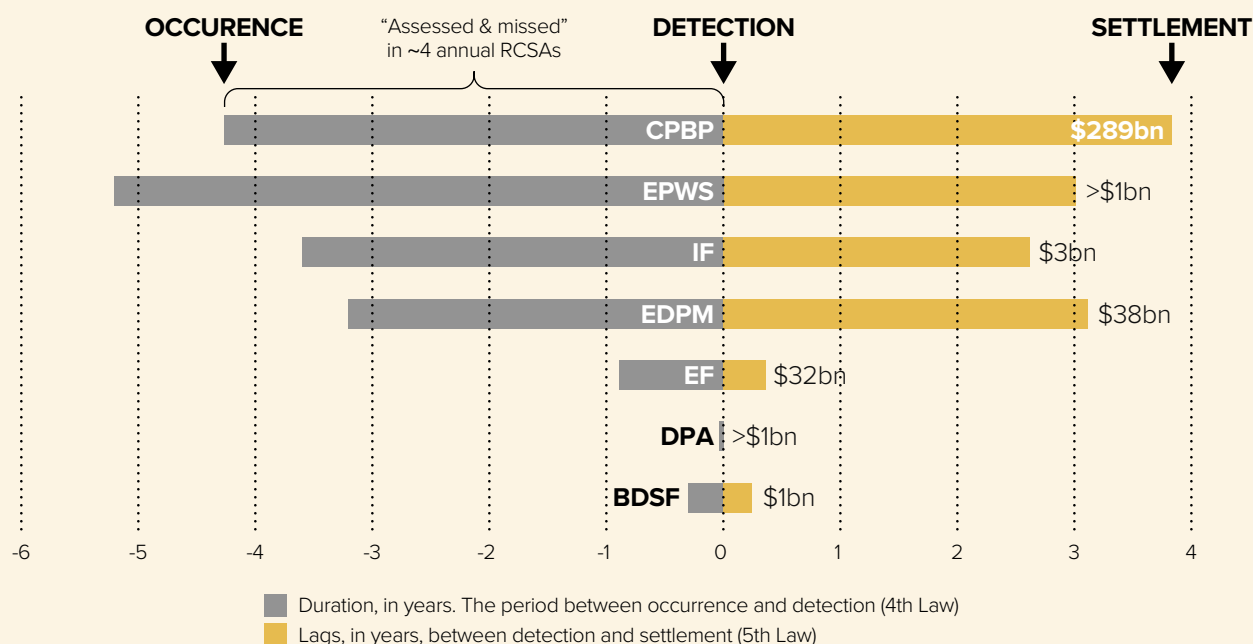
and interventions. Professional criminals are the obvious exception to the observation that humans are generally honest, as their job is to act maliciously. Consequently, external fraud vies with EDPM as the most common loss category.

Finally, a taxonomy of inadequacies or failures not only describes the nature of operational risk events but also explains why controls fail, which is a much-neglected topic. Just as most operational risk events arise from human failings, the same is true for controls failures. This observation is important when attempting to identify predictive KRIs because metrics relating to “stretch” may foretell both increases in the occurrence of events and also reductions in the effectiveness of controls.

The importance of time

An analysis of losses $\geq \text{€}20\text{k}$ suffered by ORX members reveals that on average the durations and

AVERAGE DURATIONS AND LAGS FOR 390 LOSSES $\geq \$0.1\text{bn}$ SUFFERED BY THE G-SIBS



“ This sensitivity of operational risk to economic shocks is arguably its most important characteristic

lags for most of the Basel event categories are relatively short, primarily with the exception of CPBP, which displays average durations and lags of 1.6 years and 0.7 years respectively. A similar analysis for large losses $\geq \$0.1\text{bn}$ in the public domain for 31 current and former global systematically important banks (G-SIBs) (see Average durations and lags for 390 losses $\geq \$0.1\text{bn}$ suffered by G-SIBs), however, reveals much longer durations and lags. For example, for CPBP, which is the largest loss category by value in this sample, both the duration and the lags in settlement are each around four years.

The chart shows that these very large operational risk losses were on average subject to four annual RCSA cycles without being detected, detracting from the reputation of this tool.

Sensitivity to economic cycles

Similarly, an analysis of the losses $\geq \$0.1\text{bn}$ suffered by the same G-SIBs over the last three decades displays three spikes of increasing size, associated with different economic shocks: the hike in US dollar interest rates in 1994, the bursting of the dot.com bubble in 2001/02, and the global financial and euro crises (see Analysis of 442 large losses $\geq \$0.1\text{bn}$ for 31 current and former G-SIBs by end date).

This sensitivity of operational risk to economic shocks is arguably its most important characteristic. The losses in the chart have been analysed to reflect the nature of the underlying impacts. Over 60 per cent of these operational risks, by value, are underpinned primarily by either credit risk or, to a lesser extent, by market risk – providing some indication of the

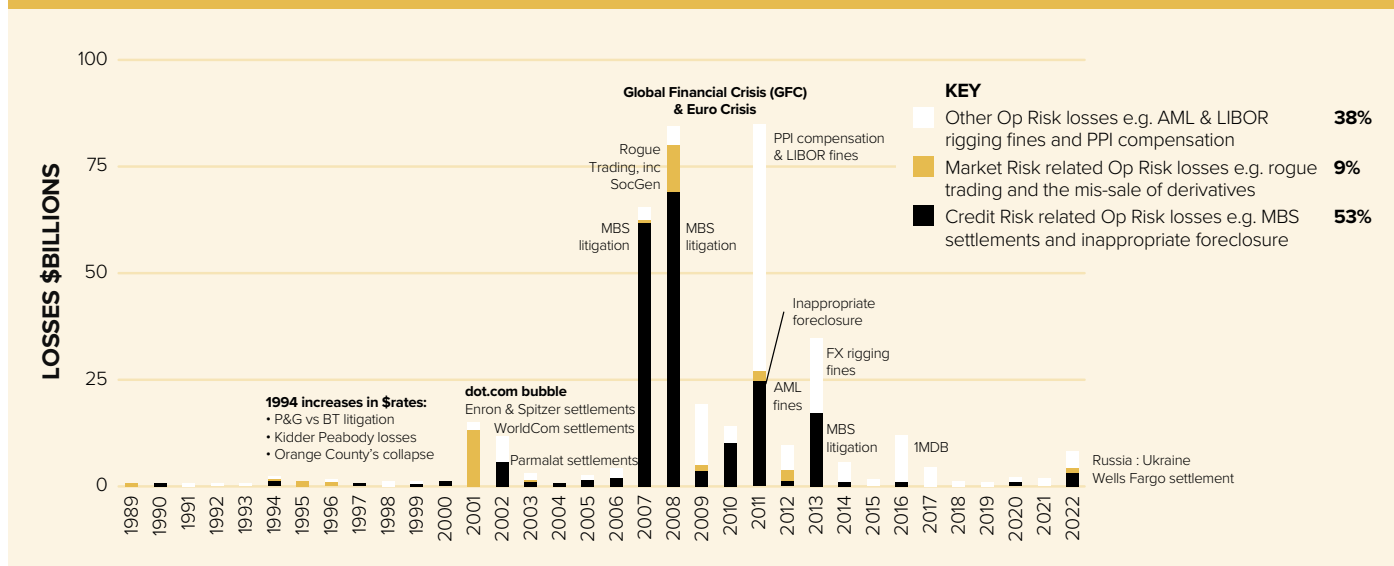
mechanism of this sensitivity. Comparison of large losses ($\geq \$0.1\text{bn}$) suffered by 31 current and former G-SIBs pre- and post-global financial crisis reveals that both the frequency and severity each increased by about three times.

Let's now consider the mechanisms for each of these sensitivities in turn.

First, frequency is due to a combination of changes in stakeholder behaviours, for example previously law-abiding customers being driven to commit fraud due to financial pressures; inappropriate responses of firms and staff members, for example the inappropriate mortgage foreclosure scandal in the US in 2008; and direct economic impacts, such as supplier defaults.

In addition, an economic shock may trigger the uncovering of historical failures arising from

ANALYSIS OF 442 LARGE LOSSES ≥\$0.1BN FOR 31 CURRENT AND FORMER G-SIBS BY END DATE



“ Actively taking operational risk to generate fee and commission income is disproportionately risky

changing stakeholder behaviours, or market moves and defaults. For example, market falls led to client redemptions and the uncovering of Bernie Madoff's \$64 billion Ponzi scheme in 2008. Similarly, the introduction of negative interest rates revealed design deficiencies in some structured products – the absence of stable foundations.

Second, economic shock can influence the severity of losses. Changes in asset values and markets may underpin the scale of compensation that needs to be paid to customers as a consequence of any historical or current misconduct. For example, the compensation paid by UK banks to small and medium-sized enterprises for the mis-sale of interest rate derivatives in the run-up to the global financial crisis was linked to the scale of the fall in rates – from 5.5 per cent to 0.5 per cent in the space of a few months. If UK interest rates had only fallen to 3 per cent, then the scale of compensation would have been roughly halved.

Disproportionate risk

Banks expose themselves to differing risks in order to generate three types of income – trading, interest, and fees and commission income.

To dig a bit deeper, trading income primarily involves the active taking of market risk, while also generating credit, liquidity and operational risks as by-products. Creating interest income primarily entails actively taking credit risk (for example, from advancing loans to customers) while also generating market, liquidity and operational risks as by-products. Finally, fee and commission income is obtained by charging customers for services, such as soft underwriting, structuring securities and fund management to name a few. Providing these services typically involves taking operational risk only. Examples of losses resulting from such activities include investor litigation (remember WorldCom and the fallout from mortgage-backed securities), compensation paid by funds that invested in Madoff's Ponzi scheme, breaching of US

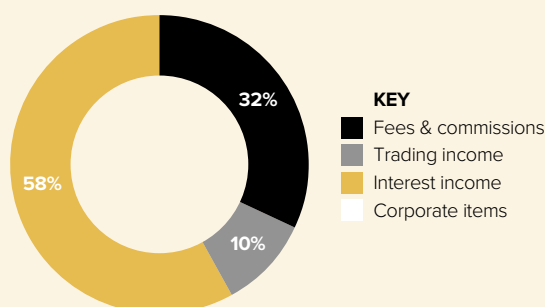
sanctions and the mis-sale of PPI.

A comparison of these sources of income mapped to associated losses reveals that actively taking operational risk to generate fee and commission income is disproportionately risky (see *The relationship between large losses and income streams for 31 current and former G-SIBs*).

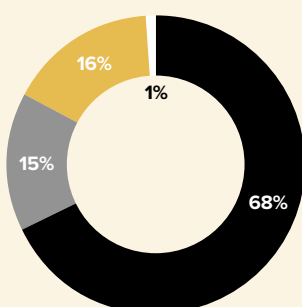
Armed with this knowledge, we can now understand what our first diagram means in terms of operational risk (*Distribution of the value of losses by the value of individual loss events (1998 to 2018)*). The left-hand-side of the chart is driven by high-frequency, low-impact operational risk losses that primarily arise from human errors and external malicious acts, with typically short durations, mainly relating to retail banking. In contrast, the right-hand-side is driven by low-frequency, high-impact losses that primarily arise from systemic misconduct over extended periods of time relating to retail, commercial and investment banking. A significant proportion of these losses

THE RELATIONSHIP BETWEEN LARGE LOSSES AND INCOME STREAMS FOR 31 CURRENT AND FORMER G-SIBS

**SPLIT OF
INCOME TYPE
FOR 2017**




**LARGE LOSSES FROM
2007 TO 2017 ANALYSED
BY INCOME TYPE**



medium-frequency risk / medium and high-impact operational risks. As we have seen, these risks are often driven by systemic misconduct over extended time periods, often associated with the generation of fee and commission income, which are also likely to be sensitive to economic shocks.

In contrast, firms should de-scope risks leading to high-frequency and low-impact operational risk losses, as these can be better managed through much more real-time monitoring of KRIs, incident management and root-cause analysis. It is these processes and not RCSAs that are currently keeping EDPM losses relatively stable over time and external fraud losses in check. Unfortunately, when I ran a poll on LinkedIn in February 2022, only 2 per cent of the 60 respondents believed that RCSAs should just focus on these medium and low-frequency, and medium and high-impact risks. The other 98 per cent all wanted RCSAs to include high-frequency, low-impact operational risks.

Apocryphally, Einstein said that the definition of insanity was “doing the same thing over and over again and expecting a different outcome”. When the profession first developed its toolset in the 1990s, it clearly had far fewer years of experience of operational risk than it does now. The growing body of evidence that operational risk shows distinct patterns and trends in its behaviours should drive the tailoring of all of the profession's tools, including RCSAs, in order to deliver more commercial value for firms. 

are associated with the generation of fee and commission income. The losses shown in the right-hand-side of the chart are also clearly sensitive to economic cycles, with examples including mortgaged-backed securities (MBS) litigation, the mis-sale of interest rate derivatives, inappropriate foreclosure, etc.

Obtaining more value from RCSAs

According to the Basel Committee, “banks should identify and assess the operational risk inherent in all material products, activities, processes and systems”. For banks, a key tool for meeting this principle are their RCSAs. But a survey of RCSA practices conducted by ORX in 2019 identified a number of continuing challenges, such as RCSAs often being out of date and not informative enough, and inefficiencies in the RCSA process. These challenges reflect that the RCSAs are often a periodic activity, typically annual, and that much time and resources are invested in running these processes, which can be perceived as being just tick-box exercises. In other words, too much effort is being expended to obtain too little value. It is quite striking that after almost 30 years of conducting RCSAs, the

operational risk profession is still struggling to obtain commercial value from this activity. In other words, too much effort is being expended to obtain too little value.

This is unfortunate as RCSAs should provide tangible commercial value to firms by identifying high inherent risks, which can be used to select scenarios, tailor insurance policies and support the internal capital adequacy assessment process (ICAAP). They can also be used to identify key controls, which mitigate these high inherent risks, and which consequently can then be subject to attestations and second or third lines assurance. Finally, RCSAs can identify weaknesses in the design of controls and collate residual risks that are outside of appetite, but which have not previously been formally escalated, as they may be perceived to be known issues, although they may in practice be completely unknown to senior management.

An understanding of the nature of operational risk, based on our discussion here, should help firms to obtain more value from their RCSAs. In addition, it should also help them to expend less effort. In particular, firms should focus their RCSAs on the effectiveness of controls in mitigating low and








Michael Grimwade is head of operational risk for ICBC Standard Bank. He is a former director of the Institute of Operational Risk. His most recent book is *Ten laws of operational risk*. IRM members receive a 30 per cent discount on the print version using the discount code TLPR3 from Wiley.com.

The contents of this paper are the author's own views rather than those of ICBC Standard Bank.

Change tomorrow with industry leading GRC software

Camms.






With powerful, agile and integrated solutions in governance, risk, compliance and strategy, Camms' business software will help you make the right decisions, manage risks and focus on what matters. Working with tens of thousands of users at organisations across five continents, and with over 25 years of experience, Camms thrive on watching their clients achieve results and stay a step ahead. Helping firms meet goals, influences business decisions and board strategy is in Camms' DNA. To learn more, visit www.cammsgroup.com.

 Daniel Kandola
 +44 (0) 161 711 0564
 sales@cammsgroup.com
 www.cammsgroup.com
 Suite 4.3, Parsonage Chambers
3 The Parsonage
Manchester, M3 2HW
United Kingdom

Cost-effective technology for risk & compliance professionals



1RS provide cutting edge 1RS ERIC (Risk & Compliance), 1RS CASS and 1RS SMCR solutions, which have been designed and built by Risk and Compliance professionals with over 25 years of experience. Our solutions are supported by experts, and we continually update the products to reflect best practice and changes in regulatory expectations. We are trusted by banks, vehicle finance, wealth management, investment banking and management, brokers, and more throughout the United Kingdom and Europe. For more information, visit <https://1rs.io>

 Andrew Firth
 +44 (0) 20 7175 6177
 hello@1rs.io
 1rs.io
 38 Borough High Street
London
SE1 2AL

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, audit & compliance software

Symbiant®

Symbiant is a market leading provider of Risk, Audit & Compliance software. They have a full range of modules that can be connected for a wholistic view. Customise your own layouts and reports or use the ready-made options. All modules are a fixed £100 per month. Contracts are only 30 day. Visit the website to watch the quick overview videos or to arrange a no obligation web demonstration.

 Mark Long
 +44 (0) 20 8895 6410
 irm@symbiant.co.uk
 www.symbiant.co.uk
 20-22 Wenlock Road
London
N1 7GU

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.

 N/A
 +44 (0) 20 3978 1360
 info@protechtgroup.com
 www.protechtgroup.com
 77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

The productivity paradox

Time management and productivity have become buzzwords of the global self-help industry – but do their methods make matters worse?

Toffler is a fan of self-help books. Over the years, classics such as Stephen Covey's *The seven habits of highly effective people* and David Allen's *Getting things done* have helped us to become highly effective and, well, to get things done.

Covey, for example, encourages readers to be a fly on the wall at their own funerals. What would you want people to say about you? he asks. Having found the answers to such existential conundrums, his book helps readers to build a personal productivity system around their newly discovered values.

Clearing ground

Allen, on the other hand, starts from the bottom up. Readers list all of their real and fantasy tasks (the latter, for example, include such velleities as clearing out the loft) and work in incisive ways to tick off those tasks.

Both books are excellent at achieving two things: getting through to-do lists and creating more things to do to add to those lists. That is the productivity paradox. The more you do, the more there is to do.

Ex-Guardian columnist and author Oliver Burkeman has pitched in to this field with his own book *Four thousand weeks: time management for mortals*. Admitting

to having been a productivity geek for much of his working life, he came across the idea that people live for an average of 4,000 weeks. Faced with such an existential timeline to get *everything* done, he began to wonder whether an endless to-do list generated

less pressure you'll feel to ask whether any given activity is the best use for a portion of your time."

Realising that not everyone can become an anti-productivity guru, Burkeman throws readers a few crumbs of comfort. Try "strategic underachievement"


“Productivity, in fact, dulls the senses to reality and makes people more machine-like – the more they automate their processes, the more automated they become

a feeling of limitlessness, unconstrained by the amount of time people actually have to live. It has become normal, he says, for people to feel as though they *must* do more than they *can* do.

Automata

Productivity, in fact, dulls the senses to reality and makes people more machine-like – the more they automate their processes, the more automated they become. The result diminishes the quality of everyday experience and our ability to choose tasks wisely: as Burkeman says, "the more firmly you believe it ought to be possible to find time for everything, the

and "failing on a cyclical basis". Those involve ignoring things on the to-do list intentionally (forever) or ignoring them for a shorter period before giving them the attention they deserve.

Toffler's favourite, though, is to practise doing nothing: "When it comes to the challenge of using your four thousand weeks well, the capacity to do nothing is indispensable," he says, "because if you can't bear the discomfort of not acting, you're far more likely to make poor choices with your time, simply to feel as if you're acting." All you need to do for preparation is to remember to put "do nothing" on your to-do list. 

Improve your
chances of
assessment
success



Scan me!

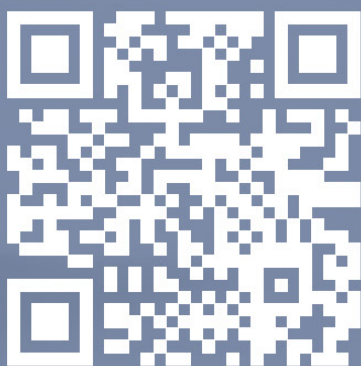
Blended Learning

Sign up and join our online interactive workshops to fully get to grips with the study materials and develop an effective study plan.

www.theirm.org | Tel: +44 (0)7469 353441 | Email: joanna.kraska@theirm.org

irm

Build your career as a risk professional



Scan me!

Training with the IRM

With training courses covering a wide range of enterprise risk management topics, our courses are delivered by industry experts so you can immediately apply the latest in best practice techniques. As well as being practical and interactive, the courses allow you to log CPD hours and some offer accreditation.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm