

# Enterprise Risk

Autumn 2019 / [www.enterpriseriskmag.com](http://www.enterpriseriskmag.com)

The official magazine of the Institute of Risk Management

---

**North American focus – Stepping across the pond:** IRM's state-side initiatives / **Down to earth:** lessons from NASA / **Navigating chaos:** holistic risk management | **Spotlight on slavery:** UK laws updated / **Faster business cycles:** agile




**Creating the right vibe:** John Scott, head of security education at the Bank of England

ONE-DAY INTENSIVE FORUM WITH DAVID TATTAM

# Enterprise Risk Management - The Six Essentials

**23 September 2019**, 08:30 am - 5:30 pm  
Pewterers' Hall, Oat Lane, London EC2V 7DE



Only £95.00 +  
VAT per seat\*

**Get a solid foundation with this one-day intensive forum covering:**

- |                                      |                            |
|--------------------------------------|----------------------------|
| 1. Risk Taxonomies and Risk Appetite | 4. Controls Assurance      |
| 2. Risk Assessment                   | 5. Operational Resilience  |
| 3. Risk Metrics                      | 6. Reporting and Analytics |

**Register now:**

[info.protechtgroup.com/erm-six-essentials](http://info.protechtgroup.com/erm-six-essentials)

\* Refreshments, lunch and networking drinks included

### 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 © 2019 Institute of Risk  
Management. All rights reserved.  
Reproduction without written permission  
is strictly forbidden. The views of outside  
contributors are not necessarily the views  
of IRM, its editor or its staff.



Developing risk professionals



## A good cliché

**A**s an editor, I appreciate crisp, original writing. That is what contributors to this magazine – me included – aim to achieve, even though we inevitably have our wobbles. But I have been wondering recently, what is wrong with a good cliché?

The word cliché only appears in English around 1892, suggesting that attitudes to originality in writing have changed over the past hundred years or so. Initially, people used it to point out weather-worn phrases, such as *at the end of the day*, or *at this moment in time*. During the 20th century opportunities to slip into cliché spread to other commonplace things, including visual imagery, stock situations and ideas.

The word itself has origins in printing. From the 18th century onwards, stereotypes have been created of complete newspaper pages by locking columns of type, illustration plates and advertising plates together into a mould that could be used in a printing press. Cliché refers to the sound – a sharp click – that arises as the metal plates are stamped into a mould to make the stereotype block.



## The complaint against cliché has its origins in automation and mass production

The complaint against cliché has its origins in automation and mass production. A cliché is the unthinking reproduction of words, behaviour, models, systems and organisations. It is a phenomenon that digital reproduction accelerates. Cutting and pasting text, duplicating images and organisational models and charts almost without limit aids in the dissemination of cliché.

On the other hand, why reinvent the wheel – to use a well-worn phrase? Under the broader definition of cliché, professional standards, frameworks and qualifications all rely on such stereotypes developed over many years from experience. Understanding their origins and the purpose of such models can be an incredibly powerful way of getting to grips with real-world problems without having to start from first principles.

That is what I was thinking as I began to edit this issue of the magazine. Risk managers and their stakeholders have begun to realise that corporate governance models, cybersecurity systems, risk management processes and other business tools only really work if people do not treat them as automated ways of solving problems.

In other words, a good cliché is one that is not used in a clichéd way.

**Arthur Piper**

Editor



# 10<sup>th</sup> Risk Leaders

A Decade of  
Discovery & Disruption

14<sup>th</sup> November, Inmarsat, London

## Keynote Speakers



**Professor Daniel Ralph**

**Judge Business School, Cambridge University**

Risk management exemplars from the energy and consumer sectors



**Jim Winters**

**Managing Director, Global Fraud Management, Barclays**

Cyber fraud and the challenges it presents to a global organisation



**John Scott**

**Head of Security Education, Bank of England**

Changing behaviour to support cyber security



**Robert J Trent PhD**

**Professor of Supply Chain Management, Lehigh University**

How myopic financial strategies increase corporate risk



**Lakshmi Shyam-Sunder**

**Vice President and World Bank Group Chief Risk Officer**

Session title tbc

### Other speakers include:

- > Dr Andrew Coburn, Chief Scientist, Cambridge Centre for Risk Studies
- > Dan Tapsell, Contracts Manager, Broadgate Search
- > Karlene Agard, GradIRM, Aravun
- > Alex Deas, CMIRM, Network Rail
- > Jemma Boyce, GradIRM, London City Airport
- > Chris Hanlon, IRMCert, Monza Bank

View the full agenda and register your place at

[www.theirm.org/riskleaders2019](http://www.theirm.org/riskleaders2019)

Headline Sponsor



irm



10

## FEATURES

**10 Creating the right vibe**  
For John Scott, head of security education at the Bank of England, encouraging people to take action on cyber-risk involves ditching the fear factor and building a culture of proactive carefulness

**16 Stepping across the pond**  
In the first of three articles in our special North American focus, we look at how IRM is expanding its reach into the market

**18 Down to earth**  
While technology has become more complex since NASA's 1969 moon landing, risk managers need to keep their feet on the ground

**22 Navigating chaos**  
The only way to manage risk in a chaotic business world is to take a holistic approach that ties governance, risk management and compliance together across an entire enterprise

**28 Spotlight on slavery**  
A review of the UK's Modern Slavery Act is set to bring in more detailed reporting and public scrutiny

**31 Faster business cycles**  
The building blocks of agile risk management

## REGULARS

**07 IRM Viewpoint**  
Trouble in Australia's finance sector has put the spotlight on risk management

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

**32 Events**  
Enhance your knowledge and develop your professional network at IRM-related events across the country

**33 IRM Focus**  
Complexity is a reality in today's highly interconnected world. That is why IRM is creating a new Special Interest Group to better understand the phenomenon

**34 Directory**  
In need of insurance services, risk management software and solutions, or training – look no further than our listings

**38 Toffler**  
Risk managers are increasingly looking to case studies of past successes and failures to engage their stakeholders on risk. But history comes in many flavours



16



18



22



28

## Making opportunity knock

*Is the key risk indicator the harbinger of doom or opportunity?  
How to get the attention of the Board when risk fails to excite*

..... BY IAN BAKER

**T**he key risk indicator (KRI) has a generally bad reputation, even though it is probably the most valuable component of enterprise risk management (ERM) that no-one uses. But maybe it is the KRI's reverse twin, the key opportunity indicator (KOI), that we should be promoting because boards prefer opportunity to risk. Fact.

Risks will happen all by themselves and we spend much of our time planning for how to either prevent or control risk and working out what to do if one happens. But opportunities do not work this way – they do not just “happen” like risks do – they need to be actively managed to achieve a successful outcome, and this is where we can leverage risk techniques and processes to help the organisation get ahead.

### Leveraging risk techniques

Imagine a cloud-based software service that monitors real-time, business-critical information to feed a dashboard of internal and external KRI statuses, tracking multiple live data feeds, such as performance metrics, financial rates, sales, income, share prices, commodity values, weather, tweets or trends or even keywords relating to relevant information provided by news sites or social media.

Individual data feeds can be homogenised to allow thresholds to be described so that alerts, alarms and actions can be initiated when the data feed reaches certain predetermined conditions or breaches a pre-set threshold. These KRI states can be aggregated into logical circumstances where multiple conditions syndicate to trigger a response or alert, such as a combination of performance, fiscal and political conditions that may indicate that a risk condition is about to occur, if not already occurring, as tolerance or detection thresholds are exceeded.

These KRI output states can be linked directly to an ERM system as inputs to risk causes that can automatically trigger risk or issue occurrence detection. Automated risk responses can be emailed with business continuity

protocols attached, and risk warnings can be immediately distributed to other corporate data dashboards.


### Aligning the stars


But now imagine that the signal sent to the board's dashboard is not one of doom, but one of opportunity: “The stars are aligned: strike now! Buy that company! Enter that market!”



**Imagine that the signal sent to the board's dashboard is not one of doom, but one of opportunity**

By reversing the polarity of KRI monitoring, a capability can be configured to monitor for optimal opportunistic states, providing a capability for the organisation to identify and take advantage of future optimal situations where key enablers such as financial rates, market changes, political or socio-economic states, competitor blunders or unnoticed holistic conditions prevail.

How many times have we been presented with an opportunity to buy that rare object or searched for the perfect house within an impossible timeframe and said, “I wish I'd known earlier” – and because we haven't planned or budgeted for the opportunity when it arose, we were unable to take advantage? We get alerts every day on pricing and availability for all sorts of consumer goods, so why don't we do the same for our businesses? KROs can give you the edge and get the attention of the board. Who says risk can't add value? 

 Ian Baker is the Founding Director and Futurologist of riskHive Ltd. riskHive has been developing this concept into their existing KRI tool and it complements their existing ERM system. Contact: [www.riskhive.com](http://www.riskhive.com)



## Refocusing on risk



*Trouble in Australia's finance sector has put the spotlight on risk management*

**T**he banking sector in Australia has been going through a rocky time. The Royal Commission into misconduct into the banking, superannuation and financial services industry reported in February this year and follows the *Prudential Inquiry into the Commonwealth Bank of Australia* in 2018. The catalogue of errors made across the industry makes for uncomfortable reading.

IRM's partner organisation, the Institute of Operational Risk, is holding an event in September to explore the lessons that can be learnt from these hefty tomes (see below for details). In particular, the session will examine the standard these inquiries have set for the next level in financial services risk management.

One of the disturbing things that emerged from the investigation into the Commonwealth Bank of Australia (CBA) was that governance and risk mechanisms appeared to be in place. Despite this it was fined \$700 million plus legal fees for breaches of anti-money laundering and counter-terrorism financing laws – the largest civil penalty paid in the country's corporate history.

The CBA's current chief executive, Matt Comyn, acknowledged the seriousness of the breaches and said the bank has so far spent around \$400 million trying to fix the problems with technology and people, according to ABC News. "While not deliberate, we fully appreciate the seriousness of the mistakes we made," he said in a statement.

In the regime that was in place prior to the appointment of a new chair in 2017, the tone at the top did not encourage good risk management, according to the Prudential Inquiry. The mechanisms for setting that tone are generally established both through internal and external communications and it is demonstrated through the actions the board takes to manage risk effectively. "Importantly, it is also demonstrated through the rigour applied to monitoring and demanding mitigation of key risks and closure of control weaknesses," it said.

Understandably, the bank wanted to achieve a consistent message about its strategy, policies and values. Instead of these matters being mainly driven by the board


and its committees, people historically deferred to the chief executive officer. While this distinction could be described as subtle, it had far-reaching consequences.

"For that reason, the board did not have a highly visible presence, and the lack of apparent urgency by the board and its committees in dealing with non-financial risks may have imparted a tone of inaction to the rest of the organisation," said the report. "This has likely deprioritised the importance of maintaining rigorous risk management practices in non-financial risks as compared to the pursuit of financial performance and other risk objectives."



**Lack of apparent urgency by the board and its committees in dealing with non-financial risks may have imparted a tone of inaction to the rest of the organisation**

The risk committee itself tended to focus mainly on financial risks, rather than those of an operational, compliance or non-financial nature, the report found. Control weaknesses were often identified, but there was less attention paid to how and when they were closed: "Effectively, monitoring the timely closure of issues affecting risk management was not the primary responsibility of any gatekeeper committee."

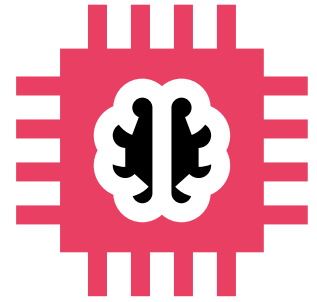
It is hard not to conclude that some at the bank believed that because the structures of corporate governance appeared to be in place, effective risk management and mitigation would follow. Sadly, it did not. 



Carolyn Williams is IRM's director of corporate relations. To register for the event, go to: [bit.ly/2lZDDiY](https://bit.ly/2lZDDiY)

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

## Artificial intelligence to add trillions in value



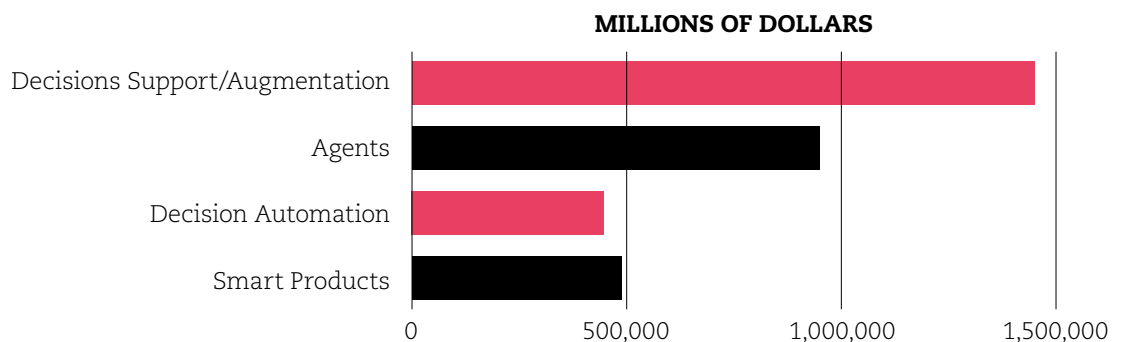
In 2021, artificial intelligence augmentation will:



**CREATE**  
**\$2.9 trillion**  
of business value



**CREATE**  
**6.2 billion**  
hours of worker productivity globally



Source: Gartner August 2019

## Global enforcement on human trafficking

**Prosecutions fall while convictions rise**



**Prosecutions**



**Convictions**



**Victims Identified**



**2018**  
**2017**

11,096  
17,471

7,481  
7,135

85,613  
96,960








Source: Department of State, USA Trafficking in persons report 2019. \*Figures are reported estimates.



## Uninsurable risks dominate global threats

Accelerated rates of change jump in importance for corporations



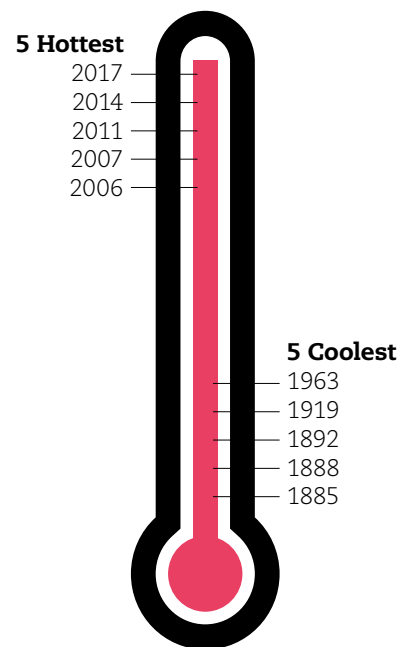
CURRENT TOP SEVEN RISKS		2019	2017	STATUS
	Economic slowdown / slow recovery	1	2	●
	Damage to reputation / brand	2	1	●
	Accelerated rates of change in market factors	3	38	●
	Business interruption	4	8	○
	Increasing competition	5	3	●
	Cyber attacks / data breach	6	5	●
	Commodity price risk	7	11	●

● Uninsurable ● Partly insurable ○ Insurable

Source: Aon, Global risk management survey 2019

## Britain warms up with climate change

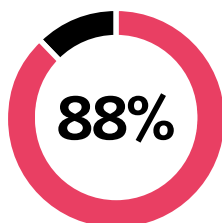
Hottest and coolest years show warming country



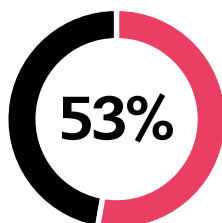
Source: The state of the UK climate, the Met Office

## South Africa's ERM maturity

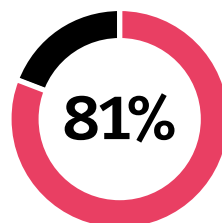
Most risk professionals report high levels of ERM integration and strategic influence



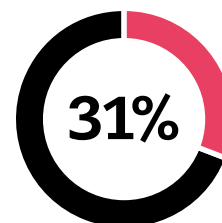
Fully or partially integrated ERM programs in operations



ERM is being used to inform and influence strategy



Risk executives reporting quarterly to their board (committee)



ERM's implementation was ordered by the board

Source: RIMS, the risk management society®, and IRMSA, The Institute of Risk Management South Africa: 2019 Enterprise risk management benchmark survey: South Africa

# Creating the right vibe

For John Scott, head of security education at the Bank of England, encouraging people to take action on cyber-risk involves ditching the fear factor and building a culture of proactive carefulness

..... BY ARTHUR PIPER

**I**n October, the Bank of England (BoE) is planning to roll out a three-year programme aimed at taking its cybersecurity defences to the next level. The launch will coincide with National Cybersecurity Awareness month, where BoE teams up with organisations to raise the profile of the latest in cyber-defence nationally.

John Scott, head of security education at BoE, is particularly excited to be talking publicly about his risk-based approach to the issue, which focuses on identifying the most important cyber-risks at BoE and providing staff with the positive behaviours to help mitigate those threats. His roadshow will include a session at IRM's Risk Leaders Conference this November.

Scott's approach is built on two interrelated trends that he believes are hampering organisations' attempts to deal with cyber-risk. First, the rapidly growing range of devices that connect to the internet – for everything from online banking to home security – has added layers of complexity to cybersecurity systems. This increasing technological entanglement makes it more likely that risks will crystallise because potential security weaknesses multiply.

Second, bewildering levels of interconnectedness can lead people to switch off because they feel less in control. He cites Alvin Toffler's influential 1970 book



**Fear causes people to magnify risk and leads to disengagement**  
.....



*Future shock*, which argues that when change accelerates to a certain level, people experience a state of mind equivalent to the kind of paralysing jolt one can feel when dropped into a completely different culture. When the environment feels out of control, it becomes more difficult to assess risk or to believe personal actions can make a difference.

At ground level, he likens it to the situation in which more people are afraid of flying than of driving a car, when the statistics show the former is safer. Fear causes people to magnify risk and leads to disengagement. "In my work, in trying to change behaviour and culture, we need that engagement," he says. "We need people to feel that they can do something to help secure themselves and that it isn't out of their hands and they're not just trapped on an aeroplane, as it were."

## Not understood

Those looking for easy answers are likely to be disappointed. Risk and risk transfer relating to online life is relatively poorly understood. While many risks can be covered by well-established insurance policies, for example, insurers do not have the depth of data in cyber-risk to devise policies that can provide the same certainty. Legal disputes about what specific policies cover are commonplace, and it will take decades for insurers to build the data that reliable policies can be created from.

For Scott these issues contribute to the underlying fears people have about the cyber-landscape and how businesses can subconsciously put out messages that ultimately make people too afraid to act. "Dr Jessica Barker [a cyber-consultant

with a background in sociology] has gone into companies where people have almost been paralysed with fear because they're so scared of doing the wrong thing – opening a link or clicking an attachment that could bring the company down – that they're actually not doing anything. And the standard advice we give is 'don't click on links that you don't expect,'" he says.

Such blanket bans aimed at thwarting so-called phishing attacks are unrealistic across an entire organisation, he believes. Press officers, sales executives, journalists and many other people have jobs whose daily work is to click on links from people they may not know. The answer is to encourage staff to be careful, rather than fearful. Scott's job is to help create a culture that makes this psychological shift possible.



**Press officers, sales executives, journalists and many other people have jobs whose daily work is to click on links from people they may not know**

## Culture

While there are many ways of defining culture, for Scott three stand out. The first two – “the way we do things here” and “the thing you do when nobody’s watching” – prise open the difference between what is generally considered acceptable behaviour and the kind of behaviours that are dictated by company policy. The two conflict when people find workarounds for official policies in order to get something done, for instance. Scott rules out the idea that you can control culture because of these often-subtle shadings of behaviour.

Work by Gerry Johnson and Kevan Scholes on a concept called Cultural Web Analysis is the one that resonates best with him. Simply put, they argue that you cannot directly drive culture, but you can analyse and influence the six factors that do: stories, symbols, power structures, organisational structures, control systems, and rituals and

routines. He finds the symbols (preferring the term semiotics) and the stories particularly compelling facets of the model, and they are ones that he applies in his work as an educator and trainer at BoE.

In fact, when Scott and his team started their project to build awareness about cybersecurity within the Bank, the building itself proved to be a symbolic stumbling block. The Threadneedle Street property was originally designed and built by the architect George Sampson in 1734 in the classical, or Palladian, style – but was substantially expanded to fill the same 3.5-acre site in the 1920s and 1930s by Sir Herbert Baker. The modern bank bullies the surrounding landscape with huge windowless walls, resembling something of a cross between a Palladian castle and a Soviet-style government block. Security is tight on the doors, and two-factor computer authentication was already in place back in 2013 when the staff mainly moved to having laptops rather than desktops.





## The next step in cultural change is when people start looking for other things that they can do that aren't in the policies

---

but Scott sees signs that the next phase of the Bank's cultural change programme, which started in 2018, is beginning to bear fruit. Some of BoE's departments have put cybersecurity into their team's performance review systems – which means they could be rewarded if they hit those targets. He sees more and more people spontaneously behaving with a security mindset.

"The next step in cultural change is when people start looking for other things that they can do that aren't in the policies, that aren't in the demands placed on them," he says. It is part of Scott's role to spread those stories around the Bank and put security innovators in different departments in touch with each other. Eventually he believes his two-person team will play more of a facilitating role.

### Risk behaviours

---

Working with risk teams across the business has been a key part of the exercise. While he initially focused on areas where everyone in the Bank could make a difference – such as not sharing passwords – now risk maturity has increased, the task is to tie specific, constructive behaviours to each major risk. A first step involved working with the risk management team to understand the risk taxonomy, their assessment and scoring methodologies. But when they analysed how many behaviours were associated with those risk controls, there were simply too many.

"We found that we were giving out 65 bits of advice to staff in terms of security behaviours, and that's ridiculous," he says. "You can't expect anybody who's also got a day job to remember 65 different things,

especially because some of the risks were far less likely to happen." It was not that lower-priority risks did not need to be managed, but they clouded the behaviour needed to deal with the priority risks.

"Now we're talking to our risk division and making sure that we're always looking at their risk assessments and making sure the behaviours we prioritise are the ones that address the biggest risks," he says. Having the backing of the risk management team provides Scott with the knowledge and authority to say to management that they are focusing on the right risks. But it also opens the door to more nuanced risk discussions and helps those conversations revolve less around "yes" or "no" behaviours and towards something that is more likely to help tackle the complexity of the cyber-risks BoE faces.

It has also enabled the Bank to stop imposing bank-wide risk mitigation behaviours on all departments equally. Scott can dig deeper into risk in a specific part of the organisation and adapt the security behaviours as necessary. In addition, those discussions may unearth problems that have developed with the suggested behaviours so that the whole feedback process on risk becomes more dynamic.

"Managers don't feel that they're getting a generic message, and they feel that actually we're addressing their concerns, because they've already fed into that risk process," he says. Sitting physically next to the cyber-risk team has helped build up rapport so that recommendations for managers to come and talk to Scott are commonplace. That is effective but can be time-consuming. For example, he is currently speaking to about 300 people in the Prudential Regulation Authority division in groups of up to eight people at a time. "That's a lot of work, but it's a very fruitful way of addressing a risk that we've identified," he says.

### Supporting roles

---

This approach to influencing corporate culture needs to be supported through full-time roles, he says. He believes that if it were only a part of his role, it would most likely be sidelined by other tasks

Staff could not install software onto computers, and access to many social media sites was blocked by default. The building felt safe.

"There was a real challenge in trying to get people to understand that as good as we can get the defences, actually we're never going to get 100 per cent – but without saying 'there's nothing you can do about it'," he says. The first, three-year phase of his project was aimed at raising awareness both of the potential threat and, simultaneously, what practical steps staff could take if problems arose. The team's first tagline was "you are the first line of defence" because by the time an attack had penetrated the Bank's cyberwalls, it was incumbent upon staff to act carefully. Scott never put out a threat message, ran a seminar or gave a talk without providing practical steps of action that staff could take to help mitigate the risk. The key idea was to eventually move from awareness to behavioural change.

Change does not come quickly,



Above: Bank of England, London.

**“Managers don’t feel that they’re getting a generic message, and they feel that actually we’re addressing their concerns, because they’ve already fed into that risk process**

and responsibilities. Neither Scott nor his colleague have technical or security backgrounds – although both are fully up to date with current trends. In fact, in organisations with similar roles the evidence is that people with communications, education and human resources backgrounds are better placed to lead because they have strong interpersonal skills and can talk about security and risk at the right level for most people in the business.

Scott has worked in academia and charities for most of his life both as an IT trainer and in the 1990s as a webmaster when it was a relatively rare profession to pursue. He spent

six years as a staff and student IT trainer at UCL, and his softly spoken calm manner gives the impression of someone who can listen with patience and interest to questions he must have heard a thousand times. He has also spent years organising events that provide controlled environments for people to play out their fantasies – or simply have fun.

“Many years ago, I used to run live role-playing events at the weekends – such as JRR Tolkien re-enactments,” he says. When he moved to London in the early Noughties, he fell in with people who ran a nightclub and eventually ended up as their events manager. He ran cabaret nights at Soho’s famous, but sadly closed, Madame Jojo’s – but the time commitment needed to do it properly, and the lack of money that it generated, meant that it would never have been a viable career option even if Scott had wanted it to be.

The urge to create environments that affect the way that people behave runs through Scott’s psychology. “Whenever you put on an event, whenever you put on something that you want people to enjoy, you’re trying to manipulate emotions,” he says, “and I don’t mean that in a negative way. You can’t force someone to change their emotion, but you’re trying to create the circumstances that mentally puts them in a good place.”

He admits that view can seem cold and calculating, but it is a way of getting people engaged in something that they will either enjoy, or that will be good for them – or for the place in which they work. A nightclub, BoE – the places are widely different, but the approach is very similar. Creating a positive environment where people are not too stressed to enjoy the music, or too frightened to use their computers. Perhaps unsurprisingly, the *Lord of the Rings* character Scott most identified with was Samwise Gamgee. He was the hobbit who ultimately made it possible for the other main character – Frodo Baggins – to defeat the forces of evil. ☯

**John Scott will be speaking at IRM’s 10th Annual Risk Leaders Conference on November 14, 2019 – A decade of discovery and disruption. Book tickets at: [bit.ly/2lsgENi](http://bit.ly/2lsgENi)**



**HOW DO YOU KNOW YOU'RE COMPLIANT**  
IF YOU DON'T TEST YOUR CONTROLS?

**Symbiant<sup>®</sup>**

**IS THE ONLY SOLUTION**

to give you real time monitoring  
of your risk exposure and  
control assessments



Affordable Risk, Audit and Compliance Management Software

For more information and a free trial visit  
[www.symbiant.co.uk](http://www.symbiant.co.uk)

# Stepping across the pond

In the first of three articles in our special North American focus, we look at how IRM is expanding its reach into the market. In the second, US guest author Mike Lutomski shares his experiences of risk managing at NASA, and in the third US guru Michael Rasmussen extols the virtues of GRC

..... BY CAROLYN WILLIAMS

**W**hen IRM first launched its new Digital Risk Management Certificate last year, we were pleasantly surprised to see an unexpected number of enquiries and webpage visits

from the United States and Canada. Although IRM has had some active members in both these areas for many years, the number is very small in relation to the overall size and maturity of the market.

The interest in our innovative new Digital Risk Management Certificate indicates that there could be some interesting opportunities for IRM education in that region – we don't believe that there is an equivalent distance learning course of this level anywhere else. At the same time the enquiries coming into IRM from North America about qualifications and training are starting to rise.

The IRM Board's strategy to "internationalise and diversify" includes an objective to examine whether IRM can do more for the North American market. One historical obstacle to potential students has been the very small number of examination centres that IRM could offer in the US and Canada, meaning that students might have to travel long distances to take their exams. This has now changed, with IRM's new partnership with Pearson VUE providing hundreds of test centres across the region. Other



**There has been a sharper focus on managing enterprise risks in the US government, moving beyond financial risk controls to a broader approach looking at all types of risk**

.....







**IRM's intention will be to build presence and partnerships to raise the profile of the Institute as being a forward-looking, global, sector-independent and modern risk management educator**


US, focusing on the Eastern Seaboard region. Linda is a longstanding IRM technical specialist and has held senior risk positions with Zurich and with energy giant Exelon Corporation. Linda will be acting as the voice of IRM in the US and will be looking to arrange some suitable events and meetings.

## Collaborating

We are also collaborating with a US organisation to produce our next new certificate qualification on the very topical subject of supply chain risk management. We have established a study materials partnership with the Supply Chain Risk Management Consortium, based at Lehigh University in Pennsylvania. The consortium includes many major US companies and also has strong links with the supply chain and logistics community. Professor Bob Trent, one of our collaborators, will be speaking at this November's Risk Leaders conference.

Finally, IRM's first training course tailored for the North American market is being launched in Canada by our partners, Baldwin Global. This is a three-day course in Enterprise Risk Management for leaders, influencers and decision-makers covering strategy, culture, emerging risk and digital disruption. We expect this to be rolled out across the region in 2020.

Word of mouth is the best advertisement for promoting what IRM stands for. We would be pleased to hear from anyone with further advice or ideas on building this special relationship. ☺

 **Carolyn Williams is IRM's director of corporate relations.**

administrative issues are also being addressed, with work underway to look at matters like multi-currency pricing and payment – which is not as straightforward as it sounds.

Even when IRM is fully open for business to US students, there still remains the challenge of raising profile and explaining who we are, what we do and what an IRM qualification means. ERM is generally accepted and practised in commercial organisations across the US, which is of course the home of the COSO ERM guidance (well known to generations of IRM students).

## Sharper focus

More recently, there has been a sharper focus on managing enterprise risks in the US government, moving beyond financial risk controls to a broader approach looking at all types of risk. According to a recent survey from Guidehouse and the

Association for Federal Enterprise Risk Management (*Federal enterprise risk management, 2018 survey results*), 58 per cent of federal agencies have created enterprise risk programmes within the past three years. The same survey also found that less than 10 per cent had a well-understood risk appetite statement that is integrated into strategy and decision-making. In addition, it found that there was limited awareness of any qualification or certification that might assist in building ERM competency and almost zero awareness of any originating outside the US.

IRM's intention, therefore, will be to build presence and partnerships to raise the profile of the Institute as being a forward-looking, global, sector-independent and modern risk management educator.

Our current initiatives include the appointment of Linda Conrad as the first IRM global ambassador for the

# Down to earth

While technology has become more complex since NASA's 1969 moon landing, risk managers need to keep their feet on the ground

..... BY MICHAEL LUTOMSKI



**M**any people struggle in setting up or running a risk management process for their enterprise. They waste time on trying to nail down the fine details of the database, how to link other enterprise data to the risk database, how not to duplicate data from other processes – and they spend weeks talking to people about how processes “will be” implemented. They talk about how they will set up a review panel, who will attend, who is required to attend and on and on.

What people forget is that fundamentally risk management is a communication system. It's not rocket science – pun intended. Over the years in organisations large and small, government and private, I have been exposed to all sorts of risk management processes and databases. I will share some of my lessons on what is essential and what is optional in a risk process and how to continuously evolve the process commensurate with the maturity and size of the business.

## Stepping back

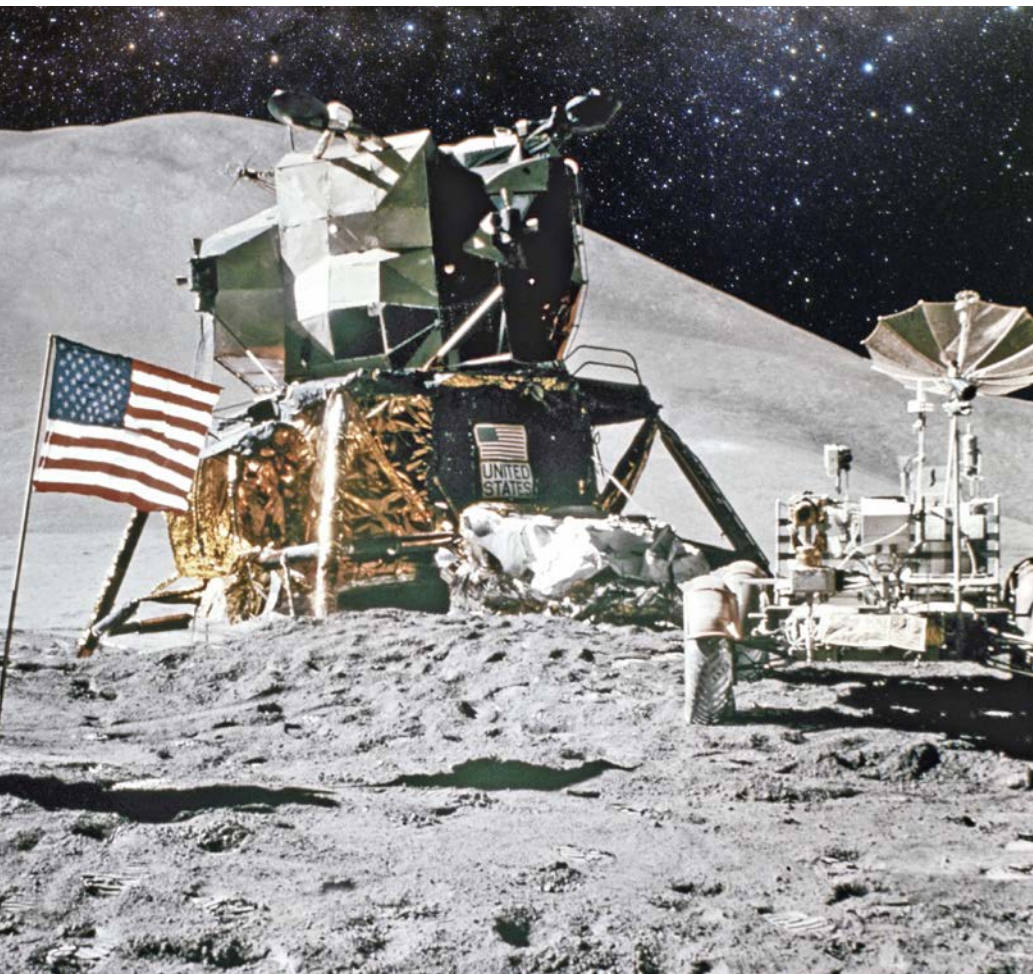
.....  
The first thing I like to do is to step back and consider why we are all doing risk management and what a risk management system is. I like to joke about how did NASA put a man on the moon in 1969 without a risk management process and risk register? How did they



**What people forget is that fundamentally risk management is a communication system**

.....





prioritise their risks and know where to spend money? How did they identify risks? How did they determine if their risk list was comprehensive? Now that the 50th anniversary of the first of six moon landings is behind us, it is a good time to reflect on the issues that these questions raise for us today.

In the engineering world, as in almost every world, you do not have meetings just to meet. You have them to discuss obstacles, issues and problems that are occurring in your business, and to propose solutions, forward-action plans, schedules and so on. Risk management is what is done at all levels of an organisation when the team is seeking to accomplish any significant goals – whether meeting next quarter's sales targets or putting footprints on the moon. That includes identifying threats to those goals, finding ways to counteract them and finding ways to increase chances of success.

What managers define, and

sometimes mandate and require, is just a more systematic process of recording these risks in a clear and concise way. Trying to be more thorough in identifying risks, writing down how to mitigate or avoid the risks and frequently writing down who is doing what, and when they are doing it – this is what we all think of and call risk management. It is what we all have been doing and will continue to do in our personal lives and in business.

### Keeping it simple

The KISS principle – Keep it simple Stanley – is always relevant. I find that sometimes risk advocates and risk consultants can over-complicate risk management for organisations that are just not ready for a high level of sophistication. It is important to build a house on a solid foundation and that often means keeping it simple.

It is extremely important when starting up a risk system,

**“ If management are not even using the risk process in their decision-making, then it is not really important how well risks are analysed**





I have always advocated for the direct participation of all stakeholders in a firm, and not to make ‘shadow’ or redundant hierarchies to manage risk



or rebuilding it, or reinvigorating a risk process, to start with the fundamentals or first principles. For example, if management are not even using the risk process in their decision-making, then it is not really important how well risks are analysed, how the information is being presented and if risk schedules are being integrated together.

Start with communication. Find out if anyone is listening and what the right ways are to get them to listen. Dig deeper. Why are they not listening? Did someone, or a burdensome process, turn them off years ago before they became the decision-maker?

Sometimes, you may have to start from scratch and explain why you have a risk process and what its purpose is to get some type of buy-in from the group of decision-makers you are working with before you can move forward. Start at the level your audience is at. Do not speak as though your audience has the same level of understanding of risk and processes as you have. You may have complex and very dense data and metrics displayed on charts about the risks, but no

matter how beautiful the charts if few to anyone understands it, you are moving your objectives backwards.

We can all be tempted to try to show off our levels of competency, demonstrate the value we can bring and explain in detail the rationale of our department. Save that for another opportunity.

### One step at a time

You cannot fix all the problems in your organisation at once. Educate people on what you’re doing and why. Show value, even if it is small value at the beginning. Then step up the process when your customers – the decision-makers, executive staff, your stakeholders – are ready.

In my experience when a new manager, chief executive officer or other decision-maker is appointed, it is a mistake to just keep the gears turning and assume they have buy-in and believe in the established process – no matter where they came from, or how mature and valuable the process was yesterday.

This is true in industries such as financial services where risk management is required. As we

like to repeat over and over again, risk management is not about compliance. If it is seen only as a compliance function, it can easily be seen by management as a “tax” the business has to pay to operate in that market. Where risk managers need to do compliance work, they should make it relevant and value-added to their organisation. No matter how small and maybe even feeble that task may feel at the beginning, it will pay dividends in the long run as people begin to understand what risk management can deliver.

### Participation

One of the keys to a successful risk process is participation. I have emphasised the participation of senior management, but it takes a village, or at least the key members of a village, to make it work. I have seen too many times that one person, or a small part of the organisation off to the side, try to implement risk management. This is flawed, misleading or dangerous in my line of work. Every department needs some type of direct involvement. How can a risk manager working in relative



isolation identify all the risks to the avionics of a vehicle, for instance, better than the avionics department? Even more critical is, who can mitigate the risks, technical risks, schedule risks, cost risks better than the department that is responsible for that function or service or hardware?

I have always advocated for the direct participation of all stakeholders in a firm, and not to make “shadow” or redundant hierarchies to manage risk. The established managers in the organisation are responsible for managing the risk and owning the risk for their products and services. Any outsider trying to peer in from the outside and identify and manage risk will be at a huge disadvantage and furthermore have little credibility.

The people or managers that are responsible have to play along at some point in the process to make it a success. They can delegate certain functions, or heavy lifting, but they have to make the decisions of prioritisation, where to spend resources, when and where to communicate large risks up the chain to more senior managers that can help them avoid or mitigate a risk. They cannot delegate their responsibility down to a staff position that has no responsibility or authority.

## Risk tolerance


Knowing the risk tolerance and capability of the organisation or department is key. Without this knowledge, the risk manager cannot know what risks should be elevated and what risks can be solved on the ground. Even an intern should know what to do if the stapler runs out of staples, and what to do when they smell a gas leak. These are exaggerated risks of very different likelihoods and consequences, but they should know what risk they can accept and what risks they should act on, which to kick up the chain (preferably with great urgency when needed).

Risk managers should develop at least some loose and common knowledge of triggers or levels of acceptable risk at all basic levels in an organisation. Some of these will be obvious triggers to hit the action button, some will need defining and some will be subjective triggers where you are just not comfortable. Many corporations today are defining risk appetite statements that will cover these areas. While this is a slightly different topic, it does define boundaries for taking risk and it gives guidance on what may be well outside a company's


risk tolerance or capabilities.

Risk managers need to have a strategy for improving or building the risk management process to get it where you want it to be, where management wants it to be or where it is required to be. Whether it is established and sophisticated, or you are starting from scratch, every process has room for improvement. You cannot force people into it, or build it in a day, or a week or even a month. You have to sell it, show value, build trust that you are not just a risk fanatic who wants his or her process to be the most important and get the most attention. You have to pick your battles one by one.

If in doubt, make it simple and easy to understand, easy to participate with low or no barriers to participate. Your goal should be to have your process strengthen communication, help inform decision-making, help managers and leaders make better decisions. Building a quality and resilient risk process, is well ... a process. It takes patience and time to get it functional and valuable. 📧

 **Michael Lutomski is a human spaceflight and risk expert. He worked at NASA for 27 years, including ten years as International Space Station risk manager.**



 **Even an intern should know what to do if the stapler runs out of staples, and what to do when they smell a gas leak**

# Navigating chaos

The only way to manage risk in a chaotic business world is to take a holistic approach that ties governance, risk management and compliance together across an entire enterprise

..... BY MICHAEL RASMUSSEN



**T**he physicist Fritjof Capra once said, “The more we study the major problems of our time, the more we come to realise that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.” Capra was making the point that biological ecosystems are complex, interconnected and require a holistic contextual awareness of the intricacy in interconnectedness as an integrated whole – rather than a dissociated collection of systems and parts. Change in one area has cascading effects that impact the entire ecosystem.

This interconnectedness and a demand for a 360° contextual awareness apply to the world of business. Organisations need to see the intricate relationships of objectives, risks and boundaries of the enterprise. Business operates in a world of chaos. In chaos theory, for instance, the “butterfly effect” means that something as simple as the flutter of a butterfly’s wings in the Netherlands could create tiny changes in the atmosphere that have a cascading and growing force that ultimately impacts the development and path of a hurricane in the Gulf of Mexico. A small event develops into what ends up being a significant issue.

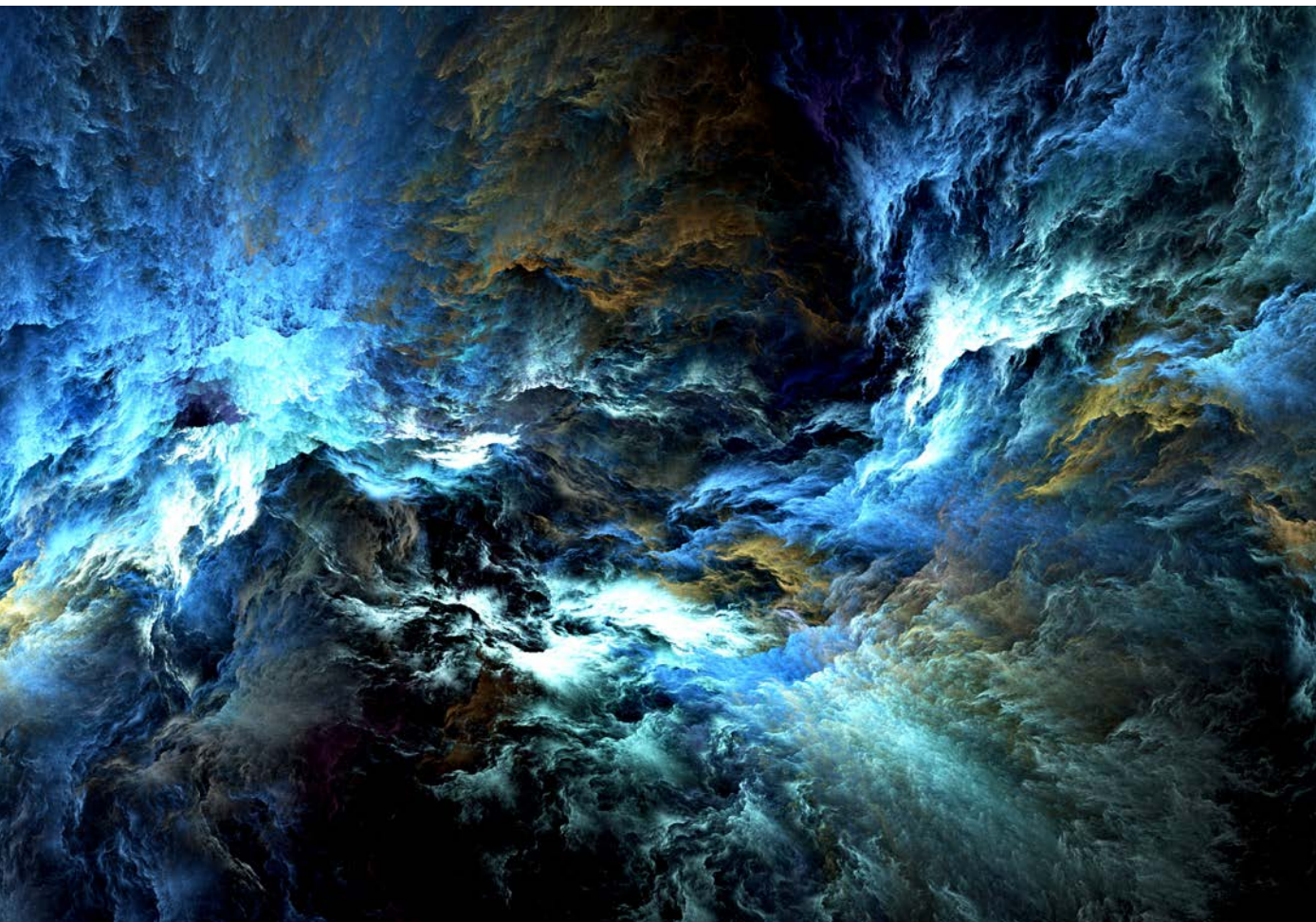
Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalisation, distributed operations, competitive



**Gone are the years of simplicity in business operations**

.....





velocity, technology and business data encumbers organisations of all sizes. Keeping business strategy, performance, uncertainty, complexity and change in sync is a significant challenge for boards and executives, as well as management professionals throughout all levels of the business. This challenge is even greater when risk management is buried in the depths of departments and approached from a compliance or audit angle, and not as an integrated discipline of decision-making that has a symbiotic relationship on performance and strategy. Organisations need to understand how to monitor risk-taking, measure whether the associated risks taken are the right risks and review whether risks are effectively managed.

## Holistic

Today's organisations have to have holistic visibility and 360° contextual awareness of risk in the context of

objectives across the enterprise. The complexity of business and intricacy, and interconnectedness of risk and objectives, requires that the organisation implement a governance, risk management and compliance (GRC) management strategy. GRC, by official definition in the GRC Capability Model published by OCEG, is: "a capability to reliably achieve objectives [governance], while addressing uncertainty [risk management], and act with integrity [compliance]."

This definition of GRC provides the framework for what the think tank OCEG calls principled performance. There is a natural flow to the GRC acronym. *Governance* sets the context by defining the objectives of the organisation. These can be entity-level objectives, so division-, department-, process-, project- or even asset-level objectives. It is the evaluation and establishment of objectives that provides the context for risk management. Without



**It takes all three elements of governance, risk management and compliance working together to provide stability and balance for the organisation**



## BENEFITS OF GRC

Organisations striving to improve their GRC management capability and maturity in their organisation will find they are more:

- **Aware.** They have a finger on the pulse of the business and watch for a change in the internal and external environments that introduce risk to objectives. Key to this is the ability to turn data into information that can be, and is, analysed and shareable in every relevant direction.
- **Aligned.** They align performance, risk management and compliance to support and inform business objectives. This requires continuously aligning objectives and operations of the integrated GRC capability to those of the entity, and to give strategic consideration to information from the GRC management capability to affect appropriate change.
- **Responsive.** Organisations cannot react to something they do not sense. Mature GRC management is focused on gaining greater awareness and understanding of information that drives decisions and actions, improves transparency, but also quickly cuts through the morass of data to uncover what an organisation needs to know to make the right decisions.
- **Agile.** Stakeholders desire the organisation to be more than fast; they require it to be nimble. Being fast isn't helpful if the organisation is headed in the wrong direction. GRC enables decisions and actions that are quick, coordinated and well thought out. Agility allows an entity to use GRC to its advantage, grasp strategic opportunities and be confident in its ability to stay on course.
- **Resilient.** The best-laid plans of mice and men fail. Organisations need to be able to bounce back quickly from changes in context and risks with limited business impact. They need sufficient tolerances to allow for some missteps and have the confidence necessary to adapt and respond to opportunities rapidly.
- **Efficient.** They build business muscle and trim the fat to rid expense from unnecessary duplication, redundancy and misallocation of resources; to make the organisation leaner overall with enhanced GRC capability and related decisions about the application of resources.



### What confuses organisations is that they think GRC is about technology

context, risk management fails.

Risk management assesses and monitors risk to objectives within the context of governance to take action on risk through identification, analysis and then treatment (risk acceptance, avoidance, mitigation or transfer). ISO 31000 defines risk as to the “effect of uncertainty on objectives” providing a natural flow and integration of governance to risk management.

Compliance provides boundaries to frame risk management. Risk management, by itself, is neutral and analyses options. A risk assessment may very well determine that the organisation most likely can get away with an unethical course of action. Compliance frames the

ethical principles as well as the obligation boundaries (for example, regulatory requirements, contractual commitments or corporate social responsibility values) for risk management to work within. Compliance provides the follow-through on risk treatment plans to ensure that risk is managed within limits and controls are in place and functioning. Risk management fails without compliance as compliance is needed to ensure controls are in place and operational to mitigate risk.

### Three legs

The components of GRC provide the three legs of the stool that





question is, how mature is the organisation's GRC capability? Is it a reactive and disconnected process with departments going in many directions with much redundancy? Or is it mature, integrated and coordinated across the organisation that aims to deliver on agility, efficiency and effectiveness of GRC-related processes in the context of organisation strategy, performance and objectives?

The research organisation GRC 20/20 has identified two approaches that organisations take to manage GRC – anarchy and federated. Anarchy is based on ad hoc department silos. This is when the organisation has departments doing different yet similar things with little to no collaboration between them. Distributed and siloed GRC management initiatives never see the big picture and fail to put risk management in the context of organisational strategy, objectives and performance. The organisation is not thinking big picture about how GRC management processes can be designed to meet a range of needs. An ad hoc approach to GRC management results in poor visibility of the organisation's relationships, as there is no framework for bringing the big picture together; there is no possibility to be insightful about risk, compliance and performance. The organisation fails to see the web of risk interconnectedness and its impact on performance and strategy, leading to greater exposure than any silo understood on its own.

Federated GRC is an integrated and collaborative approach. The federated approach is where mature organisations will find the greatest balance in a collaborative and connected view of GRC management and oversight. It allows for some level of department and business function autonomy when needed, but also focuses on a common governance model, processes and architecture that GRC functions across the organisation can participate in. A federated approach increases the ability to connect, understand, analyse and monitor connectedness and underlying patterns of performance, risk and compliance. Different functions participate in GRC management with a focus on coordination and collaboration

“ There is no single technology solution that does everything GRC .....

offer support and stability to the business and its operations. You take one leg away and the stool is no longer stable. It takes all three elements of governance, risk management and compliance working together to provide stability and balance for the organisation.

Every organisation does GRC today. They may call it enterprise risk management (ERM), operational risk management (ORM) or integrated risk management (IRM). Some may not have a name for it. Every organisation is doing GRC, no matter what they call it. You will not find an organisation that states they do not govern the organisation, that risk is not managed and compliance is neglected. The

## GOVERNANCE, RISK AND COMPLIANCE

**Group Chair: Robert Toogood Secretary: Lucy Smithwick-Eldred**

GRC is a term used to describe an integrated approach to activities related to governance, risk management and compliance. Increased corporate failures and enhanced regulatory requirements have heightened corporate awareness about the value and importance of making sure these key activities are effectively designed, integrated and managed.

While the GRC approach has been in existence for over a decade, a recent survey from the Open Compliance and Ethics Group (OCEG) suggests that only 13% of respondents were able to claim they had harmonised or successfully achieved this level of integration. However, 93% of respondents that had successfully integrated these areas reported meeting or exceeding their original expectations.

### Group aims and objectives

The purpose of the group is to explore what GRC really is, and how it can be used across all functional areas of an enterprise.

Based on feedback received from the member feedback questionnaire, specific areas of interest for the SIG will include:

- Explore what GRC really is and agree a common (or assumed) definition, with focus on understanding purpose, scope and boundaries of each individual element and then how these come together to provide integrated GRC
- Share experiences, both good and bad, of our attempts so far to implement GRC
- Identify possible international best practice GRC guidelines
- Prove/demonstrate benefits of/from GRC implementations
- Develop GRC training and communication programmes
- Facilitate GRC benchmarking between organisations
- Investigate use of financial and other GRC-related metrics


 **Join the group to receive information about future meetings, or please contact [events@theirm.org](mailto:events@theirm.org) for further details.**



**Successful GRC management requires the organisation to provide an integrated process, information and technology architecture**

enterprise GRC platforms. However, these solutions are not GRC in themselves. Nor is there any single technology solution that does everything GRC. There can and should be a central core GRC platform that connects the fabric of governance, risk management and compliance processes, information and other technologies together across the organisation. This architecture is the hub of GRC management and requires that it be able to integrate and connect with a variety of different systems and enterprise applications to deliver on GRC.

Successful GRC management requires the organisation to provide an integrated process, information and technology architecture. This helps to identify, analyse, manage and monitor GRC, and capture changes in the organisation's risk profile from internal and external events as they occur. Mature GRC management is a seamless part of governance and operations. It requires the organisation to take a top-down view of risk linked to objectives, led by the executives and the board. It also involves bottom-up participation where business functions at all levels identify and monitor uncertainty and the impact of objectives. While that may sound like hard work – and it is – organisations that get a good grip on their GRC initiatives have a much better chance of thriving in today's complex business world. ☞

 **Michael Rasmussen is an Honorary Life Member of the IRM and an internationally recognised pundit on governance, risk management and compliance (GRC) and founder of GRC 20/20 Research, LLC.**

through common processes and integrated technology architecture.

### Maturity

The primary directive of a mature GRC management capability is to deliver effectiveness, efficiency and agility to the business. This is in the context of managing the breadth of risks on organisational performance, objectives and strategy. This requires a strategy that connects the enterprise, business units, processes, transactions and information to enable transparency, discipline and control of the ecosystem of risks and controls across the extended enterprise.

Organisations need a mature GRC capability that brings together a coordinated strategy and

processes. This is supported by a strong information and technology architecture that provides an integrated view of objectives, risks, compliance, controls, events and more. However, what confuses organisations is that they think GRC is about technology. That is putting the cart before the horse. GRC is about a capability delivered through a coordinated strategy and processes across the organisation. Technology enables these processes to work together and function, but it does not define them. Too many organisations think GRC is something they purchase. GRC is not something you buy; it is something you do: GRC is the actions and activities of governance, risk management and compliance.

There is technology for GRC and we often call this integrated or



**CIR** | Risk Management

10th ANNIVERSARY

AWARDS 2019

# BOOK YOUR TABLE

**The 10th annual Risk Management Awards**

**6 NOVEMBER 2019**

**London Marriott Hotel  
Grosvenor Square**

**Celebrating success in the  
practice of risk management**

**@CIR\_Magazine #RiskManagementAwards**

**[cirmagazine.com/riskmanagementawards](http://cirmagazine.com/riskmanagementawards)**

Sponsored by



Headline partner



Supported by





# Spotlight on slavery

A review of the UK's Modern Slavery Act is set to bring in more detailed reporting and public scrutiny

BY SARAH WINT

**I**n July this year, ITV News reported that the UK's largest-ever UK modern slavery ring had been discovered and dismantled. More than 400 people had been forced to work for as little as 50p a day while the criminal gang masters earned a total of £2 million. The police spent three years investigating the well-organised criminal gang that was led by the Brzezinski family. It exploited the homeless, ex-prisoners and alcoholics, the report said.

The ring lured its victims from Poland and then trafficked them to the UK with the promise of good money. When they arrived in Britain, those who had been misled found that they were housed in squalor and used as what a judge described as "commodities".

Judge Mary Stacey said their "degradation" of fellow human beings had been "totally unacceptable", jailing the five ringleaders for between 11 and four-and-a-half years. She added: "Any lingering complacency after the 2007 bi-centenary celebrations of the abolition of the English Slave Trade Act was misplaced. The hard truth is that the practice continues, here in the UK, often hiding in plain sight."

## Complacency

In his predictions for the top and abiding risks of 2019, Ray Flynn (CMIRM), an IRM board member and risk



**Risks involving unethical or illegal behaviour, in particular, are either overlooked or considered more remote than they should be**



Image credit: John Gomez / Shutterstock.com

“ Any lingering complacency after the 2007 bi-centenary celebrations of the abolition of the English Slave Trade Act was misplaced. The hard truth is that the practice continues, here in the UK, often hiding in plain sight

management consultant, warned that there had been a growing mountain of prosecutions and allegations of misconduct over the last few years at both an individual and organisation-wide level. They ranged from corrupt practices to inadvertent involvement in modern slavery, sanctions busting, sexual harassment, anti-competitive behaviour and the misuse of personal data.

“Despite nearly all of these being covered by recent legislation in a number of countries, this trend is likely to continue in 2019. Why?” Flynn asked. “The fact is that organisations tend to be a lot better at addressing external than internal risks, and risks involving unethical or illegal behaviour, in particular, are either overlooked or considered more remote than they should be.”

Despite the UK’s groundbreaking Modern Slavery Act (2015) highlighting the realities of contemporary labour abuse, Flynn said that executives and risk managers were often reluctant

to entertain the prospect of fellow workers, or even business partners, suppliers or subcontractors, as capable of underhand practices. Risk assessments often never got off the ground prior to developing policies and procedures because people were often doubtful that their organisations and suppliers would carry out such crimes. “This complacency, which can border on arrogance, left those entities affected unprepared, resulting in a much heavier price in remediation than they would have forked out in mitigation, with the right approach before an ‘incident’ has taken place,” he said.

### Strengthening the laws

It is timely, then, that a government-commissioned review lead by the MP Frank Field has recently recommended strengthening the provisions of the Modern Slavery Act. Risk managers should be able to detect signs that the practice is going

on through well-known indicators (see *Red flags*). But the *Independent review of the Modern Slavery Act 2015: final report*, published in May this year, warns that companies are not doing enough to secure the transparency of their supply chains. Under section 54 of the act, a company must state the steps it has taken to ensure that slavery and human trafficking is not taking place in its business or its supply chains – or it can say it has done nothing.

“Evidence gathered by our expert advisers shows that there is a general agreement between businesses and civil society that a lack of enforcement and penalties, as well as confusion surrounding reporting obligations, are core reasons for poor-quality statements and the estimated lack of compliance from over a third of eligible firms,” it concluded.

There are six areas that statements may cover – but do not have to – under the act. These are the organisation’s structure, business and supply chains; relevant policies;

due diligence; details of risky parts of the supply chain and action taken; key performance indicators to show the effectiveness of the business's approach; and staff training. The report recommended that these should be mandatory in future.


## Next steps


The government received the report positively (*UK government response to the independent review of the Modern Slavery Act 2015*) and has promised to hold a consultation on

its recommendations. That includes a commitment to revise the rules on supply chains. One of the innovations that is likely to come out of the process is a template that describes in more detail what organisations need to cover in the six key areas.

"Recognising that organisations will need to retain the flexibility to set their own priorities based on the specific risks faced by their business, the template will be non-exhaustive and will evolve over time to reflect emerging best practice about the most effective ways to

address modern slavery risks," it said. The template will be included in revised statutory guidance which will be published in 2020.

In June 2019, the government announced that it would be creating a registry where all of the statements produced by companies on anti-slavery would be publicly available. The model for this is likely to mirror that introduced for reporting on gender pay equality in businesses. It will not have escaped the notice of risk managers that this system has put the spotlight on companies that do less well than others – with all of the reputational damage that goes with such public outcries. With more detailed, public reporting on this sensitive issue on the cards, it could be time to get ahead of the game. 

 The IRM has published *Modern Slavery Act, a guide to compliance*, which is available for free on the website.

## RED FLAGS

### How to recognise the signs of human trafficking and slavery

- **Restricted movement:** Often victims of modern slavery will be kept against their will in environments with security measures in place to prevent escape.
- **Overtime:** Sometimes workers will need to work overtime just to make minimum wage.
- **Recruitment fees and loans:** When the fee paid or loan taken by the worker cannot reasonably be paid off in time based on wages received.
- **Documents:** Where employers take possession of workers' documents and the workers do not have free access to them.
- **Payment:** Where workers are not paid as part of a formal and documented system.
- **Subcontracted work:** Where workers are subcontracted throughout the supply chain.
- **Prison labour:** Prison labour can be used for commercial purposes under improper conditions.
- **No complaints procedure:** Exploited workers are typically unable to improve their situation because there is no one in their organisation who cares.
- **Living conditions:** In certain situations, workers may live together on site or in accommodation provided by the employer.
- **Union infrastructure:** When workers do not have access to union representation, they are less able to express their grievances and protect their rights.
- **Emotional indicators:** Victims of modern slavery will often exhibit signs of anxiety and fear.

Source: *IRM Modern Slavery Act, a guide to compliance*.

## PROPOSALS FOR IMPROVING THE QUALITY OF ANTI-SLAVERY STATEMENTS

- Section 54(4)(b), which allows companies to report they have taken no steps to address modern slavery in their supply chains, should be removed.
- In section 54(5) "may" should be changed to "must" or "shall", with the effect that the six areas set out as areas that an organisation's statement may cover will become mandatory. If a company determines that one of the headings is not applicable to its business, it should be required to explain why.
- The statutory guidance should be strengthened to include a template of the information organisations are expected to provide on each of the six areas.
- Guidance should make clear that reporting should include not only how businesses have carried out due diligence but also the steps that they intend to take in the future.
- The Independent Anti-Slavery Commissioner should oversee the guidance available to companies.
- The legislation should be amended to require companies to consider the entirety of their supply chains. If a company has not done so, it should be required to explain why it has not and what steps it is going to take in the future.

Source: *Independent review of the Modern Slavery Act 2015: final report*



# Faster business cycles



## *The building blocks of agile risk management*

BY MATT TAYLOR

**T**he rapid pace of technological innovations within industry threatens to disrupt organisations' ability to compete. This increased velocity poses new challenges to risk and compliance functions as they strive to ensure sound practices throughout the development of new initiatives or products. As a result, they must be able to digitise their operations and adopt strategies to reduce go-to-market lead time.



Protiviti's latest paper examines risk management designed appropriately to keep pace with agile organisations, the practices that allow for operational excellence and focus on customer experience.

Agile initiatives require nimble execution teams working rapidly to spur business changes, according to the report. However, how can control functions, including risk, compliance

and business control teams, execute credible challenge near real-time? Answer: they will need to rethink their interaction models for executing credible challenge and advising the business in near real-time methods.

By taking advantage of technological and analytical capabilities to efficiently deliver business and risk insights, their oversight culture can become more agile.

### Customer upside

Aligning risk management with agile execution enables companies to improve customer satisfaction swiftly, thereby giving organisations a competitive advantage.

They can be integrated into digital communication platforms used by agile teams to obtain key information throughout sprints – specialists in their team can challenge and test key controls ensuring agile teams align to firmwide standards at the onset, without sacrificing agility, and allowing risk and compliance to advise at a rapid pace.

The first latest initiative worth exploring is dynamic workflow and assessments. A single source of truth can map projects and initiatives to process, risk and control taxonomies, integrate automated and preventive controls throughout project execution and capture all key project information. This enables automated monitoring, allowing


organisations to achieve scalability and business leaders and control functions to run automated deep-dive analysis on in-flight projects with the result that post-mortem analyses on initiatives can assess the new equilibrium state of residual risk, and adapt their oversight.



**Aligning risk management with agile execution enables companies to improve customer satisfaction swiftly, thereby giving organisations a competitive advantage**

The second is risk bots. Artificial intelligence enables the application of risk data in business processes in an unprecedented way. Now risk bots could advise by suggesting applicable risks and controls based on data obtained from similar projects. It is already being applied to customer service departments, allowing reallocation of time toward more analytical activities or true high-priority initiatives.

### The way ahead

Successful organisations will implement methodologies for allowing product initiatives to succeed at a faster rate. By adopting an agile risk management philosophy using technology-supported risk frameworks to maintain both speed in execution and a strong risk culture gives companies a competitive edge in deploying market-ready products and services that integrate with their existing business strategy and environment and maintain long-run sustainable operations. 



**Matt Taylor is a managing director in Protiviti's Risk and Compliance team, which specialises in helping organisations design and implement sustainable risk management strategies. Contact: 020 7930 8808**

## RISK MANAGEMENT – MEGA PROJECTS – SCOTLAND RIG

### 📍 Glasgow Caledonian University, Cowcaddens Road, Glasgow, G4 0BA

Topics will include the UN Charter on Business and Human Rights with Governments and Global Organisations, SRAs and how they are utilised in Nuclear Industry & the use of Value Management and Cost Risk Analysis to achieve business objectives and enhance decision making on large projects. GCU will provide an update as to what is happening in the academic future of risk management.

📅 20th September 2019

🕒 09:00-12:15

👤 Donna Festorazzi

☎ –

✉ events@theirrm.org

## ANTI TERRORISM – UNDERSTANDING THE RISKS – NORTH EAST RIG

### 📍 East Room, Civic Hall, Calverley Street, Leeds, LS1 1UR

Our first speaker works with the Counter Terrorism unit for Leeds City Council and will talk to us about the current Threat levels and discuss the Protect and Prepare strand of the 4 P's (Prevent, Protect, Prepare and Pursue). Our second speaker is delivering Project Servator, a national project which was developed, by experts at the Centre for the Protection of National Infrastructure in partnership with the City of London Police.

📅 20th September 2019

🕒 10:00-13:00

👤 Neil Hodgson

☎ –

✉ events@theirrm.org

## LESSONS FROM THE AUSTRALIAN FINANCIAL SERVICES INDUSTRY

### 📍 Pewterers' Hall, Oat Lane, London, EC2V 7DE

This event is organised by IRM's partner, the Institute of Operational Risk, and sponsored by The Protecht Group, it will review the key lessons for financial service companies arising from the 2019 Royal Commission report on the Australian banks and the Prudential Regulatory Report on Australia's largest bank – The CBA. These Inquiries have set the standard for "The Next Level" in Financial Services risk management.

📅 24th September 2019

🕒 15:30-18:00

👤 –

☎ –

✉ events@theirrm.org

## CLIMATE CHANGE AND RISK MANAGEMENT

### 📍 LexisNexis, Lexis House, 30 Farringdon St, Holborn, London, EC4A 4HH

Practical demo of Climate Change. Discussion of evidence around climate change and forecasts for change Commercial perspectives: an infrastructure viewpoint. A Chief Risk Officer view. Breakout in groups to consider issues. Feedback and discussion with round table of speakers. Networking.

📅 24th October 2019

🕒 15:00-17:45

👤 –

☎ –

✉ events@theirrm.org

## STRATEGIC RESILIENCE – DRIVING COMPETITIVE ADVANTAGE – MIDLANDS RIG

### 📍 PwC, Cornwall Court, 19 Cornwall Street, Birmingham, B3 2DT

The Midlands Regional Group is delighted to be partnering with the Operational Resilience Special Interest group for our next meeting to focus on Strategic Resilience. The event will be supported by PwC who are hosting the event at their Birmingham office. Details on speakers will follow, but places will be limited. Please register early to secure your place.

📅 14th October 2019

🕒 09:00-15:30

👤 Susan Howlett

☎ –

✉ events@theirrm.org

# Understanding complexity



*Complexity is a reality in today's highly interconnected world. That is why IRM is creating a new Special Interest Group to better understand the phenomenon says Greg Lawton*

**T**he phrase complexity, like strategy, is a catch-all term that means many things to many people. Before the 21st century this generality had little consequence. The world was less connected. Today, with the age of interconnectivity in full swing, it has global impact and is a key concept for risk managers to get to grips with. That is why I have helped to create an IRM risk and complexity special interest group – and would urge you to get involved.

But why look at complexity specifically if it is all around us? Businesses, governments and societies that recognise complexity as a key change driver will find themselves in a new era of productivity and performance. Those that don't will fall behind.

## Defined

One definition of complexity is that it is the propensity for emergent phenomena to arise due to the interconnected nature of a system. In practice, when things become connected, they start to exhibit behaviours over and above what could be expected from the simple addition of their parts. In this way, seemingly simple things come to life: brain neurons combine to give intelligence, financial markets wave an invisible hand and social media posts go viral.

But like many of the forces of nature, complexity doesn't have a moral compass – it simply exists. For instance, it also allows misfiring neurons to cause life-threatening seizures, the collapse of individual banks to trigger global financial crisis and fake news to drive division throughout nations. At its heart, complexity is a multiplying force that turns common occurrences into global events. It is driven by interconnectivity, and as this grows the power of complexity will also grow.

## Measurement

While something may be complicated, it doesn't necessarily mean that it is complex. Imagine building a skyscraper. The list of materials may be long and diverse, but not complex. The time it takes to complete sections of the


building may be ambiguous, but that creates uncertainty, not complexity. But when it comes to estimating a final delivery date and fixed cost, complexity begins to kick in as all of the different factors are combined.



**Complexity is a multiplier that turns common occurrences into global events**

Complexity is a real factor that can be measured, which enables risk managers and others to perform experiments on it and figure out how to control it. However, here lies a red herring. In our quest to control complexity we will be tempted to apply our latest black-box computing methods to skip the learning curve. But if we wish to tame complexity, like anything else, we must first understand it.

## Get involved

One day complexity will be fully understood. Due to events like the global financial crash of 2009 we have realised that taming complexity is important for the future, and we have subsequently made major leaps forward in our understanding. Unfortunately, as the force of complexity acts across multiple domains the research is generally scattered. In the future, when the findings of complexity science have been brought together, we will be in a better place. To better understand complexity and see the latest findings I would invite you to get involved in our new special interest group by using the email below. 



Greg Lawton is an IRM Affiliate member and CEO of Nodes & Links, a London-based, venture-backed company that is world-leading in the application of complexity science to business and project risk management. To get involved in IRM's risk and complexity special interest group, please contact [membership@theirrm.org](mailto:membership@theirrm.org). All welcome.



## Due diligence solutions



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

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

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

## Empowering your resilience



C2 is an established Business Continuity software provider with a continuing commitment to its customers to evolve with the market. Our mission is to provide intuitive and innovative solutions for the global business resilience market and reshape the industry as we know it today. Our Business Continuity Software is used to alleviate and assist with the day to day management of an

organisation's Business Continuity Management System requirements. We provide BCM software and practical solutions to some of the world's largest utility companies, world leading finance and investment organisations, global telecom organisations and more. Find out more: <https://continuity2.com/>

 **Richard McGlave**  
 **+44 (0) 845 094 44 02**  
 **info@continuity2.com**  
 **continuity2.com**  
 **Prism House, Scottish Enterprise**  
**Technology Park**  
**East Kilbride, Glasgow, UK**  
**G75 0QF**

## 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**  
 **+44 (0) 1275 545874**  
 **ian.baker@riskhive.com**  
 **www.riskhive.com**  
 **riskHive Software Services Ltd.**  
**Dilkush, Farlers End**  
**Bristol**  
**BS48 4PG**

---






## Financial risk management and Solvency II software

---



RemitRix helps insurers manage financial and actuarial risks by harnessing the power of Machine Learning to improve actuarial predictions. Our product RemitRix Agile is a web based financial risk management platform. RemitRix Agile includes classical risk management tools such as ESG, VaR, Solvency II full solution, optimization tools and more. It is easy to deploy and manage. It is

planned to fully integrate with our future actuarial solution.

 **Effi Mor**  
 **+44 (0) 20 3608 3987**  
 **info@remitrix.com**  
 **www.remitrix.com**  
 **RemitRix**  
**Shoham Street 8**  
**Ramat Gan**  
**Israel**

---

## Risk and audit management software solutions

---



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

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

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

---

## Risk, insurance and safety technology solutions

---



Ventiv Technology is the preeminent provider of global risk, insurance, and safety technology solutions. Working in partnership with our clients to understand their challenges and key business objectives, our solutions adapt to your precise needs and evolve with you. Providing a central platform

to work across your company and functions to eliminate silos and help embed risk management. Delivered with Ventiv's extensive risk management and technology experience to provide unsurpassed client value and operational excellence. Ventiv pride themselves on data security and have recently added another certification to their tool belt – ISO27018:2014; standard for protecting privacy in the cloud.

 **Steve Cloutman**  
 **+44 20 3817 7373**  
 **steve.cloutman@ventivtech.com**  
 **www.ventivtech.com**  
 **Ventiv Technology**  
**30 Eastcheap**  
**London**  
**EC3M 1HD**

---

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

## Risk management software

### AGENARISK

AgenaRisk is a model design and execution environment for Bayesian Networks, designed for organisations that need to assess and manage risks in areas where there is little or no data, where direct measurement is not possible, and in the face of new, often novel, circumstances.

Organisations use AgenaRisk to model a variety of problems including operational risk, actuarial analysis, intelligence analysis risk, systems safety and reliability, health risk, cyber-security risk and strategic financial planning. Models developed in AgenaRisk can be integrated into a wider service using AgenaRisk Developer and ultimately deployed using AgenaRisk Enterprise.

 **Ed Tranham**  
 **+44 (0) 1223 263880**  
 **sales@agenarisk.com**  
 **www.agenarisk.com**  
 **11 Main Street  
Caldecote  
Cambridge  
CB23 7NU**

## Risk management software

### alyne

ALYNE – is an industry leading and award-winning, Regulation Technology Software company – that makes it easy for organisations to reduce the cost – of managing risk and compliance obligations and is built by industry experts. ALYNE – is a next generation, cloud solution that makes risk and compliance management as easy as browsing social media. ALYNE – with its unique pre-built

library of controls, integrated risks and assessment templates – mapped to regulations and standards, is ready to use out of the box – with dynamic reporting and real-time risk insights. ALYNE's – innovative approach – enables organisations to make the right executive decisions and outcomes – and to drive business advantage.

 **Pierre Silavant**  
 **+44 (0) 7767 444 755**  
 **pierre.silavant@alyne.com**  
 **www.alyne.com**  
 **41 Luke Street  
Shoreditch  
London  
EC2A 4DP, UK**

## Risk management software

### MAGIQUE GALILEO

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

 **Trevor Williams or Verna Hughes**  
 **+44 (0) 203 713 4590**  
 **info@magiquegalileo.com**  
 **www.magiquegalileo.com**  
 **Magique Galileo Software  
Birchin Court  
20 Birchin Lane  
London, EC3V 9DU**



---




## 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](mailto:nscotcher@origamirisk.com)**  
 **[www.origamirisk.com](http://www.origamirisk.com)**  
 **30 Moorgate  
London  
EC2R 6PJ**

---

## Risk management software

---



The Protecht Group is a leader in Enterprise Risk Management Software and Services that enables organisations to achieve their strategic objectives through efficient, effective and agile Risk Management. Protecht. ERM™, Protecht's flagship product, has been deployed in a SaaS model since development commenced in 2002 and

remains ahead of the curve on innovation and functionality. Used by government agencies, regulators, commercial and not-for-profit organisations of all sizes and risk maturity, Protecht. ERM™ allows companies to seamlessly integrate risk management into their day-to-day activities and gain operating efficiencies through its flexible web-based forms, workflow engine and highly adaptable reports and dashboards. Protecht is more than a software company, we guide you through your risk management journey.

 **Keith Davies**  
 **+44 (0) 7828 163 802**  
 **[keith.davies@protechtgroup.com](mailto:keith.davies@protechtgroup.com)**  
 **[www.protechtgroup.com](http://www.protechtgroup.com)**  
 **131 Finsbury Pavement  
London  
EC2A 1NT  
United Kingdom**

---

## Risk management software

---



Xactium is a cloud based GRC software provider that helps Risk Managers to transform the way that organisations value and manage their enterprise risk. As the central risk platform used by the FCA to supervise the market, it has also been adopted by a wide range of financial organisations such as Direct Line Group, JLT, MS Amlin,

Leeds Building Society and Argo Group. Xactium is the world's first enterprise risk-intelligent system, with the revolutionary use of embedded AI (Artificial Intelligence), 3D visualisation and automation that dramatically improves efficiency and creates innovative analytics. Reporting is made easy and timely, and predictive insights enable senior managers to prioritise resources. Overall, Xactium releases more time and resource for the risk team to help promote best practice and demonstrate the value of risk across the business through actionable insight.

 **Steve Birch**  
 **+44 (0) 114 2505 315**  
 **[steve.birch@xactium.com](mailto:steve.birch@xactium.com)**  
 **[www.xactium.com](http://www.xactium.com)**  
 **Xactium House  
28 Kenwood Park Road  
Sheffield  
S7 1NF**

# History lessons

*Risk managers are increasingly looking to case studies of past successes and failures to engage their stakeholders on risk. But history comes in many flavours*

**T**he first historians in the Western tradition saw the past as a treasure trove of moral and military lessons. Thucydides, for example, in his epic telling of the Peloponnesian War between Athens and Sparta, which started around 431BC, was as rigorous as it was possible to be in his recounting of events. Having fought on both sides, he interviewed many of the participants and discounted tales of divine intervention in his account of the 30-year conflict.

But his task was a moral one – he wanted to recount the truth of events so that people in following generations would learn from them and avoid making the same mistakes. That included graphic details of plague infections so that doctors may recognise the symptoms in future. Ultimately, Athens failed, in his view, because it deviated from its original plan not to engage in land battles with the Spartans and not to open up new theatres of war until it had succeeded in defeating the enemy. It did both and lost.

## Learning

Thucydides and his text became widely known throughout the ancient world. But that civilisation did not survive. It may have been this fact that led the 19th-century German philosopher GWF Hegel to muse that the only lesson we can derive from history is that people never learn lessons from history.

In fact, Hegel helped to ignite a renewed interest in history as a social process. He inspired Karl Marx's history of "political economy" that, indirectly, led to the Russian revolutions of 1917. The point was not to understand the world through history but to change it, Marx believed.

Today, historians are more aware than



**“** The only lesson we can derive from history is that people never learn from history


ever that their own perspective is part of the social processes they describe. Thucydides' search for the truth was complicated, as he already knew, by social forces that are hidden from view. Learning from history means not only identifying important events and recounting them truthfully but also standing back and recognising the impact of one's place in it.

## One-sided

In film culture, for instance, the history of the 20-year conflict in Vietnam has been consistently cast as an American tragedy. Not until the monumental 2017 documentary series *The Vietnam War*, by Ken Burns and Lynn Novick,

has the story of both sides been seriously treated on television.

This raises important questions about how risk managers can compile and use case study material – a history of disasters and successes – effectively and truthfully. Unlike Thucydides, they are unlikely to have witnessed all sides of a disaster where there have been outside causes. Yet, as objective participants, they should be able to interview people and piece together an accurate picture of how the organisation saw itself at that point in time. Collating the material in those circumstances should be possible.

On the other hand, they may be as blind to their own prejudices as movie makers have been to theirs over Vietnam. Perspective cannot be easily understood because it belongs to the larger culture of the organisation. Those stakeholders outside of the business may need to be consulted: non-executive directors, regulators, pressure groups and customers. That may prove to be an uncomfortable procedure. But without it, as Hegel said, organisations are unlikely to learn the lessons of their own histories. 



# Is your ERM framework solution agile enough?

- Fully Interactive risk bowties and visualisation graphics
- Monte Carlo simulation for cost and time (combined)
- Dynamic risk scoring across multiple impact perspectives
- Actions and controls effectiveness tracking and reporting
- Automated reminders, alerts and reporting scheduling
- Over 70 national languages and unlimited currencies



Whether you call it 'agileGRC' or 'Integrated Risk Management', riskHive is the solution

The riskHive is a highly secure, hyper-configurable 'works-right-out-of-the-box' ERM Portfolio application. It can be easily aligned with your risk framework to quickly and effectively deploy your global ERM toolset. A browser-based user interface and 'Unlimited User' licence makes riskHive a true enterprise risk application.

Its main screens and reports can be designed to replicate existing forms and documents and so help you to transition quickly and seamlessly from spreadsheets to database with all the associated capability benefits but with minimal training and reduced initial set-up, configuration and commissioning costs.

So whatever you call your risk solution, the riskHive is the cost-effective, fast-deployment toolset you need.

Talk to us if you:

- Need to consolidate multiple excel or word risk registers
- Want easy automated or single-click monthly reporting
- Want full visibility of risk throughout your organisation
- Have difficulty in understanding how risks interconnect
- Lack a single version of the truth in your organisation
- Want to give your Board and Shareholders even more confidence in your risk and compliance reporting

Find out more at [www.riskhive.com](http://www.riskhive.com)  
or contact us for a demonstration at  
[info@riskhive.com](mailto:info@riskhive.com) or talk to us on  
+44 (0)1275 545874





# AN SMCR SOLUTION THAT HELPS YOUR SENIOR MANAGERS SLEEP AT NIGHT

Prepare for the arrival of the Senior Managers & Certification Regime with Xactium SMCR.



- Get access to a centralised and detailed management of Senior Management Functions (SMFs) and Prescribed Responsibilities.
- Create and share detailed Responsibility Maps within your organisation.
- Easy to follow workflow for senior managers to view and approve all responsibilities and functions assigned to them by the organisation.
- Assign risks and actions related to specific Prescribed Responsibilities and track their progress.
- Powerful reporting and dashboard tools.
- Easily produce a variety of documents that set out the firm's management and governance arrangements, with a click of a button.
- Generate branded certificates as part of the Certification Regime.
- Available alongside our Xactium Compliance system, part of our integrated GRC solution.

If you would like more information go to  
[www.xactium.com/smc-software](http://www.xactium.com/smc-software)