

# Enterprise Risk

Summer 2023 / [www.enterpriseriskmag.com](http://www.enterpriseriskmag.com)

The official magazine of the Institute of Risk Management

**A helping hand:** Beate Degen, chair of the recently launched IRM Advisory, aims to help risk managers and boards strengthen risk discussion culture



**Why the banking crisis is back:** North American failures put the sector under pressure / **The reach of regulation:** UK banking rules overhauled / **The rise of the risk bots:** ChatGPT raises the heat / **Risky behaviours:** IOR issues guidance on the tricky topic of people risk / **Waking the sleeper risks:** new methods can bring hidden threats to light

# Do you manage risk in your organisation?



Scan me!

## Get risk ready with the IRM

There has never been a better time to increase your earning potential and career prospects by gaining an internationally recognised risk management qualification.

**a.r.u.** | Anglia Ruskin University

**EDINBURGH**  
THE CITY OF EDINBURGH COUNCIL

**Gateshead**  
Council

**NHS**

**Norfolk**  
County Council

**The Open University**

[www.theirm.org](http://www.theirm.org) | Tel: +44 (0)20 7709 9808 | Email: [enquiries@theirm.org](mailto:enquiries@theirm.org)

**irm**

**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 © 2023 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.



## Good to talk

**H**aving meaningful risk conversations is a key challenge for businesses and their risk professionals. In theory, it should be easy. Risk managers are armed to the teeth with analytical tools and methods to help identify and quantify risks. In many cases, those tools are tried, tested and reliable.

But they do not always work. One of the least welcome strands of news earlier this year was growing instability – followed by actual large-scale failures – in the global banking system. Silicon Valley Bank (SVB) not only showed that inadequate risk management at the top of an organisation can have disastrous results, but it also underlined regulatory failings that most people had thought had been dealt with after the financial crisis of 2007-2008.

## Eyes shut

The Board of Governors of the Federal Reserve System admitted in their analysis of the collapse that regulators had taken their eye off the ball. Not only did they not appreciate vulnerabilities at SVB, but they were also slow to act (see *Why the banking crisis is back* by Michael Rasmussen and William Gonyer in this issue, pages 16-19).

More worrying, however, is that board members of SVB were in the dark about the risks they faced. The bank failed its own liquidity stress tests and only managed interest rate risk for the short term. When risk management procedures turned up the wrong answers, they altered the questions: “the bank changed its own risk-management assumptions to reduce how these risks were measured rather than fully addressing the underlying risks,” the Federal Reserve said.

This seems absurd from the outside, but I wonder how it felt to be working within the kind of corporate culture that prevailed at SVB. During my research for the cover story for this issue, I spoke to Beate Degen, chair of IRM Advisory, which launched recently. The service aims to help organisations improve the quality of board discussions and strategic and tactical decision-making processes and offer other forms of boardroom guidance.

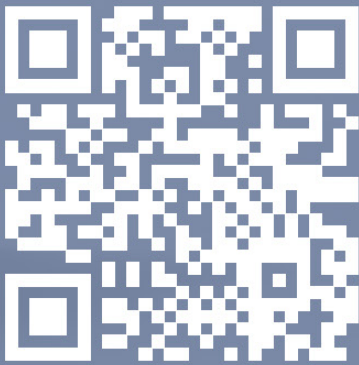
## Understanding

She made a distinction that could help risk managers constructively think through the differences of their own understanding and approach to risk to that of board members and directors.

While it is crucial to understand how a CEO sees, say, a long-term investment in expensive safety equipment as a cost when the company is under intense financial pressure, understanding why that is the case is not the same as agreeing with that view. The risk manager’s role is partly to open up a space of both mutual understanding and critical dialogue. At times, those discussions will be difficult. But they are also crucial to prevent organisations playing fast and loose with assumptions about risks that have serious, real-life consequences.

**Arthur Piper**  
Editor

# 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](http://www.theirm.org) | Tel: +44 (0)20 7709 9808 | Email: [enquiries@theirm.org](mailto:enquiries@theirm.org)

irm



## Features

**10 A helping hand**  
Building a strong risk discussion culture across organisations is key in today's unpredictable world, as Dr Beate Degen, chair of the recently launched IRM Advisory explains

**16 Why the banking crisis is back**  
The latest banking crisis in North America has put potential failures regulation, governance and risk management back in the spotlight

**20 The reach of regulation**  
The UK's review of banking rules is a welcome opportunity to reform what does not work – yet the outcome could also shift the country's financial system into unknown territory

**22 The rise of risk bots**  
ChatGPT has raised the profile of artificial intelligence programs, proving they can do tasks previously thought to be the unique preserve of humans. The implications of society and risk management could be profound

**26 Risky behaviours**  
People risk is often difficult to identify and harder to control. The latest in the series of IOR operational risk sound practice guides lays the groundwork for an effective approach

**30 Waking the sleeper risks**  
Traditional risk management calculations can hide important risks from view. Bringing them to light is imperative if organisations are to improve their resilience

## REGULARS

**7 IRM Viewpoint**  
IRM's new Australia Regional Group aims to help professionals boost the risk maturity levels in their organisations in an unprecedentedly busy time

**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**  
Keeping the internet on in Egypt



IRM Advisory Services Ltd

# IRM Advisory

## Advice, Guidance and Mentoring

---

### Level up your risk performance

IRM Advisory will advise, guide and mentor you in levelling up your risk performance by helping you get the most out of your risk frameworks and programs.

From understanding your risk appetite to setting the proper risk levels and developing an enterprise-wide risk culture.



Scan me!

[hub.theirm.org/advisory](https://hub.theirm.org/advisory)  
[advisory@theirm.org](mailto:advisory@theirm.org)



## Raising the game

---

IRM's new Australia Regional Group aims to help professionals boost the risk maturity levels in their organisations in an unprecedentedly busy time

**W**hether you are working on the mega

metro projects in the east of the country, involved in the Trilateral Australia-UK-US Partnership

in the south or supporting the country's resource giants in the west, one thing is certain – there is plenty going on in Australia. In fact, we will soon be gearing up to host Brisbane Olympics.

With all this going on, there is plenty to keep Australia's risk professionals busy. Luckily, one thing Australia does have is a wealth of experience and expertise in the management of risk; after all, they led the way with the AS/NZS 4360 published in 1995 many years before the ISO 31000 appeared. So this gives us a good idea about the nation's mindset for managing their uncertainties.

### New levels

When we are talking about these once-in-a-lifetime projects, then were talking about a whole new ball game in Australia in terms of size and nature. So there really is no choice but for organisations to lift their management of risk to new levels to ensure success in achieving these countrywide goals and objectives.



Those lucky people working in the world of risk will undoubtedly have challenges to face. The first of those is the number of risk professionals available to support the delivery of these all-important

works. The lack of resources is a key risk to many organisations in Australia. Not having the quantity of risk professionals and managers (or the required competencies) is a major contributor to that key resource risk.

Another challenge risk professionals face is the current level of risk maturity that exists across many of the organisations and sectors. While good processes, systems and people are in place in most, many are still behind the curve. Organisations need support, training and development, tools and techniques to uplift their risk maturity levels to meet demands. That chimes with my own experience of living in numerous states and territories across the nation, and from delivering the Fundamentals of Risk Management (FoRM) training for IRM in Australia – as well as from independent reviews that show major project cost blow-outs where poor risk management systems and practices have been specifically highlighted.

### Head-on

While this may be daunting for Australia's risk professionals, facing these challenges head-on will undoubtedly support their risk learning and ongoing development. Being a part of projects and organisations will also help.

It is always good to have a network of risk professionals who are on hand to discuss and share risk experiences and to provide support and guidance too. That is one reason we have set up IRM Australia Regional Group. It provides current IRM members throughout the region with an opportunity to network with one another and to help develop an IRM risk community across the nation. It is a chance to welcome new members to IRM too.

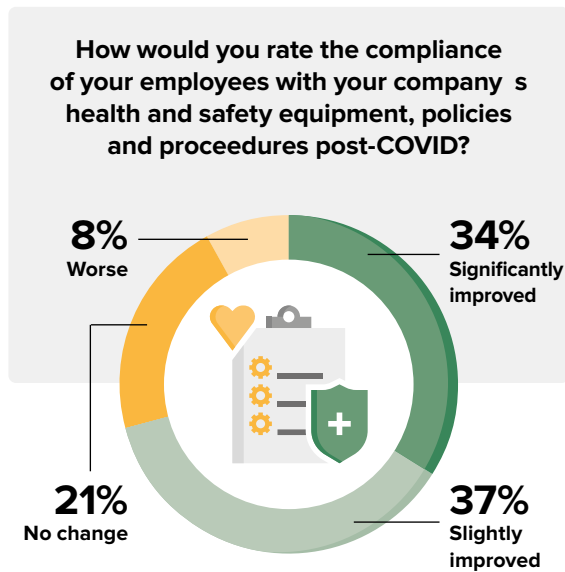
By bringing together some of the best risk minds and experience across Australia via the group, we hope to support Australia to increase overall risk maturity levels and provide mentoring opportunities to junior risk professionals. The group members currently meet monthly and aim to host three networking events each year and release a thought leadership paper annually. [Please get in touch.](#) 

 **Colin McCrorey, IRMCert,**  
is chair of IRM Australia  
Regional Group.

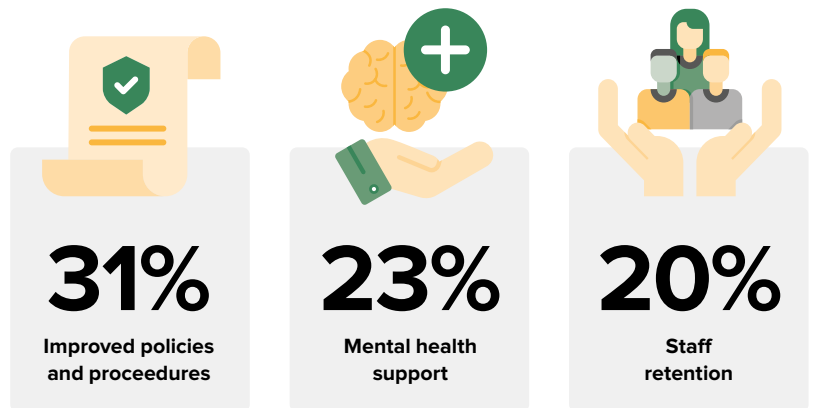
The latest stories and news affecting the wider business environment as interpreted by our infographics team



## Post-Covid world boost to health and safety compliance



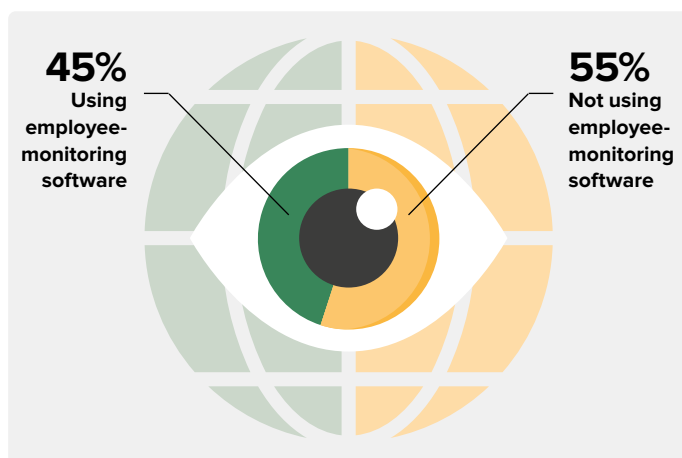
Thinking about the next five years, which of the following do you think would help to improve your company's health and safety compliance? (Rank one choice)



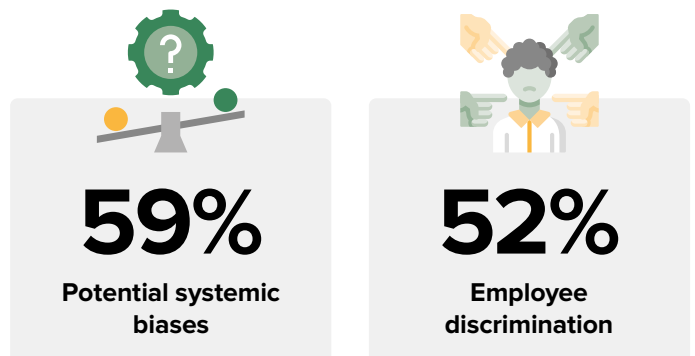
Source: RS Safety Solutions, Under the surface of health and safety

## Big brother is watching

Businesses are split over the use of employee-monitoring software



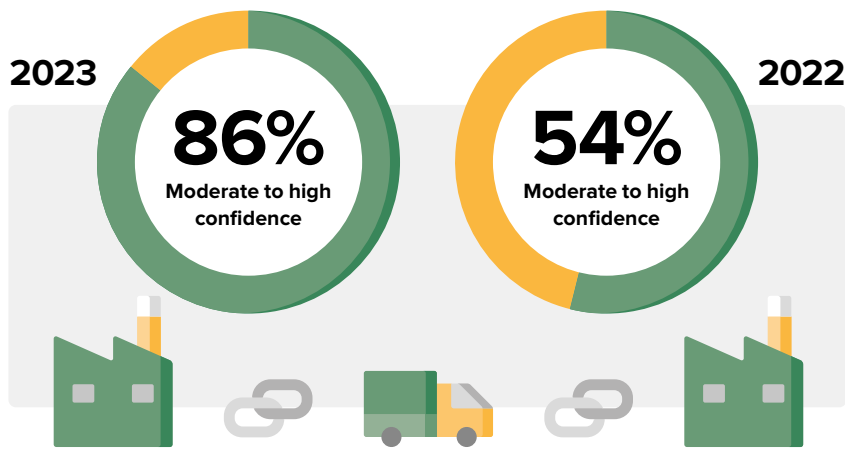
Yet concerns over AI solutions remain high because of risk of:



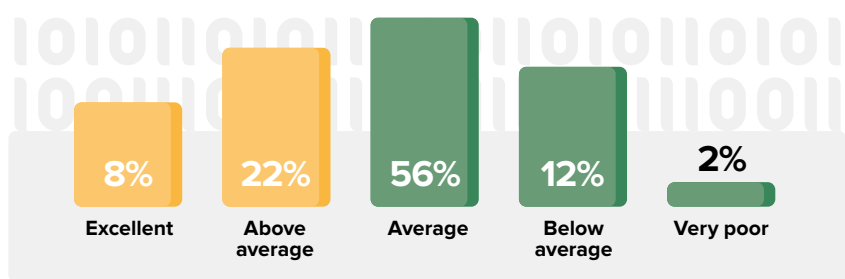
Source: Littler annual employer survey report, May 2023

# Supply chain confidence grows

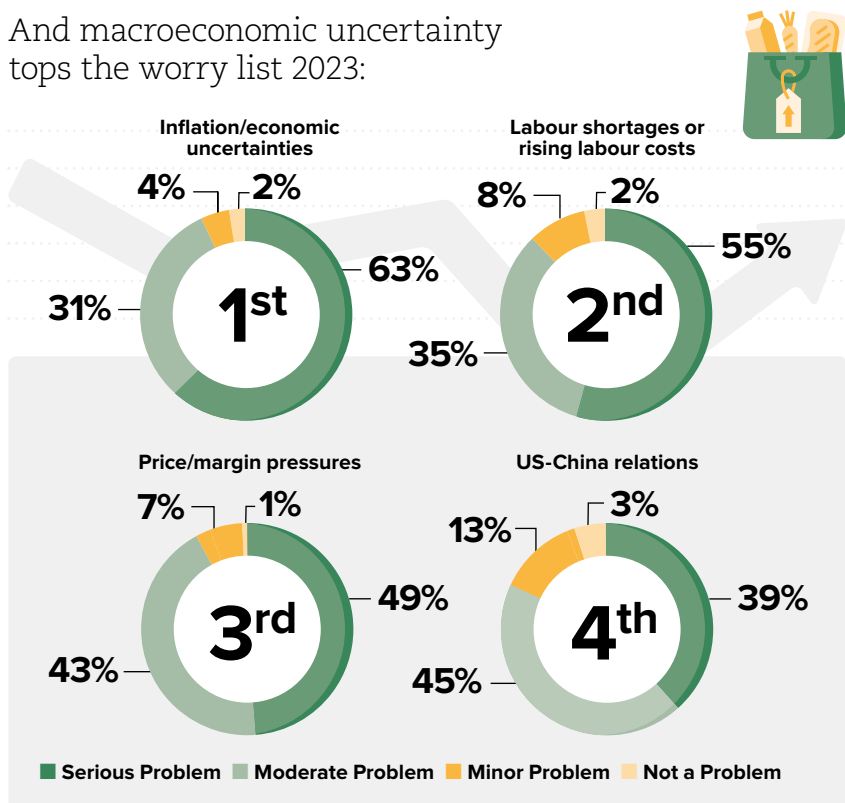
Rate the level of confidence in your end-to-end supply chain to support your 2023 business growth initiatives



While digitalisation efforts lag:



And macroeconomic uncertainty tops the worry list 2023:

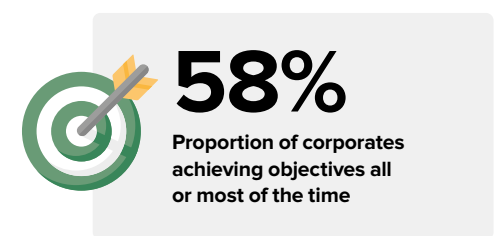
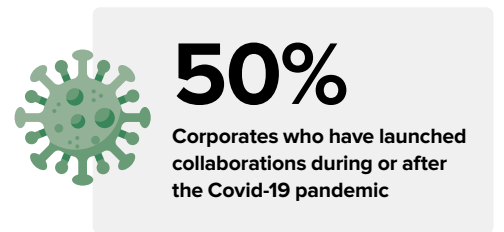


Source: CGS Annual Report: Supply chain trends and technology 2023

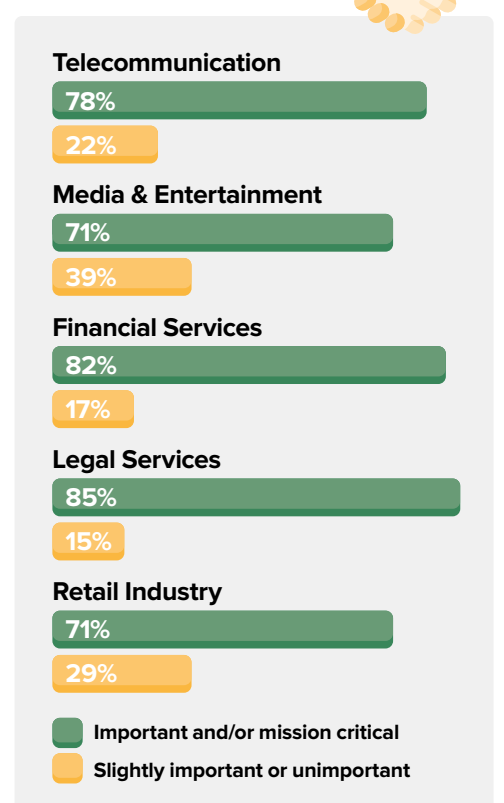
# Corporations look to start-ups for innovation



Large businesses are increasingly teaming up with new businesses to inject energy into their innovation efforts



Key sectors for collaboration:



Source: Open innovation report 2023, SopraSteria

# A helping hand

BY ARTHUR PIPER

Building a strong risk discussion culture across organisations is key in today's unpredictable world, as Dr Beate Degen, chair of the recently launched IRM Advisory explains

Every year, the World Economic Forum's (WEF's) *Global risk report* makes a big splash in the media and among risk professionals. Equipped with list rankings and in-depth analysis on the threat landscape, its annual publication has become something of a call to arms to tackle the major threats the planet faces. In its long-term championing of issues such as climate change and biodiversity risks, past issues can have an eerily prophetic feel to them.

Take the pre-pandemic edition released in January 2020. "A recent first-of-its-kind comprehensive assessment of health security and related capabilities across 195 countries found fundamental weaknesses around the world:

no country is fully prepared to handle an epidemic or pandemic," it said. "When health systems fail to mitigate vulnerabilities and adapt to changing contexts, they increase the likelihood of economic crises, political instability, social ruptures and state-on-state conflict."

## Awareness

While that final sentence feels like a description of where the world sits today, in many cases most of those risks have been around for years or decades. It is our awareness of them that has changed, according to Dr Beate Degen, chair of the recently launched *IRM Advisory*, the commercial arm of IRM. "Our perspective on risk has altered," she says. "What has happened

following the COVID crisis is that we have become more alert to high risks and to understanding the actual probability of such events occurring."

Much traditional risk management has undervalued large-scale risks that until the pandemic at least seemed rather vague and distant. While risk functions did track and record threat levels signals both within their own organisations and in the data they gathered – including from organisations such as WEF – most continued to downplay risks with a low likelihood of actually hitting home. "We need to get a better grip on those risks, where the volatility is potentially high, but we don't have data from the past we can build our assumptions on," Degen says.



**“ Risk managers must understand their board and executives and understand why they do things the way they do it**



## What has happened following the COVID crisis is that we have become more alert to high risks and to understanding the actual probability of such events occurring

Everyone working in the profession knows that risk itself is simply a part of the existential landscape for human beings. If one considers investing, for instance, a low-risk deposit in a local bank is relatively safe – depositors are rewarded not very much because (relatively speaking) not much can go wrong. In a hedge fund where risk is higher, the potential losses and gains enter into a more volatile relationship even though they operate within well-known parameters. In the realm of complex threats, such as those posed by climate change, geopolitical risk or biodiversity loss, the predictive power of those equations break down badly.

### Volatility

“You must make an upfront investment to mitigate climate risk because you cannot easily assess its impact and, therefore, the associated volatility,” she says. “People are struggling to get a grip around that volatility and, so to speak, price the risk accordingly.”

In addition, there can be a psychological gap between, for instance, extensive wildfires in California and Australia and the weather currently experienced in most of Europe so far. Because disaster feels further away, there can be a tendency to put off investment to secure national infrastructure, for instance, just because the more extreme weather may not arrive for another decade. But scratch beneath the surface and the impacts are already making themselves felt. Last year, for example, nuclear power plants in France cut output over fears that there would be insufficient water from the Rhône and Garonne rivers to cool reactors.

Climate risk is just one of many that comprise a complex system of interlocking factors which behave unpredictably (see [Complexity and risk, Enterprise Risk, Autumn 2022](#)) and, therefore, have high levels of volatility.

If risk control belongs to the traditional way of looking at managing those threats, Degen says that today professionals need to also be placing more emphasis on adaptation. “Risk adaptation means being in a position to adjust rapidly to changing circumstances, an ability that has become increasingly important for organisations,” she says. “A business’ risk culture must be mature enough to enable it to pick up on signals from within the organisation that are saying, for example, that there is a supply chain issue looming. The risks are already out there – it is understanding how and when to act at speed when they either start to impact

the business, or present new opportunities to make profits.”

To achieve this level of flexibility, organisations need to embed risk management within their corporate cultures, starting with setting the right tone at the top. In organisations that get it right, the risk management department becomes more of an ambassador for risk – someone who supports executive decision-making. But this is only possible where the first, second and third lines of assurance are working together and risk controls are embedded in both the operational infrastructure and within a well-understood risk culture, one that has a clearly defined risk appetite and tolerance and is geared towards discussing risk at all levels.

There are countless case studies of failures when these systems are not in place. In 2015, for example, Volkswagen’s cars were found by the US

## IRM ADVISORY

### ADVICE

Working with clients to identify and understand the impact potential risks could have on their businesses. Co-operating to evaluate and recommend practical and tailored solutions that help mitigate or manage risks and to ensure risk management strategies remain effective over time.

### GUIDANCE

Guiding clients every step of the way and empowering them to make informed decisions that balance risk with reward. Whether looking to address risk across the enterprise, or a specific area like cyber or climate, IRM Advisory’s experts will offer practical and actionable steps to identify, assess and manage potential risks.

### MENTORING

Helping to develop the team’s risk management skills and capabilities and providing a hands-on and personalised approach to meet the specific needs of each organisation – IRM Advisory supports organisations in building a stronger risk management culture.



**“ Risk adaptation means being in a position to adjust rapidly to changing circumstances, an ability that has become increasingly important for organisations**

Environmental Protection Agency to have software that lowered emissions from diesel engines when they were tested by regulators. When in laboratory conditions, the engines passed the emissions standards: when out on the road, they pumped out 40 times more pollutants than they did in the lab. This kind of discrepancy was already well known within the industry – and not just in Volkswagen cars. [A Swedish researcher](#) spotted low emissions lab test data compared to cars out on the road in 1998: the *Washington Post* reported on a similar case in the late 1990s – and even the

European Commission’s Joint Research Centre publicised the problem as late as 2011. No one seems to have listened. Last year, [The Guardian newspaper](#) estimated Volkswagen has so far paid out about £26 billion as a result of regulatory and legal proceedings following its mistake.

**Constructive dialogue**

Chief risk officers (CROs) who have not made headway in this area need to start by getting people on board in order to have more mature conversations about risk – and over time cultivating a better risk discussion culture at the top of the organisation.

“It starts with your board and with the executive team,” Degen says. “Risk managers must understand their boards and executives and understand why they do things the way they do it. Understanding doesn’t mean agreeing, but if you can grasp why the CEO has a certain motivation to do things, you can start to have much more informed conversations and start to exchange views in a targeted and constructive way.”

For example, if a CEO is under extreme cost pressures, a pending investment to proactively manage safety risks in a chemical plant by installing state-of-the-art



**“ If you are looking to improve the risk appetite and tolerance of your organisation, that is not something that should be done to you**

infrspectrometers could well be perceived by him or her as just an additional and unwelcome cost – not least because any potential upside cannot be quantified and assessed upfront easily. If the CRO understands this conflict of interest, it will be easier for him or her to focus on providing the right sort of information that the C-suite needs to perceive this expenditure as the investment it actually is.

She suggests CROs ask their CEOs what their no-go areas are, what sorts of arguments might change their apparently

fixed positions and where there is room for negotiation and a potential change of approach. And they need to be honest about their own biases and preferences. “It is absolutely crucial not to be too dogmatic and rigid at this stage because what you are doing is building both trust and understanding,” she says. Encouraging external voices to the board to share their expertise is also critical – it gets everyone out of their comfort zone and can provide a healthy change of perspective.

“The CRO should play an integral role in challenging the executive team and in offering different perspectives on risk and the way that is reported to them and throughout the business,” she says. “At the same time, if the executive team and the board do not take ownership for the new way of working around risk management, we are detaching the top management from the rest of the organisation.”

It is an area that IRM Advisory is looking to help organisations with – improving the quality of board discussions, strategic and tactical decision-making processes and offering other forms of boardroom guidance.

**IRM Advisory**

In fact, the concept of a bespoke advisory service has been bubbling for some time at IRM. In its extensive work with risk



## In IRM’s extensive work with risk professionals, corporate and public sector clients have been asking for impactful support with risk strategy and advice on how to support the board on such issues

professionals, corporate and public sector clients have been asking for impactful support with risk strategy and advice on how to support the board on such issues. Last year, IRM announced its own refreshed strategy and labelled its second pillar, elevating the membership offer (see IRM’s five strategic pillars). In a feature in this magazine (*Grand designs*, Enterprise Risk, Summer 2022), IRM’s independent non-executive director Stephen Sidebottom said that pillar would see the launch of a new arm to broaden and deepen the body’s current corporate offering. IRM Advisory is now here.

Degen was headhunted for the post. When I asked why she had found the offer interesting, she said that both the professionalism of IRM and the pleasure of building something up were factors, but also that she has the passion and experience to make the project successful. It is a claim that is difficult to argue with. In the 1990s, she had a passion for two seemingly incompatible subjects – industries that dealt

with petro-chemicals, and the environment. It was a time before climate-related topics were mainstream – before the creation of the United Nations Sustainable Development Goals in 2015.

Back then, the chemicals industry did have a responsible care programme, but she noticed that it struggled to bring qualitative factors into quantitative decision-making. Degen’s background was econometrics, operations research and mathematics, so she signed up for a doctorate degree at the University of Wuppertal and spent parts of the time at Boston University’s Centre for Law and Technology. Her supervisor and mentor in Boston was Professor Michael Baram, who had been writing books such as *Marine mining: Legal, technical and environmental considerations* since the mid-1970s.


“I learnt so much from him about how to look at the world and how to deal with the environment,” she says. It also opened her eyes to just how wide-ranging sustainability’s

role could be in a variety of circumstances: from smallholder farming projects to adapting capital market strategies in the commodities sector.

### Bringing it together

“It was always a very holistic approach and this is one of the reasons I find IRM Advisory so attractive,” she says. “I like to work where topics meet, and that’s probably also a personal strength – that I can combine different topics and then make something new out of them.” Degen has worked in a broad range of roles – from head of corporate strategy projects at a global chemical and pharmaceutical company, and as a partner and executive director at the global consultant EY, to her current portfolio of roles as chair and advisor to several organisations, as well as chairing for a number of years a key oversight body at the United Nations. One key attraction is that IRM Advisory is not looking to replicate the kind of large-scale consulting projects that heavyweight firms specialise in. It is instead aiming to help clients by creating the kinds of constructive dialogues that we spoke about earlier. She uses phrases such as co-development, partnership and empowerment.

“If you are looking to improve the risk appetite and tolerance of your organisation, that is not something that should be done to you,” she says. “It should be done by you with the proper level of help, challenge and support.” Similarly, conducting maturity assessments and benchmarking exercises requires a small group of highly experienced people rather than dozens of consultancy staff.

“We come very much from the heritage that we help to develop risk professionals and that we understand the problems on the ground because we have been working in that space for years,” she says. “This very strong backbone is, so to speak, the engine powering IRM Advisory’s training and mentoring.” 

## IRM’S FIVE STRATEGIC PILLARS

- 1 Creating world-class education and qualifications
- 2 Elevating the membership offer
- 3 Creating impactful global thought leadership
- 4 Building international collaboration and partnerships
- 5 Remaining financially sound.

# Why the banking crisis is back

---

BY MICHAEL RASMUSSEN AND WILLIAM GONYER

A photograph of the Silicon Valley Bank building, a modern glass and steel structure. The building's name, "Silicon Valley Bank", is prominently displayed in large, dark blue letters on the upper facade, followed by a blue arrow pointing to the right. The sky is a clear, deep blue.

Silicon Valley Bank

## The latest banking crisis in North America has put potential failures regulation, governance and risk management back in the spotlight

Springtime often becomes a metaphor for change, new growth and transformation. While change and transformation tend to be the by-product of dissatisfaction with behaviours and patterns that are no longer tenable to the present situation, sometimes this change is also involuntary in its nature – an uncomfortably forced evolution that imposes progress on us. Springtime this year has pushed forward a mass sobering for the banking industry. After riding a wave of ultra-low interest rates and high market liquidity, a domino effect of events has brought on the failure of several major regional American banks, marking the greatest shake-up of the global financial system since the financial crisis of 2007-08.

As the age-old adage goes, “there is nothing new under the sun.” The driving factors that led to the collapse of Lehman Brothers, Bear Stearns, Wachovia and Washington Mutual are almost identical to the key drivers of the bank failures within Silicon Valley Bank (SVB) and Signature Bank this year – a gross failure of governance and risk management, the exception being First Republic.

### Situational awareness


The interconnectedness of organisational objectives, risks, resilience and integrity requires 360° situational awareness of governance, risk and resiliency. Organisations must see the intricate relationships and impacts of objectives, risks, processes and controls. It requires holistic visibility and intelligence

regarding risk and resiliency.

Organisations such as banks and other financial institutions take risks all the time. Still, the failure to monitor and manage these risks effectively in an environment that demands agility can lead to a tinder box of potential catastrophe. Too often, risk management is seen as a compliance exercise and not truly integrated with the organisation’s strategy, decision-making and

\$66 billion and push far beyond average industry risk parameters with its held-to-maturity (HTM) securities portfolio, ramping what was mostly agency mortgage holdings from \$13.5 billion at quarter 4 of 2019 to \$99 billion at quarter 4 of 2021.

SVB’s big problems were with its HTM portfolio. The bank increased its security portfolio by 700 per cent, buying in at a generational top in the bond

 **After riding a wave of ultra-low interest rates and high market liquidity, a domino effect of events has brought on the failure of several major regional American banks**

objectives. It results in the inevitable failure of governance, risk and compliance (GRC) and risk management, providing case studies for future generations on how poor GRC management leads to the demise of organisations.

The collapse of SVB is one of the most blatant cases of this. For example, SVB failed to institute some of the most basic risk management practices by industry standards. Starting from the end of 2019, SVB deposits grew from \$61 billion to \$189 billion by quarter 4 of 2021. Interest rates at the time were so low that these deposits were treated as free money at ~25 basis point cost average. SVB then used these inflows to increase loans 100 per cent to

market and buying \$88 billion of mostly 10 plus year mortgages with an average yield of just 1.63 per cent. In the absence of adequate interest rate risk management, this resulted in massive unrealised losses when the Federal Reserve began hiking its benchmark interest rates.

### Deregulation

SVB’s HTM securities had mark-to-market losses as of quarter 3, 2022 of \$15.9 billion, compared to just \$11.5 billion of tangible common equity. Due to lobbying for deregulation by SVB, as well as other midsized banks such as Signature Bank (of which Barney Frank of Dodd-Frank was a board member), regulators did not require SVB

## “ Too often, risk management is seen as a compliance exercise and not truly integrated with the organisation’s strategy, decision-making and objectives

to mark its HTM securities to market. However, internally they should have been doing this anyway, as well as running risk models against changing rates.

The deregulation that enabled their increased risk tolerance came as a result of Congress passing the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA), also known as the Dodd-Frank Reform Act. The act was signed into law in May 2018, and it raised the asset threshold for systemically important financial institutions (SIFIs) from \$50 billion to \$250 billion, effectively reducing the regulatory burden on many mid-sized banks such as SVB and First Republic.

On top of this, due to the Federal Reserve Bank’s interest rate hikes, SVB saw accelerating deposit outflows (-6.5 per cent YTD in January), a mix shift away from non-interest accounts and skyrocketing interest costs (money markets now yield 4 per cent), as well as increased burn rates from the bank’s venture clients resulting in customer deposit drawdowns. As SVB’s funding costs continued to reset higher, SVB was faced with a massively high negative carry cost on its HTM portfolio, largely a fixed-yield securities portfolio.

But SVB’s greatest failures extend to the top – its leadership. The Federal Reserve’s review described SVB as “textbook case of mismanagement” and further described a failure of oversight and accountability of senior leadership by the bank’s board of directors. Only one member of SVB’s board had previous banking experience. The practices and procedures used by SVB’s risk management team raises serious questions on their competencies based on evident gaps in their risk

management frameworks. SVB’s risk management team “failed to establish a risk-management and control infrastructure suitable for the size and complexity of SVBFG when it was a \$50 billion firm, let alone when it grew to be a \$200 billion firm”, said the review. SVB had 31 identified unaddressed “safe and soundness supervisory warnings” more than triple the average number of peer banks. Furthermore, the bank was also left without a chief risk officer for 7 months in 2022, a departure that may demand an explanation. The discoveries made by the Federal Reserve and Treasury Department regarding the bank’s risk management practices only beg more questions outside of the obvious conclusions: SVB failed to institute an adequate asset liability committee, erroneously focused on short-term profits, and neglected long-term associated risks.

### Bad timing

The relaxing of Dodd-Frank also came at exactly the worst time. It happened almost a year before the beginning of the Federal Reserve’s tightening cycle and at the natural end of an era of economic expansion that was later disrupted by emergency monetary intervention measures during the global COVID-19 pandemic. Mid-sized banks could now take on greater risks, and they did so during a time of irregular economic factors of expanded emergency liquidity.

First Republic’s portfolio arguably could have withstood the fluctuations. However, First Republic lost more than half of its deposit base amid SVB’s collapse, pulling the bank into a critical territory and ultimately leading to its collapse and takeover by JP Morgan and the Federal Deposit

Insurance Corporation (FDIC). This marked the second-largest bank collapse in US history after Washington Mutual in 2008.

First Republic’s traditional savings and loan business model was arguably sound. It catered to wealthier clients in the tech sector, targeting the employees at companies like Apple, Alphabet and Meta. First Republic even had a branch inside of Facebook’s headquarters. But First Republic’s failure was purely panic induced. Even with paper losses on low-interest loans and its interest rate risk mismatch, the bank could have survived if it didn’t have to rapidly fund withdrawals by depositors seeking higher returns on deposits elsewhere, as well as outflows triggered by panic amid the failure of SVB. As a result, the bank was forced to rely on government lending facilities at rates that exceeded its income in an attempt to ride out the storm. First Republic’s





George Bailey (James Stewart) realises the money has gone from his bank in Franz Capra's depression-era classic *It's a wonderful life!*

problems are almost reminiscent of Bailey's Building and Loan in Frank Capra's 1946 film *It's a wonderful life*, only in this not so wonderful life the townspeople did not temper their panic and rally around their community bank.

### Re-regulation

The recent failure of these regional banks will likely trigger a new wave of regulations and guidelines as well as a reversal of the changes made to regulatory frameworks for midsized banks in 2018. Regulators need to consider that with the increased scale of the financial system, midsized banks that may be only regionally important can still pose a significant systemic risk as supervisory authorities do not have the resources to monitor their activities and should not underestimate the propensity for mismanagement. Asset thresholds for enhanced prudential standards for SIFIs should be reversed from \$250 billion to \$50 billion. Regulators and organisations with large deposits also need to consider the concept of dual fiduciary duty.

In the case of SVB, a bank of choice for many venture capital firms and venture-backed companies, the burden of large deposit risk cannot fall solely on the bank. Venture capital firms, while exempt from many of

the regulations and compliance burdens of hedge funds and other asset managers, were arguably negligent in managing their cash risk for their limited partners and thus somewhat complicit in the risk concentration of SVB. The leading practice of asset managers is to hedge cash risk through treasuries. A venture capital firm's responsibility to its investors must extend to its cash risk within its portfolio companies.

Too often, regulators and bank managers alike continue to make policies solely in the vacuum of a crisis. Policy developed in the vacuum of a crisis is inherently inadequate, as it usually only accounts for remedying the causation and symptoms of the present crisis. Supervisory authorities need to consider expanded guidelines for bank governance and leadership, and the policies set by leadership for financial institutions should meet qualification standards. All bank board members should be certified by supervisory authorities such as the Office of the Comptroller of the Currency (OCC), FDIC and Financial Industry Regulatory Authority (FINRA) for a minimum qualification standard.

### Cost of failure

While The US Department of the Treasury and Federal Reserve have

taken responsibility for inadequate supervisory measures of these troubled midsized banks, financial institutions now need to realise more than ever that increased legal risk tolerance does not equate to acceptable risk tolerance. Banks must institute more sophisticated internal risk frameworks that factor in significantly higher stress tests for implied volatility.

Major money centre banks are forced to adhere to a wide range of scenarios for long-term resilience, but midsized and even small banks need to develop their own internal frameworks beyond the demands of compliance that mirror the top of the industry at scale, even if it comes at the cost of profits because the cost of a bank failure is far greater than neglecting profits made unsustainably. Banks that are currently undergoing pressure should consider seeking to consolidate with peer banks before they are forced into consolidation, liquidation or shotgun acquisitions. Well-structured asset-liability committees and audit committees should become a universal practice for banks of all sizes.

The conclusions of the Federal Reserve's review of SVB implicitly stated that two of the three critical weaknesses of the bank were governance and risk management. The further conclusion of the review was that while SVB was compliant, compliance alone was inadequate because the regulation and the supervisory frameworks were inadequate in preventing the bank's failure. The second and third largest bank collapses in US history have set the stage for a new wave of regulation to reinforce neglected gaps in global financial services from the United States, European Union, United Kingdom, the Commonwealth and beyond. 🇪🇺

**i** Michael Rasmussen is an analyst and pundit at GRC 20/20 Research. William Gonyer is a partner of Group697.

# The reach of regulation

BY CLIVE THOMPSON

The UK's review of banking rules is a welcome opportunity to reform what does not work – yet the outcome could also shift the country's financial system into unknown territory

**S**ilicon Valley Bank had a UK business with 3,500 customers, reportedly mostly tech start-ups. The Bank of England, which regulated these operations, had initially thought to place them into administration once the news that the parent in the US had become insolvent (see *Why the banking crisis is back* in this issue). They instead brokered a deal with HSBC, who bought them for just £1.00 in March. With this, HSBC received the SVB business and the customer deposits, which were previously reported as £6.7 billion.

Meanwhile over in Switzerland – around a week or so after the SVB deal in the UK – a similar deal was brokered by the country's central bank. This time, it was many more times in size: UBS bought Credit Suisse, a bank deemed as systemically important, for CHF3 billion and

received the business and assets reported as US\$1.1 trillion in return. Credit Suisse shareholders will lose significantly on the

risk management and an inability to change when faced with a new world of rising interest rates.

If regulators failed to maintain

**“** **These actions by the regulators show how critical they are when the banking system goes into crisis**

deal as they will get a share of the CHF3 billion together with a single share in UBS for every 22.48 shares they have in Credit Suisse.

## Critical role

These actions by the regulators show how critical they are when the banking system goes into crisis. In both cases, the crises were of the individual banks' own making – poor governance, poor

stability, we would face a world where contactless exchange fails, cash will be king until it becomes worthless through inflation and illiquid assets would become the principal bargaining tools – a dystopian outlook which harks back to Dickensian times. Today's financial system, built from its foundation at Bretton Woods to the Basel Accords of now, provides the glue which enables



Reforms are also looking into delivering a “new direction for retail disclosure” and “removing burdensome customer information requirements”. These will undoubtedly have more of a direct impact on those who use the financial system. Again, exactly what is in mind needs to be confirmed.

### Undue risk taking

It is, of course, essential that our regulatory regime keeps up to date with what is happening in the financial system. There are undoubtedly some aspects that do need updating and reforming, such as the increasing use of shadow banking, the offshoring of certain activities bringing a need for a more integrated approach and cybercurrencies (or at least the bourses within which they trade), all of which operate “in the twilight” with no regulation.

It seems to me, however, that these reforms could provide increased incentive for undue risk taking (by lessening personal accountability), enhance a bank’s defence against mis-selling (and the ability for the customer to seek redress) and increase a UK bank’s leverage to lend.

Finally, the reforms will also impose a new (albeit secondary) remit on the PRA and FCA whereby they will have “clear, targeted recommendations on growth and international competitiveness”. These are duties which, as far as I can see, no other regulator in this globally connected world has. This final aspect of these reforms could, if not used correctly, turn a gamekeeper into a poacher. ☹

## “ These reforms could provide increased incentive for undue risk taking

us to buy an iPhone for a tenth of the price it would be if it were made in either the UK or the US, as well as supporting mortgages and pensions, and the increasing financialisation of daily life.

Given the importance of regulation to maintain our standards in this modern, hyperconnected and rapidly changing world, it is, of course, important for governments to review those regulations. And the UK government announced a series of reviews, the [Edinburgh Reforms](#), late last year.

### Devil in the detail


As in everything to do with regulation, the devil will be in the detail. The exact reforms

have not been spelt out, but the intention is to build “a smarter regulatory framework for the UK,” which will distance it from the regulation we currently use. Reviews are underway into the ring-fencing regime for banks, the regime imposing personal accountability on senior managers for mismanagement, and into the kinds of assets institutions can invest in over the long term.

These are by and large highly technical and will have their most immediate effect on the bankers and insurers who operate within those regulations. Of course, should the regulation fail, as we have seen many times in the past, we will all pay.

Interestingly, the Edinburgh

**i** Clive Thompson, CFIRM, is technical adviser to IRM and author of the “Financial risk management” chapter of *Practical project risk management, 2nd Edition* (Editor: D Hillson). The views expressed are his own and do not necessarily reflect the official position of IRM.



# The rise of risk bots

---

BY SEAN GOTORA, ALEXANDER LARSEN AND MYRIAM BOU YOUNES  
WITH SOME HELP FROM CHATGPT

ChatGPT has raised the profile of artificial intelligence programs, proving they can do tasks previously thought to be the unique preserve of humans. The implications of society and risk management could be profound

**A**rtificial intelligence (AI) is becoming increasingly embedded within society. While this was highlighted by recent media coverage of the generative chatbot ChatGPT – it writes answers to queries – the use of AI is already implemented within a range of devices from Siri and Alexa, self-driving vehicles and customer service desks to banks that use it to protect credit cards from fraud. Today, AI plays a big part in making life easier and more efficient.

Many scientists and pundits have rung the alarm bell about the risks AI poses, including OpenAI chief Sam Altman – the man in charge of ChatGPT. Yet AI also promises to improve society by increasing efficiency and productivity in various industries. It can automate repetitive tasks, freeing up time for workers to focus on more creative and meaningful work. For example, AI is used in the manufacturing industry to perform tasks such as quality control and inventory management. This allows workers to focus on tasks that require human expertise and decision-making, such as problem solving and strategy.

### Insights into the future

ChatGPT offers insights into how those processes may develop so that humans and machines may work better together.

For example, healthcare is increasingly utilising AI. It can

potentially revolutionise medical diagnoses and treatment by analysing large amounts of medical data. The patterns it identifies may help to provide personalised recommendations as well as to predict outbreaks and spread of contagious diseases. Additionally, there have been cancer studies undertaken with AI that show around 90 per cent accuracy in predicting breast and lung cancer in scans and images.

questions or go into answers at a deeper level and develop more accurate theories based on data. Teachers too can reap benefits from potentially grading papers and offering feedback. This opens up the possibility of scaling up education to reach a much larger proportion of the population than has so far been possible. Now imagine a world where everyone has, at the very least, a reasonable level of education where people

### ChatGPT offers insights into how humans and machines may work better together

Doctors are already experimenting with ChatGPT and are finding that its diagnosis can be both accurate and fast while offering potential insights that the doctors may not have caught without it. While accuracy is an issue with generative models such as ChatGPT, the ease with which it can provide a range of possible diagnoses can be a real benefit to both doctors and patients.

If we ignore the fact that using ChatGPT will enable students to cheat in their coursework, it is hard to miss the real educational benefits it can provide. We should acknowledge that this technology is available 24/7 allowing students to access it anytime and anywhere. With the AI doing some initial research for them, it allows students to answer more

are less prone to being misled or falling into poverty.

Fake news has been a troubling phenomenon for over a decade, especially with the rise of social media. The torrent of content includes some seriously misleading information that has potentially influenced elections and sparked violent protest. By opening ChatGPT up to social media, search engines and live data, people may finally have a partial solution to this problem. The app can quickly check facts and curate a database of news sources based on credibility. Using such technologies, users could score journalists based on their political leanings, for example, and get a better understanding of how the article might be trying to lead them. It could also act

as a peacekeeper by analysing social media activity to identify sources of fake news before they spread too far and become seen as established facts.

### Quality issues

ChatGPT is a language model trained on large datasets and, as such, the quality of its output is directly related to the quality of the input data used to train it – a principle known as the data quality principle. Low-quality input data leads to perpetuating or amplifying existing biases and misinformation in the dataset provided. For example, while we previously talked of the benefits of its use in healthcare to assist with medical diagnosis or treatment, ChatGPT may be trained on data that does not accurately reflect the diversity of patients, resulting in dangerous medical decisions. In journalism, a model trained on misinformation will generate news stories not based on facts – leading to the spread of more false information and the creation of echo chambers in social media. Such widespread misinformation can be used to manipulate public opinion for marketing or political agendas. This obviously contrasts with the control of fake news that we highlighted.

In addition, ChatGPT often returns incorrect answers. The model answers questions by building its answer word by word by selection of the most probable token – a piece of a word that averages four characters – to come next. Effectively, the model is guessing the answer. Since ChatGPT is not linked to the internet, the model's data is not as up to date as some other AI technologies. To mitigate these risks, it is important to use diverse and representative training data, regularly evaluate the model's performance and fairness, and involve diverse stakeholders in the development and deployment of the model.

While there are opportunities for improving education, ChatGPT could also threaten the current



education system. It has passed a law school exam and medical exam, and ChatGPT's predecessor GPT-3 passed an MBA exam. The bots did particularly well in writing essays, which prompted Stephen Marche, writing in *The Atlantic* magazine, to declare the college essay dead. But the models also produced incorrect answers, especially when answering mathematical questions. This raises concerns about students

and advances in technology is not new, the accelerated pace resulting from the implementation of models such as ChatGPT is unprecedented, and the subsequent societal impacts should be a cause of concern for governments to take immediate action. Mitigating measures can include employee retraining programmes to meet the increase in demand for new jobs related to the implementation of these

**“ ChatGPT is a language model trained on large datasets and, as such, the quality of its output is directly related to the quality of the input data used to train it**

lacking proper understanding and critical thinking skills, and relying on outdated information – especially if they become dependent on the technology.

The ease of automation of tasks using AI models is making a lot of jobs redundant. For example, personnel in customer service support are at risk of being replaced. Although job displacement due to automation

models, setting up a social safety net, revision and update of labour and other relevant regulations, and the development of long-term strategic vision for a more sustainable and inclusive economy.

### Risk management

AI and natural language processing (NLP) combined have the potential to revolutionise how risk management is conducted



## AI tools will identify and assess risks, as well as suggest or apply mitigation actions or strategies without the need for current levels of human-machine interface

within the next one to three years. Like any other technological shift, everyone in the risk industry needs to be sufficiently skilled to exploit and maximise its potential.

These tools could enhance and evolve risk management from its current state as a dark art that is highly dependent on a risk manager's personality and capabilities – especially since many risk professionals have access to limited information, which itself is subject to individual and organisational biases. Perhaps they could move the profession towards a less personality-dependent model that draws on a broader range of data.

Where to start? One clear low-hanging benefit lies in automating risk management procedures. AI and NLP's ability to process large amounts of structured and unstructured data – such as text, audio and video – from a variety of sources could help risk managers identify risks from data that has been difficult to pull together. Bringing together and analysing information drawn from such disparate sources as scientific data, operational data, operating manuals and instructions, procedures, best practices, social media, news articles and customer feedback could provide new and unexpected insights to the business.

Risk managers can analyse large amounts of data and identify patterns that may indicate a potential risk by fully utilising AI's machine learning algorithms. This can be done much faster and more accurately than by using traditional methods, such as manual data entry and analysis. Risk identification and assessments will become faster while referencing all local, geographically, industrially,

situationally specific available data and making inferences where there are gaps.


For example, within the petrochemical industry, multivariant factors and scenarios may be used to identify risks live and can reference all past and current data relating to the situation. This will enable risk managers to respond more quickly and effectively to emerging risks. By analysing data in real time, risk managers can identify potential risks as they are developing and take action to mitigate them before they become a major problem. As this technology develops, AI may even go further to suggest mitigation strategies or actions and in some cases implement them after running multiple simulations to anticipate the effect of the mitigation on the risk event. This kind of decision-making is already utilised in smart vehicles.

### Automating risk management

As AI and NLPs continue to evolve, it is likely that enterprise risk management will become increasingly automated. This will require risk managers to acquire new skills and tools to use these technologies effectively – or risk becoming caretakers of the systems, if not redundant. For example, currently many risk managers need to be proficient in programming languages, such as Python, R and SQL, and be able to understand and use machine learning algorithms and data visualisation tools. These skills help organisations and their risk professionals to analyse and interpret large amounts of data.

But in the near future, AIs and NLPs will have access to an even broader range of data. They

will be able to automatically code (prompted or unprompted), analyse data, identify patterns and reference all available worldwide data. From these processes, the tools will identify and assess risks, as well as suggest or apply mitigation actions or strategies without the need for current levels of human-machine interface. If risk managers do not identify the risk of AI and plan for appropriate upskilling in these emerging tools, the future could be bleak for the profession.

That is why it is increasingly important for risk managers to stay up to date on the latest developments in AI and NLPs, as well as to continue to develop their knowledge and skills in these areas. Attending conferences, workshops and training sessions, as well as reading research papers and articles on the subject can all help – as can joining peers in [IRM's Special Interest Groups](#). For risk managers to be able to fully exploit AI and NLPs, they need to become more creative, more informed and be able to integrate concepts to be able to ask the right questions (prompt) to the AI to get a useful result. 



Sean Gatora is chair of IRM Qatar Regional Interest Group and a member of IRM Energy and Renewables Special Interest Group. Alexander Larsen (BHRM, CFIRM) is chair of IRM Energy and Renewables Special Interest Group and Founder of Risk Guide. Myriam Bou Younes is a member of IRM Qatar Regional Interest Group and IRM Energy and Renewables Special Interest Group. This article is adapted from IRM's paper [Artificial intelligence, friend or foe?](#)



# Risky behaviours

---

**BY SIMON ASHBY**

People risk is often difficult to identify and harder to control. The latest in the series of IOR operational risk sound practice guides lays the groundwork for an effective approach

People are a central component of operational risk, as reflected in the standard Basel definition: “the risk of loss resulting from inadequate or failed internal processes, people, systems and external events”.

By extension, effective people management is an essential part of a sound framework for operational risk. The aim is to ensure that people act in a manner that does not unnecessarily increase an organisation’s exposure to risk or hinder efforts to identify, assess, monitor or control this exposure. In fact, where people are involved, there is always an element of operational risk. It is often because of the actions or inactions of people that the boundaries between operational and other risk event types are blurred.

## Scope of risk

Not surprisingly, since exposure to people risk is created through the actions or inactions of individuals or groups of people working together, its scope is wide. The nature of people risk changes often, reflecting the complexity of people and their attitudes, beliefs and behaviours.

Though the scope of people risk events is varied, their sources of origin are limited (see *Sources of people risk*). Fundamentally, people risk events come specifically from an organisation’s external and internal operating environments. In the case of the external environment, people risk events may flow from the actions or inactions of external stakeholders, as well as from external events like pandemics. In the case of the internal environment, the primary source is the organisation’s internal stakeholders, specifically the leadership (board, executive and management), along with all other employees and

contractors. By understanding the origins of people risk events, organisations can help to improve the effectiveness of their people risk management activities.

## Identifying risk

In part, the identification of people risks should occur as part of an organisation’s routine operational risk identification activities. One

the influence of people on residual exposure is determined by the way they operate the available controls – which may or may not be wholly effective. This analysis could be performed either by the relevant risk owners or the operational risk function.

Unfortunately, such an approach will not help to identify the depth of people risks in

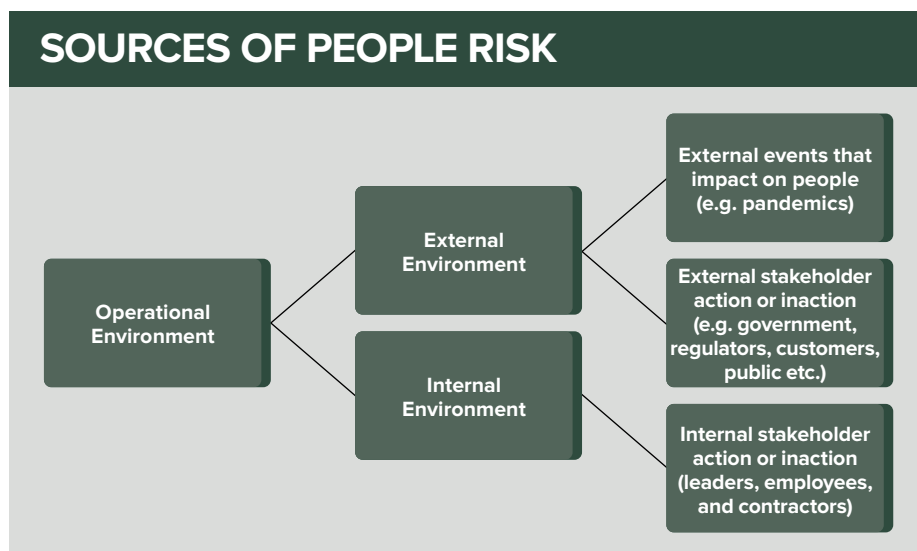
“ **The nature of people risk changes often, reflecting the complexity of people and their attitudes, beliefs and behaviours** ”

approach to the identification of people risk is to review exiting operational risk registers or risk and control self-assessments and highlight those risks whose exposure are significantly influenced by the actions or inactions of people. This could include identifying the influence of people on both inherent and residual exposure. Inherent exposure will be influenced by the extent to which people are an underlying cause of loss whereas

an organisation, because it fails to analyse why people may act to cause harm to an organisation or its stakeholders.

## Antecedents

To understand why people act in specific ways, organisations should work to identify the antecedents of this action or inaction. *Antecedents to people risk events* highlights three key antecedents: the pressures for action or inaction, the payoffs from action or



## ANTECEDENTS TO PEOPLE RISK EVENTS

### Pressures

- Visible pressures (e.g. commercial pressures to achieve strategic or operational objectives and financial pressures).
- Invisible pressures (e.g. social and cultural pressures, including the risk culture of the organisation).



### Payoffs

- Motivation (that an individual or group has for action, such as their self or collective interest or for the benefit of the organisation).
- Opportunity (to receive a payoff, for example an individual spotting an opportunity to profit from theft or fraud).
- Rationalisation (how an individual or group justifies the payoff they expect to receive or create for an organisation).



### Decision Process

- Cognitive decision biases. A systematic deviation from the norms of rational judgement. Individuals or groups create their own subjective reality and it is this reality, rather than objective input that conditions their decision making.
- Heuristics – subjective rules of thumb that are used to speed up decision making, especially when information or ability is limited. For example a reliance on intuition or “gut feel”.

they are managed. In terms of assessment, this means analysing the combined effectiveness of the various elements which comprise an organisation’s governance and control systems to determine where the holes (weaknesses) lie and whether human errors could slip through the holes in this system to cause unexpected losses.

People risk mapping is a form of process mapping that focuses on the nature of human interactions and whether these interactions could give rise to people risk, for example interactions between first-line staff and their line management along with second-line control functions and the executive team. Such interactions may be internal and external. Internal interactions occur between the staff, management and senior leadership that comprise the various departments, teams and functions of an organisation. External interactions include the influence of external stakeholders such as regulators, customers and the public.

People mapping can be used to look for inappropriate interactions. This might include collusion between two or more individuals or groups for their mutual benefit (for example, individuals in the procurement and finance teams might collude with external suppliers to make fictitious payments) or one individual or group exploiting another (for example, mis-selling). Keith Blacker and Patrick McConnell’s 2015 book *People risk management* is a useful guide to this approach.

### Monitoring

It is important that information on an organisation’s exposure to people risk is monitored and reported to senior management, including the executive team and board of directors. The effective reporting of people risk can help an organisation fulfil its legal and regulatory responsibilities for corporate governance and internal control.

People risk may be monitored and reported separately or as

inaction and the decision-making processes used to determine the specifics of an action or inaction. It is recommended that organisations take time to consider these antecedents so that they identify the factors that are most likely to impact on their people and the propensity for these people to cause harm.

Although this approach is effective, it can also be expensive and should therefore be conducted in those areas of highest risk. For example, organisations that work in safety-critical sectors (for example, nuclear, defence or chemical processing) or sectors where the actions or inactions of individuals or small groups could threaten the financial viability of an organisation (for example, banking, and financial market trading) should invest significantly more resources in this activity than other sectors.

### Assessment

While it is beyond the scope of this article to go into detail, generally speaking organisations use four key ways to assess risk: risk and control self-assessment (RCSA), culture surveys, fault tree analysis and people mapping. I would direct readers to IoR’s [Sound practice guidance paper on RCSA](#), and IoR’s [Sound practice guidance paper on risk culture](#).

Fault tree analysis is used to investigate how risk events are caused, working backwards from the event in question to understand the various human, process and systems failures and/or external events that might interact with each other to cause the event. Humans are fallible and that errors are to be expected. Hence, it is not appropriate to blame people for these errors; rather, the focus should be on the governance and control systems through which

## PEOPLE RISK INDICATORS AND PEOPLE-RELATED CONTROL INDICATORS

### People risk indicators (examples):


- Cyber-attack indicators of compromise, such as the number of login red flags
- The number of employment grievances and disciplinarys
- Reported health and safety incidents – both the number affecting staff and those affecting other stakeholders
- Risk culture metrics
- Sickness absence as a percentage of total work time available

### People-related control indicators (examples):

- Audit actions (percentage overdue)
- Breaches of internal control policies and procedures (number of reported breaches)
- Known conflicts of interest (number)
- Data protection breaches (number of internal and external)
- Staff training gaps (percentage of staff who have not completed compulsory training)

An organisation's management control system comprises the various controls that are used to gather information on and direct (through the application of positive and negative controls on individuals and social groups) the use of resources for the benefit of the organisation and its stakeholders. This system will include both formal and informal elements to direct and control the actions of people. This means that an organisation's management control system spans tangible matters like its management hierarchy as well as human-social factors like culture.

Organisations rely on a range of internal and external stakeholders to achieve their objectives. Generally, the people that comprise these groups will act in the interests of the organisation and all other stakeholders; however, when they do not, significant harm can be caused to the organisation, as well as harm to the health, wellbeing and wealth of other stakeholders.

The effective management of people risk does not necessarily require a discrete risk management framework. Often, consideration of people risk can be included in an organisation's enterprise risk or operational risk management frameworks. However, even when this is the case, consideration should be given to the use of people-focused risk management tools like people mapping or monitoring an agreed set of people risk metrics. People lie at the heart of almost every operational risk event that an organisation will be exposed to, even where such events are not considered to be people risk. 

## “ It is important that information on an organisation's exposure to people risk is monitored and reported to senior management

part of wider operational risk or enterprise risk monitoring and reporting. This will depend on the nature, scale and complexity of an organisation's activities and people risk exposures. However, it is important that all statutory reporting requirements are met, such as the UK's RIDDOR requirements.

Where an organisation monitors and reports risk and control indicators, it is recommended that it periodically reviews its suite of indicators to ensure that people risks are appropriately

represented. (See, *People risk indicators and people-related control indicators* for examples.)

### Controlling

Controlling people risk requires a diverse range of controls. This includes positive controls that motivate, support and guide actions that benefit the organisation and its stakeholders. In addition, organisations can implement negative controls that coerce, punish and prescribe to help prevent action or inaction that causes harm.

 **Simon Ashby, FIOR, is an associate professor of financial services at Vlerick Business School in Belgium and a former council member of the Institute of Operational Risk. IoR's Operational risk sound practice guides can be found here.**

# Waking the sleeper risks

BY RICHARD MACKIE



## Traditional risk management calculations can hide important risks from view. Bringing them to light is imperative if organisations are to improve their resilience

Since the pandemic, there have been several reviews considering how we can ensure that as professionals, society and governments we are better prepared. One key learning is that the basic risk management framework has allowed pandemic and catastrophic risks to be hidden. An ineffective risk management framework tied to a multiplication-driven risk-scoring matrix has the potential to create sleeper risks.

A sleeper risk, like a dormant volcano, has a perceived low likelihood of occurring but the potential to cause disaster if it does. Organisations and governments around the world continue to be blindsided by these sleepers, with post-incident investigations often highlighting that warning signs were ignored. There is an opportunity post-COVID to change our approach. The multi-aspect assessment model (MAAM) is a far more effective approach to risk ratings and strategic risk reporting.

### **Multiplication muddle**

On the morning of February 28, 2001, a Class 91 express train travelling from Newcastle to London collided with a Land Rover that had crashed down the embankment onto the railway line. The derailed train came into the path of an oncoming freight train, which resulted in the deaths of ten people. Using multiplication analysis, we can say that the events leading up to the accident were highly unlikely and would be classed as

rare – scoring a one out of five. In addition, while the event would be seen as highly unlikely, the consequences would be classed as catastrophic – scoring the highest rating of five. Multiplying the two numbers would produce a risk score in a risk report of five out of the 25 points available.

In another example, a member of staff falls over in an office kitchen that has a wet floor and breaks their wrist. The staff member cannot work

Even when risk managers adapt the scoring matrix to boost the impact score, the result is often unsatisfactory and can lead to the board focusing on the wrong top ten threats to the organisation. In a post-pandemic world, we need a more dynamic approach.

### **Risk velocity**

In the risk profession, we always consider impacts and likelihoods when assessing risks but without creating a situation where an



## **An ineffective risk management framework tied to a multiplication-driven risk-scoring matrix has the potential to create sleeper risks**

and takes legal action against the employer. In a busy office, floors do get wet, people fall over – sometimes taking legal action. The risk analysis might say there is a moderate chance of this scenario happening, scoring it three, and the consequences would also be moderate – another three. With a rating of nine, this incident has almost double the rating in the risk report than that of the train crash. In fact, very different risks can be allocated the same score using this model making it difficult to assess their real-world impacts.

With multiplication models, our risk management framework and the scoring methodology has become one of our biggest risks.

office fall becomes bigger than a train crash. In the model that I propose, the risk matrix is weighted towards impact, which does away with confusing scores and saves important risks from lingering at the bottom of the risk register. With a more accurate rating matrix we can use our risk scoring to design a proportionate approach to reviewing risks. This will ensure the focus is on the risks that have the potential to create serious problems versus the business-as-usual risks.

In fact, I have spoken at events since 2011 about what I call risk velocity and believe that it is more relevant today in our unpredictable world. The concept is very simple. V1

## RISK AND VELOCITY SCORING MATRIX

	A	AE	AD	AC	AB	AA	<b>Overall Risk Rating/Level</b> Major Significant Moderate Minor Low
RISK RATING	B	BE	BD	BC	BB	BA	
	C	CE	CD	CC	CB	CA	
	D	DE	DD	DC	DB	DA	
	E	EE	ED	EC	EB	EA	
		E	D	C	B	A	
	VELOCITY RATING						

## REASSESSING THE RISK FROM AN OFFICE FIRE

	LIKELIHOOD	IMPACT	SCORE
Multiplication assessment	1	5	5
	RISK LEVEL	VELOCITY LEVEL	SCORE
Velocity assessment	4 (B)	5 (A)	BA

so if we combine these elements on a similar matrix, we can rate the risks with a velocity score (see *Risk and velocity scoring matrix*).

### Applying risk score and velocity score

Let's look at the risk of fire at head office. In a traditional multiplication risk matrix, the likelihood would be highly unlikely or rare; however, the impact would be significant to major, due to the potential for multi-million-pound losses, loss of the building and even death or serious injury. As with the train crash example, this would be rated green or low risk, at five.

Changing to not multiplying the scores, the risk becomes a category B risk – not the highest level but, given the potential to cause significant disruption, the risk must be managed appropriately. Add in the risk velocity, the response time to a fire would need to be immediate, there will be a requirement for computer system backups, relocation to new premises and staff need to be made aware. The recovery time could be months or even years. In terms of risk velocity rating, this has now become a category A in terms of response and recovery (see *Reassessing the risk from an office fire*). We now have what was once historically a green risk hidden by a framework now escalated to a far more accurate and realistic position from a business-resilience perspective.

### Controls assurance

By having an appropriate rating structure in place, we can now consider controls assurance. This is the natural evolution and progression of risk reporting. One key challenge for organisations' executive teams and boards is

represents the time until impact. It assesses how quickly an organisation needs to respond in minutes, hours, days or weeks if a particular risk materialises. For example, the inability to recruit or retain key staff can impact an organisation immediately as you do not have the people you need whereas the inability to identify and maximise new business opportunities does not impact

the organisation today but will in future when the income and the benefits of relating to those opportunities fail to materialise.

V2 represents recovery time – the estimated time it would take for the organisation to be in a pre-loss position. Would it be one hour, one day, one week or one year? This recovery time influences the significance the risk could have on the organisation,

**“ With multiplication models, our risk management framework and the scoring methodology has become one of our biggest risks**

## OVERALL ASSURANCE LEVELS EXAMPLE DESCRIPTIONS WITH SUGGESTED ASSURANCE REVIEW FREQUENCY



HIGH	MEDIUM +	MEDIUM -	LIMITED
Controls are suitably designed, being consistently applied and are effective in practice	Some issues identified that if not addressed, could increase the likelihood of the risk materialising	Some assurances in place or controls are maturing so effectiveness cannot be fully assessed but should improve	Assurance indicates poor effectiveness of controls

Risk Scores	Overall Risk Rating	Review
20 - 25	<b>A</b>	Monthly
15 - 19	<b>B</b>	Quarterly
11 - 14	<b>C</b>	Every 3-6 Months
7 - 10	<b>D</b>	Every 6-9 Months
1 - 6	<b>E</b>	Every 12 Months

“ One key challenge for organisations’ executive teams and boards is whether they are focusing on the right risks in the right way

whether they are focusing on the right risks in the right way. If we shift the conversation to the level of assurance, the focus of reporting may change (see *Overall assurance levels example descriptions with suggested assurance review frequency*). We can map the risks onto the levels of risk assurance provided by the first, second and third lines of defence. In that way, we can adapt risk reports so that executive and the board can understand risks and order them by assurance level.

Organisations can identify weaknesses in the control framework. Also, the assurances are not necessarily risk management activities. This is good governance because the UK Corporate Governance Code makes it incumbent on the board to ensure the continuing effectiveness of the internal control framework. This is using risk management and resilience as a driving force behind positive business improvement.

We have learnt from the global pandemic that an over-reliance on potentially flawed risk scores may have contributed to its spread. Given the last global pandemic

## MULTI-ASPECT ASSESSMENT MODEL

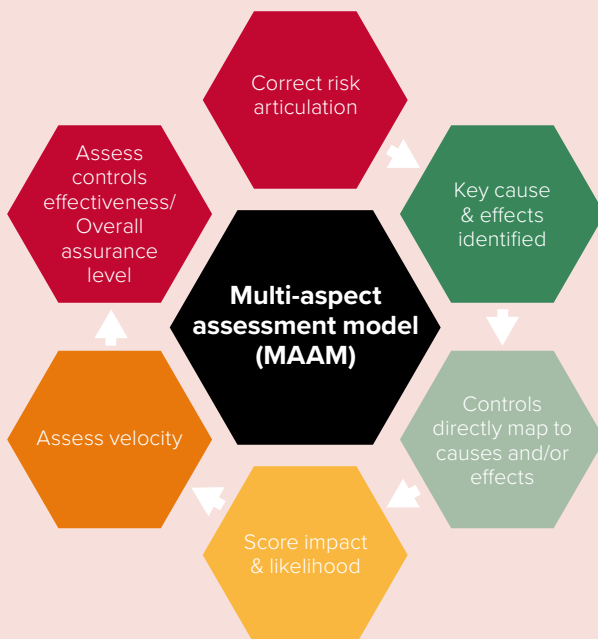




Image credit: Marc Olivier / Unsplash.com


**“ The UK Corporate Governance Code makes it incumbent on the board to ensure the continuing effectiveness of the internal control framework**


**KEY QUESTIONS FOR RISK MANAGERS**

- Do you identify and articulate the right risks, or are they more continuing issues and outcomes, rather than actual risks?
- Do you identify and articulate the key cause and effect of your risks?
- Do you map your key controls directly to a cause and/or an effect?
- Do you genuinely have the right approach to risk scoring that ensures accuracy and consistency across the organisation?
- Do you assess how quickly the organisation would need to respond should the risk materialise, and how long it would take before a pre-loss position returned?
- Do you identify the sources of controls assurance to determine a level of risk confidence (overall assurance)?
- Do you provide the board or executive with high level and/or key risk reports containing the above?

**If you answered “no” to the above, it’s possible that your organisation is focusing on the wrong risks.**

was 1918, the likelihood of another prior to 2019 would have been seen as rare but catastrophic and so would be scored as a low risk. Factoring in the response and recovery time, this risk had a low level of assurance that the public and government were prepared, and therefore should have been a priority. Applying a multi-aspect assessment of the risk would have had an entirely different outcome. The MAAM (see *Multi-aspect assessment model*) combines both the risk-scoring methodologies and an overall assurance level that the risk mitigations are appropriate and consistently applied. By plotting these two positions we can assess the risk prioritisation and ultimate threat level.

And by changing the narrative of risks, we see them in a different light. I believe that incorporating the MAAM framework will transform the way we manage risk. It accurately rates risks by their significance but, more importantly, provides confidence that the right risks are being managed in the right way. 

** Richard Mackie, CFIRM, is associate director at RSM and former chair of IRM’s Scottish Regional Interest Group.**

Delivered to  
meet your  
companies  
culture and  
work priorities



## In-House Training

We spend time with you to identify and assess your specific training needs to ensure we develop a course that meets all of your objectives.



Scan me!






[www.theirm.org](http://www.theirm.org) | Tel: +44 (0)7469 353441 | Email: [joanna.kraska@theirm.org](mailto:joanna.kraska@theirm.org)

**irm**

## 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](http://www.cammsgroup.com).

 Daniel Kandola  
 +44 (0) 161 711 0564  
 [sales@cammsgroup.com](mailto:sales@cammsgroup.com)  
 [www.cammsgroup.com](http://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](mailto:hello@1rs.io)  
 [1rs.io](http://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](mailto:ian.baker@riskhive.com)  
[doug.oldfield@riskhive.com](mailto:doug.oldfield@riskhive.com)  
 [www.riskhive.com](http://www.riskhive.com)  
 riskHive Software Services Ltd.  
Dilkush, Farlers End  
Bristol, BS48 4PG

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

## 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 holistic 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](http://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

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

# Riddle of the sands

Keeping the internet on in Egypt

**W**hen the container ship Ever Given became lodged in the Suez Canal, it was a major blow for the global logistics industry. One of the largest container ships in the world, it lost the ability to steer properly in high winds and a dust storm and then snagged and stuck on the bottom of the canal. Ever Given squatted there for six days as around 200 ships got into the growing queue of delayed vessels. The aftermath of delayed deliveries and disrupted supply chains continued for months.



**“ Digital connectivity across the European Union remains extremely vulnerable to outages in Egypt**

**Trade winds**

It was also, let’s face it, a bit embarrassing. Ships nipping through the Suez Canal between Asia and Europe save about 9,000 kilometres of travel compared with going around the bottom of Africa. That is the reason the site is one of the busiest shipping routes in the world. So the idea that a few gusts of wind could bring all of that global trade to a standstill so easily is an unwelcome reminder that certain locations are of fundamental strategic importance to many organisations.

It just so happens that Egypt is a global choke point for the internet too. In June last year, a 25,000-kilometre internet cable that winds from Asia through Africa and on to Europe and that pops up on land near the Suez Canal was snipped. The internet went off for about seven million people. That included about 90

per cent of Ethiopians and, at the other extreme, a police station in Liverpool in the UK that could not access its Facebook group. The repair was done quickly, but largely because the segment was above ground and not in the water.

**Spaghetti eastern**

A map of the spaghetti of the world’s internet cables shows why Egypt is such a crucial node in the network. Some experts speaking with Wired magazine described the place as a single point of failure for the internet last year. That may be pushing it a bit, but when the internet was affected in the June incident, another network experienced failure too – one that was supposed to be totally independent.

In fact, digital connectivity across the European Union remains extremely vulnerable to outages arising from any future snips and

cuts, according to a report to the European Parliament that was published last year. *Security threats to undersea communications cables and infrastructure – consequences for the EU*, outlines both how vulnerable such lines of communication are to accidental and deliberate threat and how little can be done in practice to mitigate those risks. The geopolitical situation in countries such as Syria, Iran, Iraq and Israel make alternatives difficult to both build and to rely on.

The Egyptian government is spending plenty of money shoring up the resilience of these sites. There are plans for a new fibre-optic cable route between the Red Sea and the Mediterranean located in the Suez Canal. Building in redundancy into our shared internet networks is critical. But quite simply because of the shape of the land and sea in that region, it is a problem that is here to stay for the foreseeable future. 🌐

**Develop the  
skills to treat  
financial  
services risk**



Scan me!

## **International Certificate in Financial Services Risk Management**

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](http://www.theirm.org) | Tel: +44 (0)20 7709 9808 | Email: [enquiries@theirm.org](mailto:enquiries@theirm.org)

**irm**

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

## **International Certificate in Enterprise Risk Management**



Scan me!

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](http://www.theirm.org) | Tel: +44 (0)20 7709 9808 | Email: [enquiries@theirm.org](mailto:enquiries@theirm.org)

**irm**