Enterprise Risk

Summer 2022 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

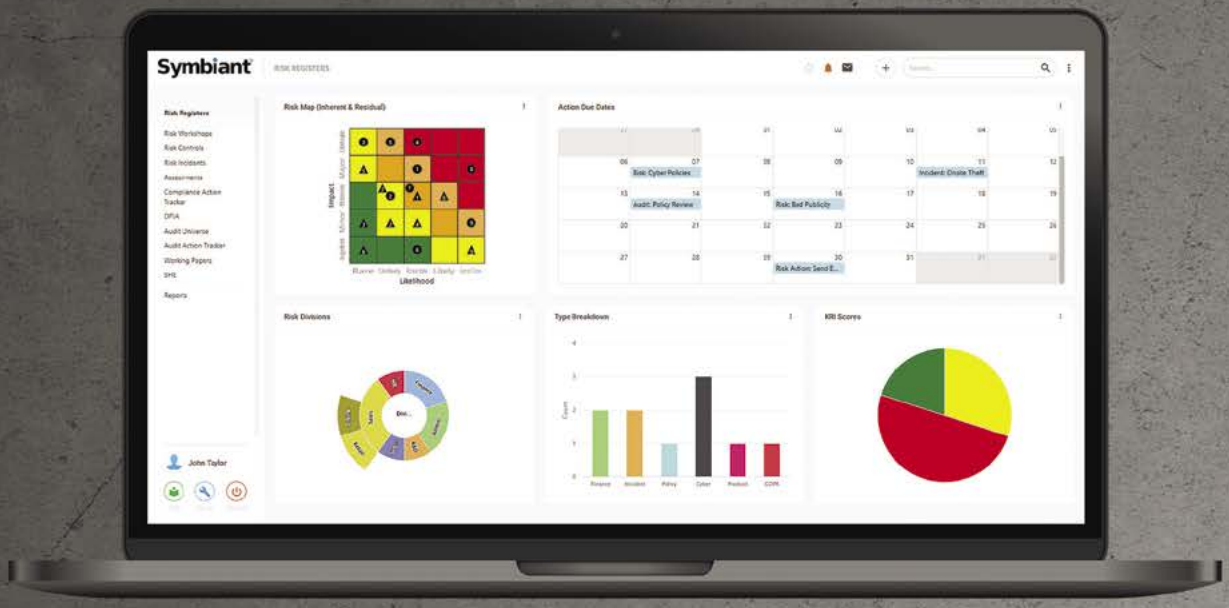
The diversity of culture: Organisations looking to create a single culture to manage risk are on the wrong path, as Martha Phillips found out

Grand designs: IRM's new strategic vision / **Getting results from great projects:** lessons from experience / **Building competency:** Nuclear Decommissioning Authority / **Digitalising the supply chain:** creating resilience

22 Years in the making

Symbiant One

A modular solution for Risk, Audit & Compliance



Clean, Simple, Effective & Affordable

Watch our overview videos at
www.symbiant.one
and see for yourself why
Symbiant is clearly the better choice

WWW.SYMBIANT.ONE Symbiant®

Enterprise Risk

Summer 2022

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

Editorial

Fit for any future

In the middle of the 19th century, a radical new way of thinking about the relationship between people and the environment gradually took root. In the natural sciences, it was the botanist Charles Darwin who coined the now commonplace phrase "survival of the fittest".

He did not mean, of course, the most hench plants and animals would win in the race to reproduce. But those species that could adapt to fit into the changing environments in which they lived would survive best.

Rapid change

That adage has found new resonance today. Several recent books have written obituaries for the recent neo-liberal, capitalist world order that favoured internationalism, open borders, free trade and low inflation and interest rates. At what is hopefully the tail-end of the most serious pandemic since the Spanish Flu of 1918, and at a time of increased conflict, it is reasonable to wonder what type of organisation is going to be fittest in the apparently new world order.

Readers will find versions of that question throughout this issue of the magazine. For Simon Ashby (see *Honing resilience*, page seven), for example, those with the most robust operations will be able to adapt rapidly and effectively to new threats and opportunities. In a different context, for Martha Phillips (see *The diversity of culture*, pages 10-15) understanding and exploiting the various organisational cultures within a business is part of the answer.

Future profession

Enterprises, in short, must deal with complexity and surprise because they are emerging features of the environment in which they operate.

Among those organisations is IRM itself. It has been about seven years since the Institute conducted its last full-scale strategic review. Stephen Sidebottom, IRM's independent non-executive chair, has led the board and the organisation through the most recent review this year, which looks forward to the next phase of the Institute's journey (see *Grand designs*, pages 16-18).

"In the new strategy, there is a re-doubling of focus towards internationalisation," Sidebottom says. "We see that as a significant opportunity for IRM to contribute to effective risk management, and an opportunity for us to grow our membership, revenue and impact."

Under the bonnet, the Institute is looking to leverage its reach in the profession and beyond by working much more closely with its communities of members. After all, any organisation is the sum total of the knowledge and abilities of its people. That collaboration will also extend to IRM's stakeholders and to communities of like-minded people in the wider world.

Building an even stronger international network of highly qualified and trained risk professionals should help organisations become fitter for whatever new surprises are around the corner.

Arthur Piper
Editor

IRM's New Virtual Training Courses

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

IRM training courses take place online and in our on-site classroom. We present practical content, designed to stimulate and engage you. Our learning methodologies reinforce theory and sure you take home the tools and techniques that offer powerful tools for risk management.

Training courses include:

- Fundamentals of Risk Management
- The Risk Essentials Masterclass
- Practical Risk Appetite and Tolerance
- Effective Risk Registers and Assessments
- Embedding Risk Management
- Optimising Risk Workshops

Benefits of IRM training:

Practical & interactive training

Industry expert trainers

CPD & accreditation

Find out more at:

www.theirm.org/training-mag

irm

Developing risk professionals

Contents

Features

REGULARS

Digital Risk Management Certificate

The essential qualification for tomorrow's risk practitioner

About the Digital Risk Management Certificate

The Digital Risk Management Certificate is the ideal qualification for anyone looking to develop an understanding of risk management in the digital era. The qualification has been designed to introduce learners to digital disruption, its causes and consequences and to equip individuals with the tools and techniques to apply their skills in an increasingly digital world.

The qualification covers how to carry out digital risk assessments, provides a detailed grounding in cyber security principles and practices and also looks at the ethical issues surrounding both privacy and machine learning. The qualification explores how appropriate risk management tools and techniques can be applied, adapted and developed in the digital context and provides a detailed introduction to cyber security principles and practices.

What our students say

Stephanie Jackson
Senior Enterprise Risk Consultant, UK Risk Ageas
"The Digital Risk Certificate has helped to provide a more rounded understanding of today's cyber and business digitisation risks and mitigation strategies. A topic which couldn't be more important in today's direction of travel. Areas of focus within the different modules are relevant to all industries making this a great qualification for all."

Robert Luu
Director of Customer Success, Galvanize, Singapore
"Whether you're directly in risk management practice or not, the Digital Risk Management Certificate is a great qualification to immerse yourself in to grasp the foundational knowledge that touches on a variety of topics of today, and the technological advancement of the future."

In collaboration with

WARWICK
THE UNIVERSITY OF WARWICK

Find out more at:

www.theirm.org/drmc-mag

Resilience, risk and recovery

irm
Developing risk professionals

Honing resilience

Recent events prove that operational resilience has strategic importance for all organisations

The effects of the pandemic and now the war in Ukraine represent the most extended test of operational resilience in recent memory. During the height of the pandemic, for example, some industries effectively ceased to exist – airlines, restaurants and hotels, to name the most obvious. Many organisations failed completely – some are still struggling to survive.

But high-impact risk events are nothing new. In 1981, for instance, a strange disease started killing half of the people it infected. Yet at the beginning of the AIDS epidemic, governments did very little to educate potential victims, let alone take large-scale measures to protect populations – even though the cause and transmissibility of the infection were unknown. And compare Western governments' energetic reactions to Russia's invasion of Ukraine this year to their tepid response to its invasion of Georgia in 2006.

Impact

So, what has changed? In my view, the social context in which events arise is now different. Not only has social media grown to influence, if not dominate, political discourse, but perhaps attitudes to the sanctity of human life have shifted. That has driven more extreme and far-reaching responses to crises than in the past. You might say there has been a change in social and political risk appetites.

Risk managers need to reflect these new attitudes in their risk assessments – and test whether the assumptions that they are working under still hold true. That could mean deepening their thinking on how severe and long-lasting the impact of events could be. In other words, is your worst-case scenario truly the worst case you can imagine?

Operations

Fortunately, operational risk management has matured in recent years to help organisations better deal with these trends. With operational risk having originally been defined as "the risk of loss resulting from inadequate or failed internal processes" by the Basel Committee on Banking Supervision (the same year that Russian tanks rolled into Georgia),operational risk management is now better understood in its true light as being of key strategic importance.

Last year, I refreshed and extended the Institute of Operational Risk's ten sound practice guides to help risk managers get to grips with everything from risk appetite to risk and control self-assessment in this area. This year, I have built on that work in a new book, *Fundamentals of operational risk management: understanding and implementing effective tools, policies and frameworks.*

Practical

In this book, I suggest that a better definition of operational risk is "the effect of unpredictable outcomes on the efficiency and effectiveness of operations." Naturally, risk professionals exist to manage those unpredictable outcomes.

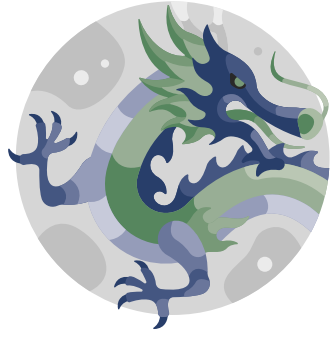
That is why I hope readers will use it as a practical manual to better understand in detail how they need to be thinking and working to improve operational effectiveness and efficiency. By gradually refining operational resilience one step at a time, risk managers should be able to make a significant contribution to how well their organisations cope with whatever extreme reactions come out of the next crisis. ER

Simon Ashby is professor of financial services at Vlerick Business School and author of *Fundamentals of operational risk management: understanding and implementing effective tools, policies and frameworks*. Members can receive a 20 per cent discount on the book using FORM20.

Trending

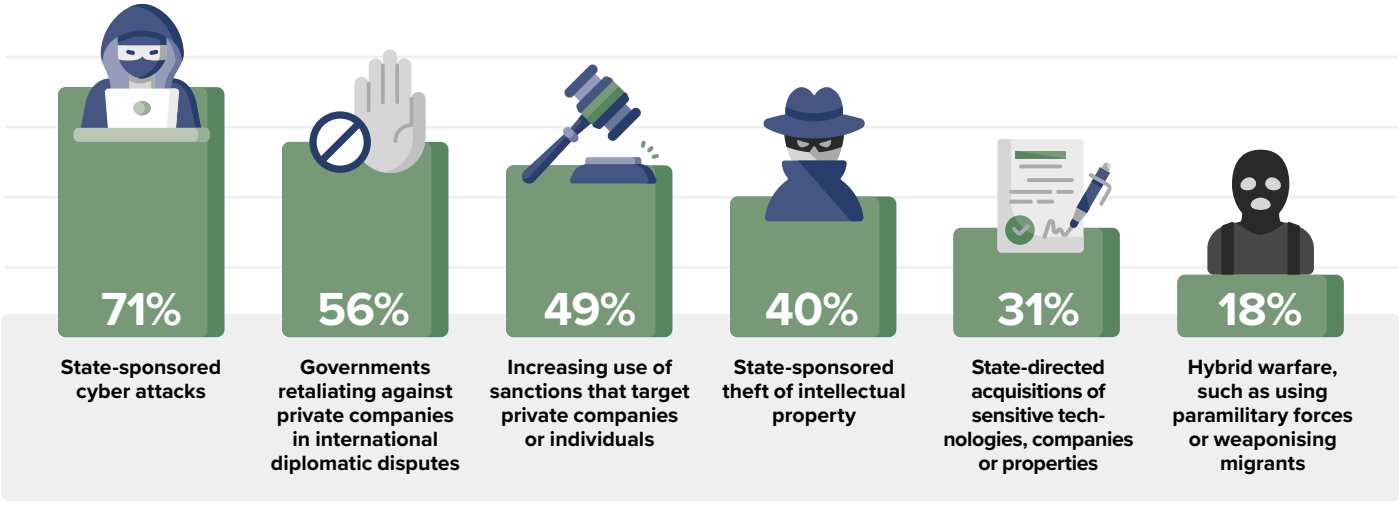
DATA

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



Geopolitical risk considered high in Asia

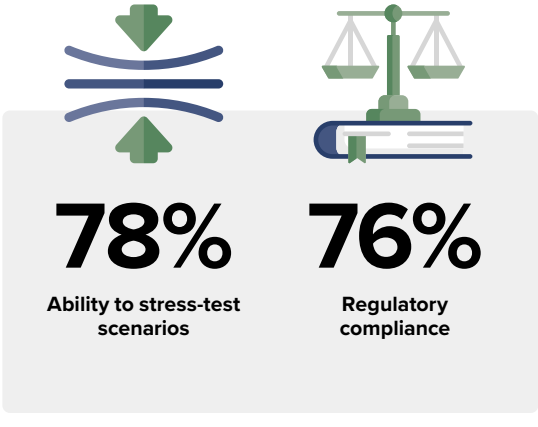
Most (95 per cent) of global companies fear loss from geopolitical risk stemming from Asia as worries about "grey zone aggression" grows



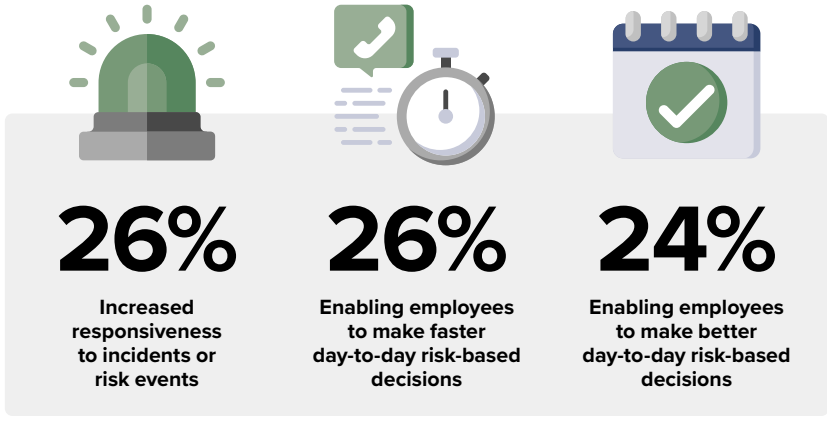
Source: *How are leading companies managing today's political risks? 2022 survey and report, WTW/Oxford Analytica*

Risk management aids resilience

Top risk management priorities over the next 12 months:



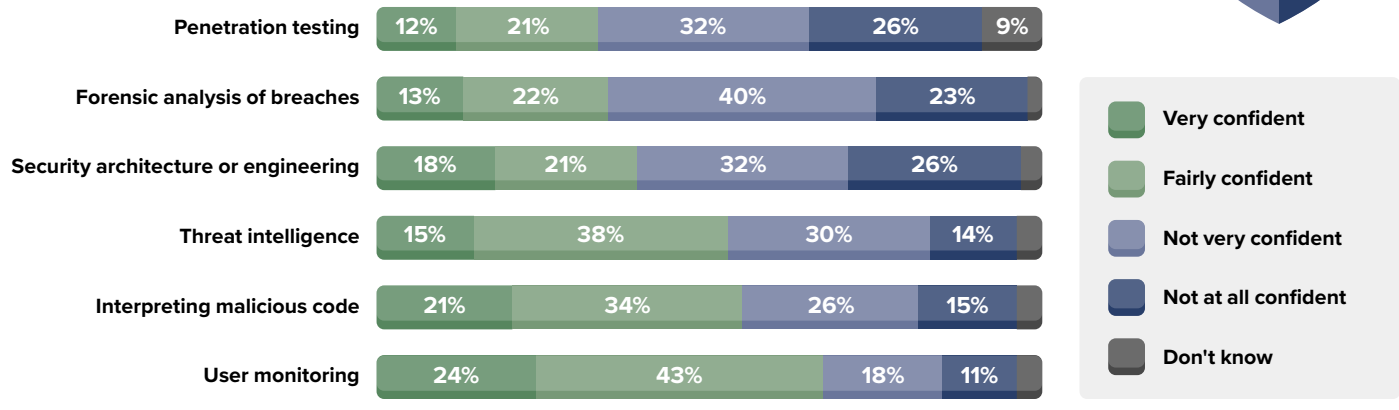
Benefits derived from enterprise risk management:



Source: *State of enterprise risk management 2022, Forrester*

Confidence in key cyber defence skills

Quarter of businesses lack confidence in penetration testing and forensic analysis



Estimated number of private sector firms with key skills gaps

355,000
(26%) have a skills gap in forensic analysis

328,000
(24%) businesses have a skills gap in penetration testing

328,000
(24%) have a skills gap in security architecture

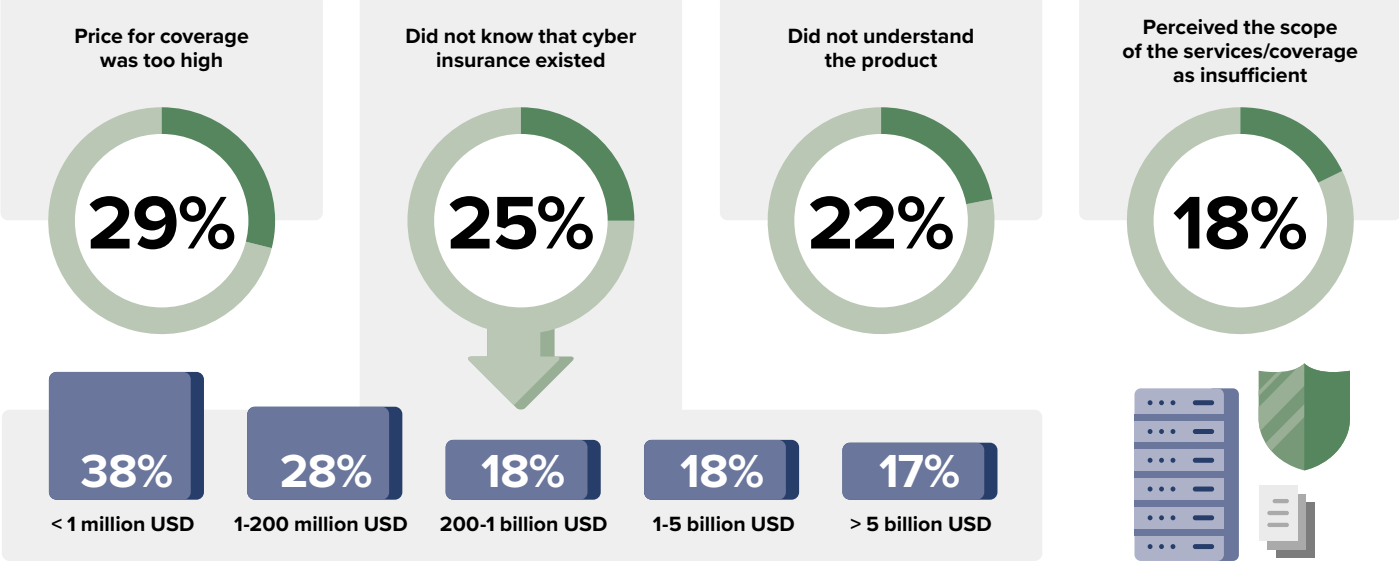
246,000
(18%) have a skills gap in threat intelligence

232,000
(17%) have a skills gap in interpreting malicious code

164,000
(12%) have a skills gap in user activity monitoring

Source: *Cyber security skills in the UK labour market 2022, UK Department for Digital, Culture, Media and Sport*

Reasons for lack of cyber insurance among C-Suite executives



Source: *Munich Re – Global Cyber Risk and Insurance Survey*

The diversity of culture

BY ARTHUR PIPER

Organisations looking to create a single culture to manage risk are on the wrong path. Not only is it impossible but could lead to less balanced risk decisions, as Martha Phillips found out

If the pandemic served as a wake-up call for organisations to get to grips with operational risk, the conflict in Ukraine has been yet another reminder that large-scale, unpredictable events can happen at any time and anywhere. These sudden shocks have come at a time of increased geopolitical tension globally and burgeoning risks from cyberattack, a failure to digitalise, climate change and shifting social expectations around working practices and diversity and inclusion.

"The nature of emerging risks is that they are becoming more difficult to evaluate," Martha Phillips, head of operational risk at AXA Health and a PhD candidate at the University of York, says. "Companies can monitor threats but knowing how and when to mobilise is challenging and costly. It's difficult to know which trends will remain, which will accelerate and which won't materialise at all. We are also facing new risks that humans have no prior experience of managing."

Forty years of political and economic integration in many parts of the globe have made risks more interconnected than ever so that individual threats have become harder to isolate, she believes. The war in Ukraine has most immediately, for example, impacted business' supply chains, regulatory and reputational risk, and cyber risk. But longer-term

> **"As risk and control professionals, we can't just deal with today's organisation anymore and the issues that we know about**

risks from rising inflation – not least because of Russia-related energy shortages – could affect market and customer behaviour in less predictable ways.

Detailed forward thinking

"As risk and control professionals, we can't just deal with today's organisation anymore and the issues that we know about," she says. Instead, organisations must get better at forward thinking – not just at a strategic level but at a deeper, detailed operational level to anticipate what might happen in future."

In practical terms, that means that control environments need to evolve to anticipate change and keep organisations within risk appetite. That sounds straightforward in principle, but businesses find it difficult to achieve. It means more investment and resources put into risks that have not (or may not) arise at a time when most organisations are struggling to cope with today's problems.

At AXA Health, Phillips is progressing a project called Better by Design. It aims to ensure that as the organisation delivers change, or develops new systems, the project team designs out any known issues at the same time as designing in compliance and resilience. "You are fighting against a human bias to get in and get out and complete the job that you are assigned to," she says. "But if you get into the habit of thinking about better by design, you can mitigate potential risk events before they arise and take account of emerging regulation at the same time."

She says that the approach tends to take more time because risk managers need to encourage business leaders to join up their respective transformation and control agendas. While leaders are often good at thinking about the business strategically, they sometimes fail to see how they can use risk processes to their advantage.

What to live with

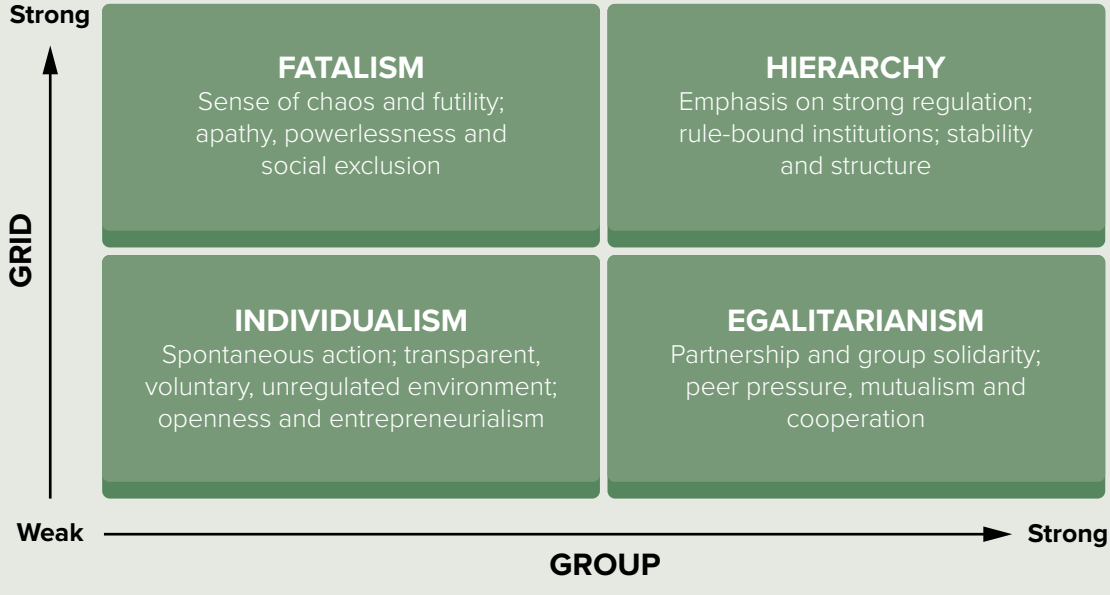
Phillips believes that most operational risks stem from a small number of the same internal and external systemic drivers. While organisations can respond to some of these issues, they may also need to recognise that they must live with others because they are a feature of the industries in which they operate.

She came to this conclusion because of the many root-cause analyses on operational risk failures that she has carried out. In brief, failure tends to originate from legacy technology that is complex and unreliable, disparate third-party relationships, poor data management and control practices, and lack of talent and capability. While the pandemic has certainly increased risk in all these areas – and will lead to more incidents arising from them – it did not cause them.

For example, the pandemic has prompted many people to re-evaluate their relationship with work, leading for some to drop out of the workforce. But, says Phillips, customer service experts, in particular, are crucial in managing many operational

RISK CULTURES WITHIN FINANCIAL SERVICES

Simplified model of multiple risk cultures that impact organisational decision-making



Source: Diagrams of Theory: Douglas and Wildavsky's Grid/Group Typology of Worldviews – Dustin S Stoltz (dustinstoltz.com)

and conduct risks. "Companies must work hard to ensure these staff are recognised and rewarded in line with their contribution to the organisation, its risk profile, and the customer experience."

"There comes a point where organisations either have to face these challenges head on and invest to correct them, or consciously commit to a more tactical approach to curb the amount of residual risk in the organisation," she says. "In other words – fund and fix, or live with events and failures of the same nature."

Resilience

Part of the impetus for this approach has come from regulation within the financial service sector that has made firms ensure their business services are resilient in the face of shocks and disruption.

Traditional operational risk management typically gives risk and controls equal importance, Phillips explains. Some risks may be assessed to have higher inherent exposure than others, or controls may be assessed as key or non-key. The Bank of England's operational resilience requirements have replaced a flat playing field with one that demands that firms formally prioritise their business assets and services in order of importance – not just based on their bottom lines, but in terms of potential customer and stakeholder harm.

For Phillips, this change of emphasis is a game-changer and one that she logically believes should apply to all sectors. It has forced firms to be clear on the type of disruption and detriment they would accept in a transparent way, with those decisions now communicated to regulators. "By contrast, operational risk tolerances tended to be more opaque, vague and open to interpretation. Not all business leaders used their risk appetite to spell out what they would accept and not," she says.

The first big test of protecting the business in line with resilience tolerances came when Phillips was responsible for complaints at Aviva. During COVID, customer-facing staff had to relocate to home working while continuing to maintain service. It was a huge project that needed to be tackled quickly. So, what should she prioritise? "In our sector, it made most sense to protect vital services for customers and regulated processes including complaints," she says. "A prioritised focus on the tasks and processes that really mattered was helpful during a time where everybody was really struggling." The resilience framework became a useful touchpoint in sustaining operations.

Storytelling

In light of the more unpredictable emerging risk landscape and the fact that operational risk is more focused on the values organisations attach to key assets, Phillips favours a strong element of storytelling in her discussions with management. That involves taking the relevant data and drawing out a narrative to ensure management is aware of what is happening

> **You can't create one culture and disseminate it throughout a business**

and the consequences that will flow from their various choices.

"Getting leaders thinking about the 'what if?', getting their brains going, is more important than having a beautiful set of documents as an output," she says.

Informed storytelling not only gets management thinking but also drives decision-making. That means building up a partnership with managers based on trust. For that to work well, risk managers need to be clear that their role is to facilitate decision-making, rather than supporting executives with, for instance, admin tasks and data entry – something she calls "risk butlering". "We all want to be helpful, but we need to remember that, like them, we are highly trained professionals," she says.

That professionalism entails being assertive with management that the risk role exists to facilitate those decisions – and to help them understand that not deciding comes with its own risks. She gives short shrift to those who want to kick an issue down the road by pretending to need more data instead of biting the bullet on a difficult choice.

"If people are not ready to make a decision, I do understand that," she says. "But I'm not prepared to perform analysis, create narratives, explain the options available to manage risk and then for the accountable people not to make a timely decision. That does not feel productive."

Organisational cultures

One of the key trends to managing risk in financial services firms – and organisations more generally – has been to focus on organisational culture. That has sprung from a realisation that without a supporting culture around risk controls, they are not effective. It was one of the key lessons that the sector learnt from the excessive risk taking that characterised the financial crash in 2007-2008.

Early in 2017, Phillips had become dissatisfied that while culture had become an increasingly important risk factor to measure in the industry, its core definition remained unclear. Organisations had responded by creating culture-based risk dashboards, but at the centre of that approach was a vague notion of what culture meant – largely because the Financial Conduct Authority (FCA) was unwilling to proscribe what cultures firms should adopt.

Not one for doing things in half measures, Phillips enrolled at the University of York as a PhD candidate to study the impact of risk cultures on decision-making. She was surprised to find little academic research on the topic and, working on the project part-time, quickly became interested in the work of one of the most famous British anthropologists of the 20th century, Mary Douglas.

While Douglas, like many of her generation of anthropologists, did her initial field work in ex-colonial countries – for her, the Belgian Congo (now Democratic Republic of the Congo) – in the 1960s she began to apply her observations on indigenous cultures to Western organisations. How institutions think, published in 1986, for example, used the sociological theories of Émile Durkheim and Ludwik Fleck to determine not only how institutions think but also the extent to which thinking itself is dependent upon institutions. Essentially, different kinds of institutions provide the cultural environment that allow individuals to think different kinds of thoughts.

Phillips realised that the theories of psychological bias in explaining risk decisions had failed to take proper account of how culture influenced those biases. Applying Douglas' insights (methodologically known as neo-Durkheimian institutional theory), to analyse risk culture in financial services firms revealed that organisations typically had not one single culture but a minimum of four different ones (See *Risk cultures within financial services*). Phillips' mixed-method findings in FTSE100 companies backed the theory up.

Implications

"I wanted to look specifically at the impact of risk culture on the appraisal of risk and types of management interventions," she says. "As expected, I identified four distinct cultures, each with subtly different attitude to risk and risk-taking in each team studied. The implications of the theory is that executives looking to create a single risk culture across their organisations will struggle, because organisations are sustained by multiple dynamic cultural forces. You can't create one risk culture and disseminate it throughout a business."

In fact, Phillips says that organisations can benefit from moderated dissent and contrasting views to stabilise the organisation and create value. Douglas' theory says that a single risk culture that becomes too prominent can destabilise or stifle the organisation. Phillips found such dynamics at work in both global institutions and groups as small as 20 people.

Since the decisions leaders make are always influenced by the culture they are in and by the types of conversations that they are having with other stakeholders, Phillips' research raises important questions about regulatory accountability. For example, how far can a leader really be in control of the culture of their organisations? How far are individual decisions really based on the individual concerned – and how far do they derive from the cultural mix that exists in the business?

Phillips emphasises that her research aims at explanation, not prescription. Chief risk officers have asked her what balance of each culture they should they strive for in their organisations.

> **We need to keep trying to break down any preconceptions about the type of person that can join the risk profession**

From the choice between fatalism, hierarchy, individualism and egalitarianism, perhaps risk professionals tend towards hierarchism – it has clearly defined roles and a structured approach to risk management that aims to protect long-term value.

"Certainly, as a risk practitioner, the hierarchical culture feels most comfortable but is unlikely to permeate all levels of an organisation," she says. Phillips argues in her thesis that ERM frameworks are hierarchist in nature, so they do not naturally align with other cultures like individualism. This can impact levels of embedment.

Her research also highlights that individuals hold both an espoused perspective and an honest perspective about risk manageability and risk frameworks. Risk managers might not always hear what others really think about their efforts to embed risk and control management, but it is important to seek and embrace differing opinions. "The fatalist's mindset might not sit well with a risk manager's objectives, but in fact, some of the time they might be right".

Diversity in risk cultures

While Phillips says she enjoyed sitting for her IRM Diploma, her work on the PhD has been both hugely stretching and rewarding. She recommends it, but only for those who are prepared for the commitment and sacrifice it necessarily demands. "If you don't believe that your contribution is necessary to the field, you literally won't have the resolve to spend six years writing 80,000 words," she says.

Phillips moved into risk after the financial crisis in 2007-2008, when she was working in marketing in New York. The idea of protecting the business and customer from future harm became a very rewarding one – a practical mindset that is unlikely to see her moving into academia at this stage in her career. But she says the move into risk from marketing was not without its detractors in her personal life, something she believes has something to do with the representation of people in the risk profession.

"We still need to do more to attract diverse young talent to the profession. And once they are there, ensure all participate and are heard," she says. "There is a tendency to revert back to particular archetypes. I always look at who in organisations is perceived as credible and carries influence, even as part of a diverse group," she says. Phillips was a head of risk by the age of 30 and while she has found that diversity in mid-senior to lower levels of the industry has improved, there is still a lack of diversity in the most senior roles and she is passionate about helping to bring about this change.

"My research highlights the need for diverse voices to avoid blind spots," she says. "We need to keep trying to break down any preconceptions about the type of person that can join the risk profession: so you can have a marketing background, you can have an arts or science background, or you may not have a degree." And if risk managers are to successfully attract the right talent to diversify their operations, they will need to get a better grip on how well their unique mix of risk cultures support risk decision-making in the business.

Grand designs

BY ARTHUR PIPER

IRM's new strategy aims to support organisations when the need for effective risk management is at an all-time high, at the same time as setting ambitious targets for growth and influence

It has been a busy time at IRM since 2015. That was when José Morago, chair of IRM's board, led the organisation through one of its periodic strategic overhauls. After an extensive consultation with members and other stakeholders, the board decided to focus on internationalising the Institute and expanding its suite of qualifications and training to reflect the increasing professionalisation and globalisation of risk management.

Over the past seven years, not only has IRM established and strengthened regional interest groups and affiliate partnerships in Africa, Asia, India, Latin America and North America, it has also refreshed its core qualifications and added several new ones in areas such as supply chain and digital risk management. Significantly, a merger with the Institute of Operational Risk (IOR) in 2020, further boosted IRM's international standing and deepened its offering to the members of both bodies.

In autumn last year, shortly after Stephen Sidebottom, IRM's independent non-executive chair, joined IRM, the board decided it would be a good time for a strategic refresh. Not only has enterprise risk management matured and spread its reach far beyond its traditional base in regulated industries, such as the financial services sector, but the world is a radically different place.

Changing world

Large-scale global risk events such as the pandemic and conflict in Ukraine have arisen at a point in time when longer-running trends, including climate change, digitalisation and resource scarcity, are beginning to bite hard. The MeToo and Black Lives Matter movements have pushed discussions about equality and diversity onto boardroom agendas, and the pandemic has loosened many people's relationship with their employers just when businesses are scrambling to attract and retain the right talent.

> **"Risk event experiences over the last couple of years have really brought risk management thinking home to people**

"Risk event experiences over the last couple of years have really brought risk management thinking home to people," Sidebottom says. "Organisations, boards and leaders are so much more aware of how they should be thinking about risk, and the importance of risk intelligence for creating a sustainable, forward-looking organisation. That is not just about the pandemic but about the world's unpredictability and volatility."

Sidebottom led the current strategic review process for the board hoping to capture what these trends and the increasing maturity of the risk profession means for members and the Institute. After a three months of extensive consultation with members, the executive team and key stakeholders, he presented a top-level briefing of the new strategy at IRM's AGM in December.

"The process has been extremely valuable because we now know where the board wants us to go given the very different world we live in today," Sidebottom says. "And our extensive conversations with members and others have given us a much deeper understanding of their needs, what they value and where they believe the opportunities are for IRM to create value."

New strategy

The new strategy comprises five inter-related pillars (see *IRM's five strategic pillars*): creating world-class education and qualifications, elevating the membership offer, creating impactful global thought leadership, building international collaboration and partnerships, and remaining financially sound.

"In the new strategy, there is a re-doubling of focus towards internationalisation," Sidebottom says. "We see that as a significant opportunity for IRM to contribute to effective risk management, and an opportunity for us to grow our membership, revenue and impact."

> **We see a significant opportunity for IRM to contribute to effective risk management, and an opportunity for us to grow our membership, revenue and impact**

A challenge will be to engage with a wider range of people who are trying to become risk savvy. That entails being more focused about articulating the value risk management adds, not only in its traditional areas of downside risk and compliance, but in helping to enhance future business performance.

"While we have been active, we need to communicate that value in a clear and compelling way across a wider constituency (not just risk professionals) – to leaders who want to create a risk-intelligent culture within their organisations so that they can understand and think about risks and decision-making in a more dynamic way," he says.

Stephen Sidebottom is IRM's independent non-executive director

More tailored offering

IRM already has a suite of highly regarded, internationally recognised qualifications. To remain world class, the Institute will make those offerings more targeted and responsive to the specific question of managing risk in today's more complex world. In addition, says Sidebottom, the board wants to consider what it can offer non-risk professionals and those risk professionals operating in regions or sectors with a less developed understanding of what risk management can provide.

Over the past 18 months, the Institute has been working with Ofqual, the qualifications regulator, to achieve accreditation for its existing educational products. It has submitted the final batch of papers for the process, and a decision should come this summer. "While it is a UK accreditation, it matters to us and members that they are of demonstrable status as we continue to internationalise and grow," he says.

Not only will the content and status of qualifications and training be renewed, but so will the way members engage with their life-long learning journey with the Institute. That goes beyond continuous professional development to encompassing how people want to grow in their role, develop new expertise and leadership competencies, and learn from other people. Over the past two years or so, the pandemic has driven the Institute to accelerate its digital and hybrid education delivery platforms and develop more flexibility and modularity in how members can engage and manage their learning.

While that has been a good start, more needs to be done. "The new strategy will help us understand how people make choices in their learning journey, how they can have more agency regarding their engagement with us, and what things they need us to support them with," he says. "That represents an important change in emphasis so that we are not selling products to them, but instead understanding their needs at different stages of their careers. We need to be able to offer members a package of life-long learning tools, and connections and communities that support them with the things they need at the time that they need it."

Communities

The Institute's burgeoning network of communities, which are organised around national, regional and specialist interests, are at the heart of the strategy. Currently, for example, a local community creates networking

opportunities and provides an all-important sense of belonging for members. The board wants to move towards automatic enrolment for new entrants into local groups so that they feel welcomed and included from day one. In addition, there may be an opportunity to created elected leaders, if members feel that would be beneficial.

The Institute is also looking for ways to simplify the membership structure. Sidebottom says it should be clearer how people can move through the system and access membership through professional experience routes. There also needs to be a better way of integrating IOR and IRM designations and perhaps a simplification of the classification of members as students, affiliates, members and associates to make the system more transparent and comprehensible.

Engagement

Engagement with external stakeholders will be refreshed to improve the impact of IRM's thought leadership. Currently, groups focused on sectoral specialisation tend to provide members with an opportunity to learn from and help create forward-looking thought leadership for the profession and beyond. Recently, the Institute has been partnering more frequently with organisations to create work of greater depth and insight. For example, IRM and the Grantham Institute at Imperial College London have partnered on climate change risk management training.

Such collaborations in future should enable IRM to partner with larger groups of people in both academia and business to improve the scope and quality of its thought leadership.

IRM'S FIVE STRATEGIC PILLARS

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

In fact, the Institute is also conducting a governance review and, as part of that process, expects to set up a global advisory council to bring world-class risk professionals, practitioners and thinkers together both as a voice and consulting group for IRM. It will provide experts and risk leaders with a way of supporting the Institute without sitting on a formal governance board. In addition, IRM expects to appoint another independent non-executive director soon.

Ambition

The board has set ambitious targets for significant growth. The Institute aims to double membership over the next three to five years and achieve double-digit annual compound growth in revenue from 2023 onwards. At the same time, there will be ongoing investment in its digital capabilities.

Currently, about half of new members work in UK-based organisations and half join from other countries. The strategy sees a larger proportion of new members coming from its international base as the communities that it has established since 2015 continue to grow in size and influence.

Sidebottom expects initiatives in the Middle East, sub-Saharan Africa and Asia, especially Hong Kong and Singapore, to be an early focus. In addition, IRM's affiliate in India has been busy laying foundations and creating relationships among professional and governmental bodies, which is likely to help to deliver strong results in increased membership and educational activity.

Financial stability

The Institute is in a much stronger financial position than it was five years ago. One challenge will be to continue to digitalise and extend its offering while achieving its target revenue growth. Sidebottom admits investment and expenditure need to be carefully balanced. The creation of a specific consultancy arm, IRM Advisory, should help. This business line essentially formalises, broadens and deepens the Institute's existing bespoke corporate offering.

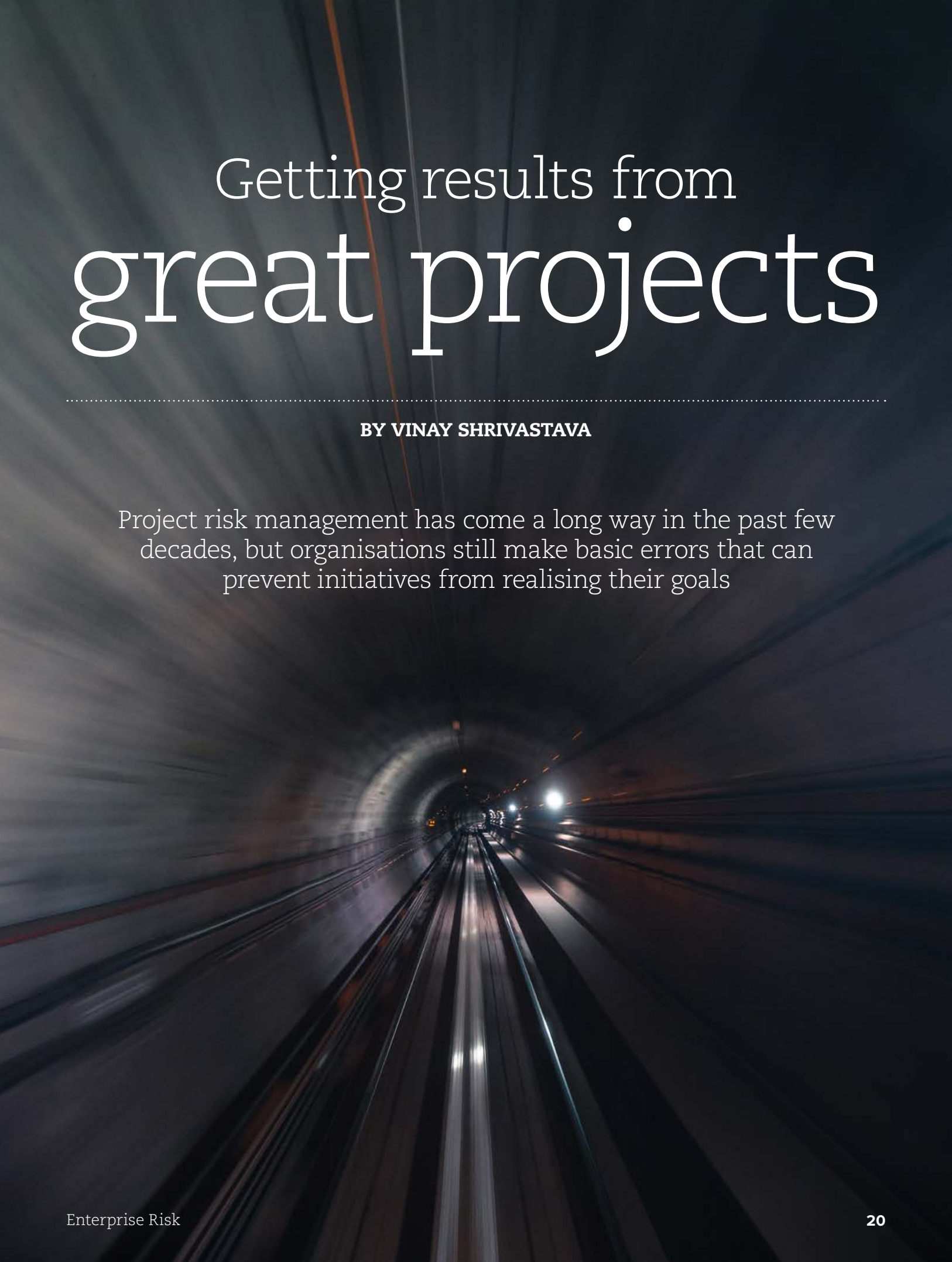
The five pillars of the strategy are, in reality, a closely interrelated set of initiatives. They take IRM's unique perspective on risk out to the world, at the same time as opening up the Institute to a wider range of international members and collaborations.

"We need to be able to offer members a package of life-long learning tools, and connections and communities that support them with the things they need at the time that they need it

Getting results from great projects

BY VINAY SHRIVASTAVA

Project risk management has come a long way in the past few decades, but organisations still make basic errors that can prevent initiatives from realising their goals



All organisations undergo change, and projects and programmes are the typical vehicles that deliver transformation to an organisation. In the current global climate – increased geopolitical risk, pandemic disruption, supply chain uncertainty, skill shortages and runaway inflation – major project teams will benefit from more investment in better tools and improved skills for managing increased levels of risk and uncertainty.

This article is a meditation on risk management drawn from over two decades of working in defence, nuclear, rail, aviation, utility, manufacturing and financial sectors in the UK and internationally. These projects typically ranged in value from tens of millions to tens of billions of pounds sterling, and gave me access to varying approaches to risk management that were adopted due to sector, project stage and/or project scale. There was a lack of consistency in the definition of what constituted best practice risk management in these projects and a notable disparity in risk management maturity among the sectors in question.

Specifically, there are a few areas where organisations can do better. Although these observations are not necessarily new, they are often overlooked and can significantly improve the agency of risk management within a major programme or organisation.

Risk and reporting

Multi-million-pound programmes are often delivered without qualified risk professionals to oversee the risk management process. For example, it is quite common practice for organisations, due to cost-efficiency reasons, to rebadge a project manager or other project professional to serve as a risk professional in order to satisfy the audit team or a client. On closer scrutiny, it is usually the case that this person has had no formal training in risk and is insufficiently aware of sound practice standards. Unsurprisingly, such programmes perform poorly from a risk management perspective.

On the other hand, it is encouraging to see many critical national infrastructure programmes recognise the need for managing data effectively and make investments in online databases. But there is still a minority that continue to manage risk on major programmes (worth hundreds of millions of pounds) with Excel spreadsheets. Data management on Excel leads to inconsistent data capture and makes the collation of programme-wide exposures a daunting, labour-intensive task that is prone to error. It is also difficult to extract systemic insight from a motley collection of disparate spreadsheets. Consequently, a programme may not benefit from an understanding of pan-programme risk trends, risk clusters and systemic risk across projects.

A major infrastructure project can easily generate hundreds or even thousands of risk items. Senior management can quite easily be overwhelmed, so much so that a top-down view of risk is created that is more convenient and accessible than it is correct. This is frequently the case when the volume of bottom-up risk data is outside of the appetite for detail of senior management.

Therefore, a key role of the risk management professional is to extract the insight buried within a risk database and bring to the surface trend intelligence that will effectively inform senior management decision-making. Put simply, it is not sufficient to report the top five or ten risks. Systemic risk trends or risk clusters against a theme of interest are just as important and more insightful. Therefore, it is especially important that any risk database is designed to be interrogable and include references to work and risk breakdown structures. Further, automated dashboards that are capable of collating huge volumes of data to executive-ready reports should be explored to their full potential.

For executive reports, less is certainly more. Some years ago, I reported to a retired colonel who was the chief executive officer on a major defence project. His advice was to limit an executive risk report to a single page of A3, and in an easily readable font size. This advice, together with notes from Winston Churchill's Second World War Brevity Memo,

> **“ There was a lack of consistency in the definition of what constituted best practice risk management in these projects**

> **Data management on Excel leads to inconsistent data capture and makes the collation of programme-wide exposures a daunting, labour-intensive task that is prone to error**

has helped me to better engage with executive leaders. Churchill's memo is timeless and can be usefully paraphrased: if a report relies on detailed analysis of some complicated factors, or on statistics, these should be set out in an appendix; and often it is best to submit not a full-dress report, but rather an aide-memoire consisting of headings only, which can be expanded orally if needed.

Approaches to risk

It is not uncommon to see risk professionals preoccupied with project objectives – are we delivering the project right? This can be more helpfully rephrased as follows: are we delivering the project to cost, time and expected quality? Arguably, risk management should take a portfolio risk management approach by extending this view to the portfolio level where it can answer this question – are we delivering the right project? Not many organisations have a consistently employed tool that tests every candidate project against the organisation's strategic objectives. This may lead to an agreed portfolio of projects and programmes that are strategically misaligned to the organisation's goals. In the end, such organisations can end up with projects delivered to cost, time and desired quality but with a significant underrealisation of planned benefits.

Assumptions management is certainly another area where organisations in all sectors can improve. All projects are based on assumptions because projects are conceptualised, designed, procured and built on incomplete or uncertain information. The making of assumptions is a necessary feature of project delivery. A mature project delivery team should have a comprehensive register of assumptions that are assessed for sensitivity and stability, so that risks may be raised for less robust items. Put differently, the integrity of a risk management process is strongly correlated to the integrity of the capture, assessment, validation and review of assumptions.

Opportunity management often receives less attention than it should. It is generally accepted that human beings are psychologically hardwired to be risk averse. This means that, from a behavioural perspective, we find it easier to prevent loss rather than to exploit potential gain. Project risk registers, therefore, are heavily weighted towards threat articulation. As a result, opportunities tend to be few and are less clearly defined than threats. Project teams may improve the yield of opportunities by having separate, dedicated workshops for opportunity identification. This is because, generally, project team members do not oscillate effectively between thinking about things that can go wrong and things that can go right within the confines of a single threat and opportunity workshop. Project teams will also more readily declare opportunities if they receive assurance that opportunities won't be banked by senior management until they become realistically achievable.

Most programmes are geared towards managing risk in the delivery stages of their projects once the contract has been signed with a supplier and execution begins. This is perhaps borne from a longstanding commercial view that risk management is synonymous with supply chain contract management. Project

Image credit: William Warby / Unsplash.com

NINE STEPS TO SUCCESS IN PROJECT RISK MANAGEMENT

1. Ensure that you have the right person in the right role
2. Use a structured, interrogable database for risks
3. Publish "bottom-up" driven insight in concise reports
4. Adopt a portfolio risk management approach – is this the "right" project?
5. Declare, assess and review assumptions
6. Hold dedicated opportunity workshops
7. Embrace the language of uncertainty
8. Ensure that your risk management process is scaled to your needs
9. Tell stories to improve risk management culture.

> **Storytelling is more effective at influencing individual behaviours than a 60-page risk management procedure**

teams can also help their project leaders with making better decisions through the deployment of risk management at the "go/no go" and option selection stages of a project. Levels of risk management scrutiny, tools and processes need to bend towards the complexity and scale of projects being delivered. A significant waste of resources can be incurred if all projects are treated as equal within an organisation.

Language and culture

It is often an act of self-harm for project leaders to offer single point estimates of cost and schedule forecasts to stakeholders. Unfortunately, there are still numerous examples of executive hubris leading to unjustifiable levels of optimism in project forecasting. This is particularly problematic at the early stages in a project's life cycle when there is the most uncertainty. While it is the norm for reporting forecast performance ranges in certain sectors (rail typically), technology sector projects don't often subscribe to embracing the language of uncertainty where it is needed.

A mature and effective risk management culture is one in which all team members feel empowered to think critically and feel responsible for managing risk – not just those team members with the word risk in their job titles. Such a culture needs to be nurtured through continuous training and education. Here, senior management have a role to play. They need to "cast the right shadow" on the process by ensuring that risk gets a platform at all leadership meetings. Equally, senior management should aid organisational learning through the storytelling. They should tell stories of failure, of lessons learnt and of controls that have prevented crises. Storytelling is more effective at influencing individual behaviours than a 60-page risk management procedure. To further drive team accountability and improve the culture for risk management, the owners of risks (and not the risk management professionals embedded within the team) should also take responsibility for reporting risks and defending control plans with senior leaders.

Programme and project risk management has come a long way since I started my career over 25 years ago. There have been significant improvements in quantitative risk analysis, reference class forecasting, risk data systems, the use of artificial intelligence and in the recognition of risk management as a legitimate profession. I still recall the start of my career in the late 1990s when risk management was largely seen as an administrative service. There have also been encouraging developments in education and certification from the Institute of Risk Management and other organisations that have helped raise the standards of practice in the UK and internationally. Further, major project performance has attracted academic interest, and there is now a wealth of publications that help share knowledge, drive innovation and continually raise the profile of risk management.

I am genuinely excited about the future of risk management in major projects and programmes and look forward to working with, and learning from, the next generation of risk management professionals.

Vinay Shrivastava, CFIRM, is head of risk for the New Payments Architecture Programme for Pay.UK, and IRM board director.

Building competency

BY WESLEY CADBY AND STUART HARRISON

Designing and launching a competency development framework for risk management at the Nuclear Decommissioning Authority helped it assess whether it had the right capabilities and provided some valuable insights along the way

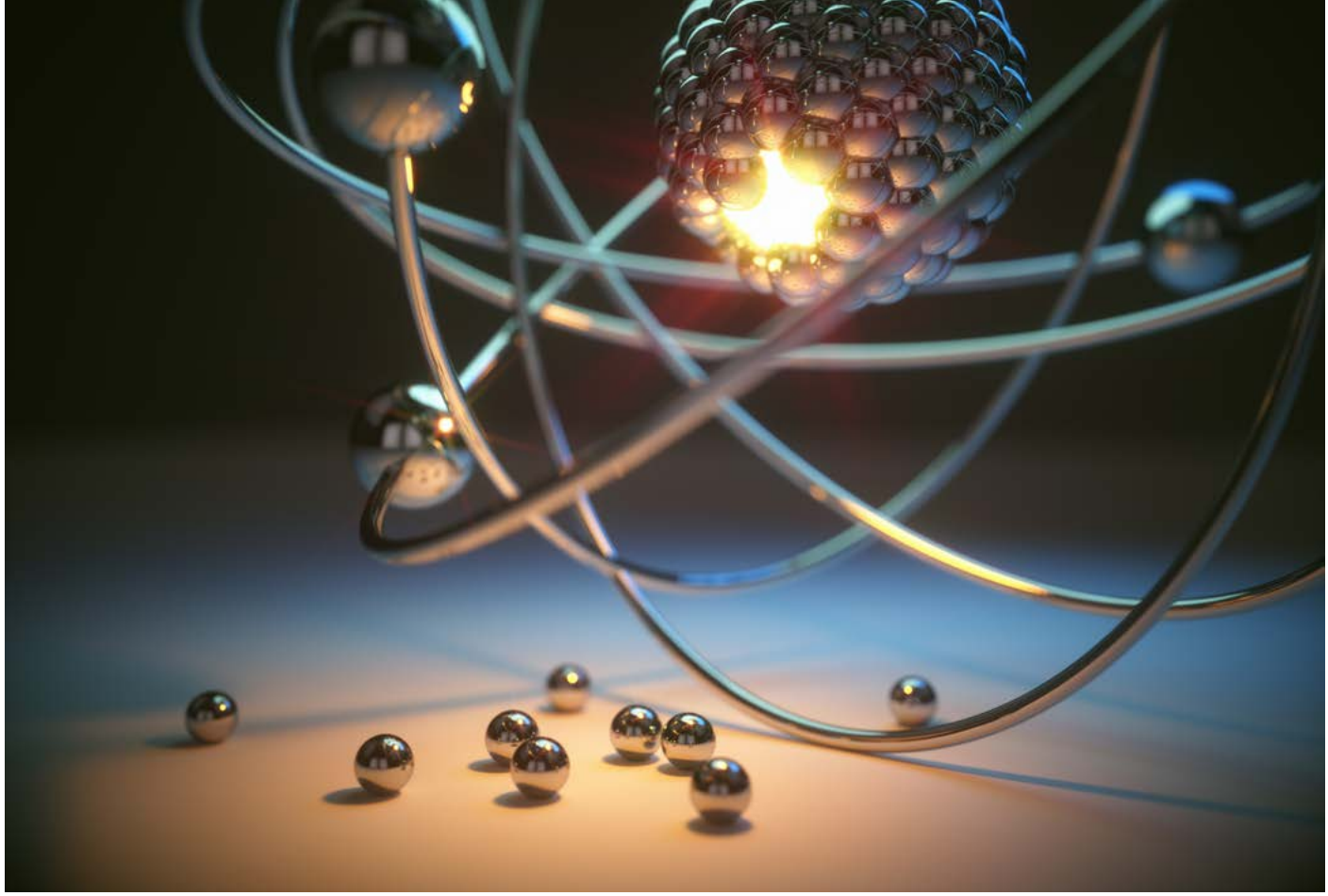
Does your function have the capability to fulfil the organisation's mission? This question was posed to the group risk and assurance leads of the Nuclear Decommissioning Authority (NDA), by their executive governance. At first glance, this is a simple question, and yet the more one considers it, the more complex the question really is. How do we define capability? What capability do we need? How do we capture it and measure it? How do we know our definitions are suitable for current and future use?

In March 2021, a project was initiated to define a set of competencies suitable for the risk and assurance function across the NDA. As a group of companies, wholly owned by the NDA, a public body, any capability definitions had to work across multiple different environments, from nuclear decommissioning projects to transport services and liabilities management.

The decision was taken early in the project to engage with external specialists who had experience of designing and implementing competence frameworks in both nuclear and other infrastructure-based large project organisations. This turned out to be a very good decision in hindsight and brought benefits to the project which could not be anticipated at the launch.

In establishing the scope for the project, the first question was whether to address risk management and assurance in a combined framework, or to address them separately. Organisationally, they are two separate functions within the NDA; however, early discussions confirmed a combined approach would bring significant benefits. The aims for both functions were the same, and the technical skill set was thought to have some commonality and overlap, even if this turned out not to be the case once defined. In fact, on completion, the common ground was much

> **The framework would focus explicitly on the technical knowledge and application required, acknowledging that this differs depending on whether a professional is a practitioner, manager or senior leader**



> **Defining principles for design and implementation allowed the project to move forward in a very clear way**

greater than anticipated.

It was also recognised that many organisational competence frameworks strongly focus on the behavioural and leadership requirements of roles. For this project it was specifically recognised that this work would not be repeated, and that the framework would focus explicitly on the technical knowledge and application required, acknowledging that this differs depending on whether a professional is a practitioner, manager or senior leader.

Developing the framework

When the external specialists were engaged, we were clear on what we wanted: a technical competence framework for our risk management and assurance professionals. We even provided an example, thinking the main support was in polishing this and designing an implementation process. By the end of the project, we did indeed have a robust technical competence framework, covering risk and assurance; however, it looked nothing like our early draft.

There is a particular nuance of developing competencies for the nuclear industry. Some of the operating sites are bound by law under what is referred to as the Nuclear Site Licence. This licence comes with 36 conditions, one of which specifically requires the licensee to demonstrate that the site has suitably qualified and experienced persons. Therefore, these operating companies already had established means of demonstrating competence.

For the purposes of capability, these arrangements did not fulfil our needs. They demonstrated that individuals were competent to do their current role (the legal requirement) but didn't necessarily cover future needs of the organisation in totality. Furthermore, not all parts of the NDA group operate under a site licence. In designing our arrangements, we had to ensure they didn't contradict and in anyway conflict with the legal requirements imposed by the site licences and at the same time provide a consistent group-wide approach.

Our specialists worked with us from the outset to understand exactly what we wanted and meant by capability. They concurred that a competence framework was a fundamental part of any capability definition and development programme. It also became apparent that the framework should be defined in a way which meets future needs, not just current needs.

> **In the worst case, they would overestimate their competence and therefore miss out on development opportunities**

For example, competencies around data analytics and opportunity framing were included, as new developments within the profession.

Design principles

In believing from the outset that we already had a suitable draft competence framework, we potentially underestimated the time required to design the framework. As the team formed, including the external support, they challenged us to take an almost engineering approach to the design. Step one: establish design principles.

They took us through multiple questions about what we wanted to achieve and why, constantly referring to the purpose. Over a few weeks, we established more than 25 individual design principles. These considered not just the risk and assurance goals, but the human elements of using a competence framework, such as how competence assessment would happen, what data was required, what we would use the data for, how it would be collected and what implications this might have on data protection. It required identification of several stakeholders across the organisation including the human resources and information technology teams as well as owners of site licence competence systems.

Defining principles for design and implementation allowed the project to move forward in a very clear way. Whenever challenges were presented, they could be tested against the principles, and this allowed decision-making based on alignment to the principles not just personal opinion.

Principles included, for example, that competencies need to be equally applicable across multiple sites and contexts; competencies will be primarily used for developmental purposes, assessing the capability across the sites and to support future portability; and competencies are to be defined for the future state to ensure it remains current, which means the levels of competence for some could be low.

To actually identify, define and produce descriptions for each technical competence, we approached this part of the project in a structured way, gathering all existing relevant competencies from across the organisation as well as looking externally at relevant professional bodies and institutions. This included the Engineering Council, Infrastructure and Projects Authority, Major Projects Association, Association of Project Management, Institute of Risk Management and Airmic among others.

Once the first draft was produced, our specialists were able to share and socialise the competencies with industry experts, to make sure the structure was appropriate and competence definitions were clear. We received extremely positive feedback from the external experts, noting in many cases that we had defined a useful, class-leading level of detail not seen in other professional frameworks.

Having had this external input and view helped significantly during the launch phase of the project when briefing staff. It added a credibility by association and quickly allayed any fears about its usefulness. The fact that the competencies aligned to external professional standards allowed the potential users the comfort that by developing themselves against these new competencies, they were actually helping their professional status as a whole.

As with the design phase, implementation principles were also captured. These were key to shaping the implementation processes and data flows, as well as developing data protection impact assessments.

Put slightly differently, 80 per cent of the effort in the project will never be seen by the user of the competency framework and associated development tools. It is all internally focused within the project team. Care had to be given to deliberately consider what the user will see, feel and experience.

Assessment

One of the most interesting challenges in the implementation process design was focused on who carries out the assessment of competence, and what evidence, if any, is required to support it. As a naturally risk-averse and process-intensive industry, the nuclear sector usually has lots of independent checks and balances. The initial assumption was that any assessment of competence would at least involve the line manager, and potentially a moderation panel.

However, this is where the design principles came into their own, along with the experience of the specialists that had been engaged. They tested the thinking that independence and evidence were required by taking us back to the design principles. The whole project was about underpinning capability not confirming if someone is competent to do their current role or performing in it – other processes existed for that.

It also became apparent that structurally, not all risk and assurance professionals reported to other professionals of the

same discipline. They may in fact report to project professionals for example. So, what would make the line manager any more competent to assess the technical competence of an individual?

In considering the implications, it was quickly realised that there were no safety and financial consequences of an individual "scoring themselves" wrongly. In the worst case, they would overestimate their competence and therefore miss out on development opportunities.

The result was a simplified process, based on self-assessment, with the emphasis going into the launch briefings to explain the benefits of self-assessing accurately. While this approach was culturally novel and sat a little uncomfortably at first, the message became clear that "we trust you to assess yourself, but if you need help, we can provide it".

Launching

In launching any new arrangements, there is always an element of selling the concepts. This framework was no different. We were introducing five new technical competence groups: shared strategic, shared tactical, shared technical, risk technical and assurance technical. Below these sit a total of 33 sub-competencies. In asking all risk and assurance professionals (more than 100 people) to assess themselves against them to get a full measure of capability, we were potentially placing a significant burden on them.

To help with this, we tested the competencies and assessment process, capturing how long it took to complete (typically 30 minutes to an hour), common areas where additional understanding was required and any issues. Every one of the comments received during testing was responded to and used to shape launch briefing materials and documentation.

Ultimately, when a process like this is brought into any organisation, the benefits must be clear. In this case, there are three levels of benefit: to the individual, to the risk and assurance function and to the organisation as a whole.

These benefits were identified early on, kept in focus through the duration of the project and articulated clearly and simply in launch documentation. They were key to the success of the project, to allow key stakeholders and senior leaders to buy in and support the project, as well as ensuring that user support was gained throughout its development and, ultimately, its launch.

Time well spent

From a project perspective, the main learning point related to the anticipated duration. Our initial thoughts were that this could be developed and launched quickly, especially as we had created an early draft.

In engaging external support with expertise in doing this before, we were shown very quickly what we did not know. Although the level of effort overall was not high, time was needed to take questions away that were presented to us, work them through and make decisions. It was this reflection time needed to properly consider these questions that resulted in a much longer duration (nearly three times) than we had anticipated.

It has resulted in a well-thought-through, externally credible and robust set of definitions of competence that all allow us to answer the question, does our function have the capability to fulfil its mission? ER

KEY LESSONS LEARNT

- In addressing capability for risk and assurance professionals within a large organisation, having a combined framework makes sense and brings significant benefits
- To underpin capability requirements, a new future-focused technical competence framework was required
- Developing design and implementation principles was key to a meaningful competence framework
- Aligning technical competencies to external standards creates credibility for the user audience
- Develop key process elements in a way that minimises implementation disruption
- Clearly state the individual, functional and organisational benefits from an early stage.

> **"When a process like this is brought into any organisation, the benefits must be clear**

Wesley Cadby, CFIRM, is group enterprise risk lead at NDA, and Stuart Harrison is managing director at Solar Flare.

International Certificate in Enterprise Risk Management

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

About the International Certificate

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

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

What our students say

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

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

Find out more at:

www.theirm.org/erm-mag

Resilience, risk and recovery

irm
Developing risk professionals

Digitalising the supply chain

BY NICK WILDGOOSE

Making supply chains more resilient and environmentally sound requires building and implementing a robust and responsive digital infrastructure

Extensive research by the analyst McKinsey suggests organisations' supply chains will face disruptions lasting a month or longer every four years. In this same report, *McKinsey Global Institute: Risk, resilience, and rebalancing in global value chains*, August 2020, it calculated that organisations across a range of industry sectors can expect to lose almost 45 per cent of one year's profits over the course of a decade, based on probabilities of existing patterns of current disruption events.

In addition to these losses, there is also the potential further loss caused by reduced market share following a disruption. In fact, organisations often do not understand their financial exposure to a particular supplier production facility or a logistical hub and have thus suffered unexpected major profit and cash flow impacts.

COVID-19 has been a further reminder of the fact that most organisations depend on having a resilient supply chain to be able to serve their customers. In fact, some businesses now compete based on the strengths of their supply chains. It is therefore critical that organisations invest the appropriate amount of resources to ensure they have the right level of supply chain resilience.

This focus on supply chain resilience needs to be driven from the top of the organisation. It must recognise the significant overlap with supply chains and the need to address climate risk from a business performance perspective in terms of the joint requirement they must drive supply chain transparency. It also needs to ensure that the appropriate level of investment is available and that the initiative is driven forward on a cross-functional basis in accordance with an agreed overall business plan.

In preparing for the future in a post COVID-19 world, organisations will need to restructure their supply chains, and in doing this it will be critical to consider risk appropriately. This is about not only pandemic risk but also the ongoing financial,

COVID-19 has been a further reminder of the fact that most organisations depend on having a resilient supply chain to be able to serve their customers

geopolitical and climate risks that will be faced by these organisations' supply chains.

It is important that these supply chain risk management efforts are appropriately integrated into those supply chain digitalisation activities that are also being progressed. As we move forward, the use of innovative technology and data sources offer a significant opportunity to drive forward improved supply chain resilience and sustainability in a way that also improves overall financial performance.

Changing risk environment

Supply chains continue to face a combination of different risk drivers such as those related to COVID-19, climate change and increasing geopolitical tensions such as the Russia and Ukraine conflict. Many of these top risks are interlinked, demonstrating the growing vulnerabilities and uncertainty of our highly globalised and connected world, where actions in one place can spread rapidly to have global effects.

The World Economic Forum (WEF) Global Risks Report 2022 (see *WEF global risks*) shows the most severe risks on a global scale over the next 10 years, many of which have strong correlations with supply chain risk. Many respondents (42 per cent) to the report – answering before the war in Ukraine – also said that they expected to be working in a volatile environment that was full of surprises.

The investment community is also taking a much closer look at an organisations' supply chain and how this is being managed from an overall business performance perspective. BlackRock's CEO, Larry Fink, announced that sustainability would be at the centre of BlackRock's investment practices in his annual letter in January 2020. Fink, whose business has about $7 trillion in assets under management, called on every government, company and shareholder to confront climate change as a unique and material financial and investment risk. You cannot tackle climate change risk without considering your supply chain, which usually represents the largest part of your overall carbon footprint.

Starting out

It can be challenging to get your supply chain resilience programme either off the ground or supported with the right level of investment, even though COVID-19 has helped move this to the top of many corporate agendas.

Organisations should focus on three key areas initially. First, they need to make a business case for supply chain resilience (see *Making the business case for supply chain resilience*).

Second, they need to obtain top-level management support. This should follow the acceptance of the business case and the establishment of appropriate corporate-wide metrics that encourage appropriate collaboration in the supply chain to optimise business performance (see Michael Rasmussen's article *Relationship trouble, Enterprise Risk*, Summer 2021). The alignment of objectives is important in

MAKING THE BUSINESS CASE FOR SUPPLY CHAIN RESILIENCE

There is nearly always a compelling business case to be made for implementing a supply chain resilience programme; the benefits that can be realised include:

- Avoiding or mitigating major supply chain disruption events protecting cashflow and profitability
- Understanding low-level disruptions and eliminating them over time. For example, avoiding increased air freight costs by switching to sea freight
- Saving staff costs from the time taken up to deal with disruption events and monitoring potential risk events (where appropriate technology solutions are implemented)
- Avoiding potential cost variances in obtaining replacement components or raw materials and inventory optimisation using improved data
- Developing supply chain transparency to protect brand value and loss of customers due to supply chain reputational damage caused by environmental, social and governance issues
- Avoiding regulatory fines, the threat of which are growing from increased levels of legislation.

> **"You cannot tackle climate change risk without considering your supply chain, which usually represents the largest part of your overall carbon footprint**

ensuring that the functional silos such as procurement, finance, operations, sales and risk are all pulling in the same direction and providing a common message to key supplier partners. The case can also support investment in, for instance, a technology and data solution to enable you to scale up for the number of risks and suppliers that you will need to monitor. The executive team can then also ensure that functional objectives are appropriately aligned so that overall business performance is maximised through adequate and aligned supply chain resilience performance indicators.

Third, organisations must overcome their silos with a clear supply chain risk governance structure and bring in a "black-box thinking" culture. This is a culture where there is appropriate transparency around the issues that are arising in the supply chain and the lessons that can be learnt to avoid them happening again. For example, the airline industry's black-box thinking approach ensures any near misses are reported to encourage learning and improvement.

Rollout

When you start to implement your improvements in supply chain resilience, or look to expand them appropriately, one of the challenges can be to determine which is the product or service supply chains on which you should focus. From a business performance perspective, this should be that product or service that contributes most to your profitability.

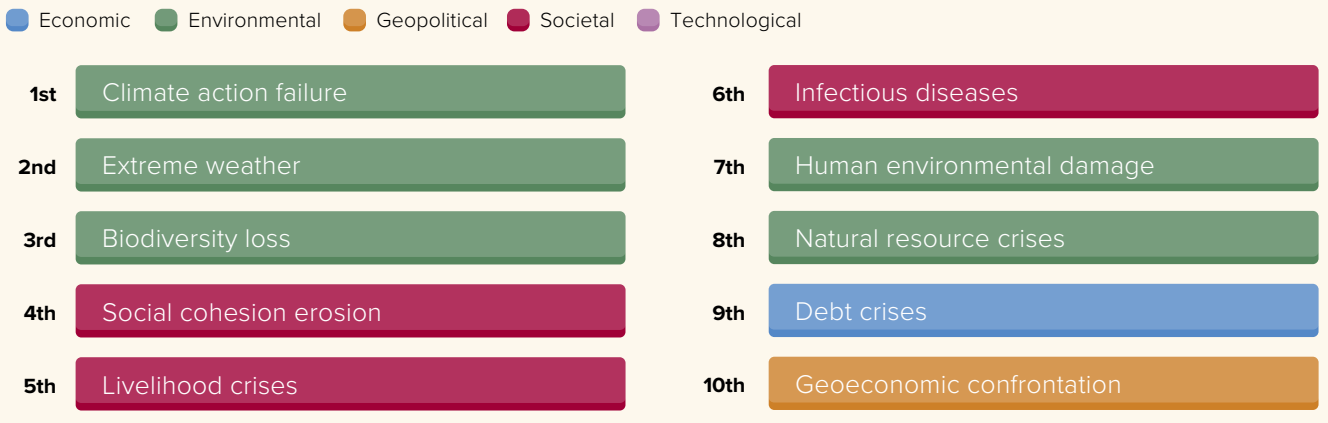
> **The key to technological solutions is that they provide actionable risk insights**

It is important when you are evaluating the risk factor information relevant to the supply chain that you take a comprehensive risk approach to the supplier and supply chain evaluation. At least consider what factors are relevant to a supply, supplier and supply chain. For example, what are the natural catastrophe or geopolitical risks to the supplier's production or service site, or the key logistics hubs required to get the product to the end customer? From a supplier's perspective consider their financial solvency, ownership, cybersecurity, health and safety, corporate social responsibility (including appropriate labour practices) and business continuity arrangements.

It is also important to consider individuals involved in the supplier's senior management team, given geopolitical tensions and involvement with undesirable individuals. Ascertain the supplier's understanding of the critical components relevant to the particular product being produced and the supply chain risk management practices that they have implemented in their supply chain. Look to conduct a news and social media search for last 12-24 months for relevant supplier factors such as frequent changes in senior management, labour unrest or fines.

It is important to recognise the importance of mapping out the various tiers in the supply chain because about 40 per cent of disruptions originate below direct (tier 1) suppliers, according to Business Continuity Institute's annual Supply Chain Resilience Report. Consider whether any of the subcomponents/raw materials present risks, for example conflict

WEF GLOBAL RISKS



Source: World Economic Forum Global Risks Perception Survey 2021-2022

ASSESSING SUPPLY CHAIN RESILIENCE TECHNOLOGY AND DATA

To be able to scale your supply chain resilience efforts effectively, even where you are only looking to monitor, say, 20 critical suppliers, the only way to achieve the required level of risk monitoring and mitigation is to make use of technology and data. The good news is we now have technology and data solutions available which are both user friendly and cost-effective. It maybe appropriate to look at combining more than one solution because of their different functional and data capabilities.

The key to technological solutions is that they provide actionable risk insights. In assessing the technology solutions and relevant providers to use from a functional and support perspective, here are some of the high-level evaluation criteria to consider:

- An ability to map a supply chain to provide the relevant level of transparency including the lower tiers of supply. This is needed from a disruption perspective and is increasingly being required from a regulatory perspective
- A comprehensive set of risk data around suppliers such as their financial solvency, ownership, cybersecurity, health and safety, corporate social responsibility (including appropriate labour practices), legal cases
- A capability to overlay near real-time supplier/supply chain risk incidents relevant to the network that has been mapped
- An ability on a global basis to understand the relative natural catastrophe, geopolitical and relevant operational risks related to a geolocation, even though data quality varies depending on the location
- A capability to review a supplier from a news and social media perspective (including local news and in multiple languages), in terms, for example, of their activities relevant to financial performance, sustainability, and ethical and labour practices. Use machine learning algorithms to remove noise from the data being provided
- An ability to look at logistical/shipping lane risks, a critical aspect of any goods-related supply chain
- Provide an insight into your multi-tier cyber supply chain security. Without relevant data flows supply chains stop operating and cyber attacks on supply chains grow
- A capability to create a digital twin to perform "what if?" scenarios on critical supply chains to enable risk mitigation efforts to be improved and impacts to be understood
- The supplier needs to be able to provide an appropriate level of local implementation support and have skilled risk analysts with appropriate scale to support your internal team where required
- An ability to provide a full audit trail and tracking of actions being taken and the results.

minerals or in relation to labour practices in respect of increasing regulatory requirements such as the UK Modern Slavery Act and the German Supply Chain Act.

Benefit case studies

There are many examples of the financial benefits that can be obtained from even small investments in supply chain resilience, including in the case of the current COVID-19 pandemic. A technology company, for example, who had already mapped out the critical suppliers that it had based in Japan prior to the tsunami in 2011 was able to buy components that it had recognised were likely to be in short supply and thus protect its financial results. A European company who understood at the start of the COVID-19 crisis that it had exposure to Wuhan province from its supply base was able to shift three months' inventory in advance, before lockdown, to protect its ongoing performance. There are many such case studies that risk managers can usefully study.

Overall, it is imperative to optimise your financial performance by ensuring that appropriate supply chain resilience is embedded in all aspects of your supply chain management processes from supplier selection to ongoing supplier management. Make use of the relevant supply chain resilience technology and risk data, which is now readily available to support these process improvements. And apply relevant, potential risk scenarios against your digital twin, such as those of climate change, to your high-value supply chains, as is increasingly expected by investors. ER

Nick Wildgoose is an independent supply chain risk consultant at Supplien Consulting and a board member of the Supply Chain Risk Leadership Council.

IRM Training Courses

Industry-leading training courses delivered by risk experts for over 30 years

Benefits of IRM training:

Practical & intractive training

Industry expert trainers

CPD & accreditation

Training courses include:

- Risk Essentials Masterclass
- Senior Risk Masterclass
- Operational Risk Masterclass
- Fundamentals of Risk Management
- Choosing and Using Key Risk Indicators
- Embedding Risk Management
- Managing Risk in a Digital World
- FoRM Financial Services
- Project Risk Management
- Optimising Risk Workshops
- Organisational Resilience
- Risk Champions
- Risk Culture
- Risk Management for Infrastructure
- Risk Management for Oil & Gas
- Climate Change Risk Management

Find out more at:

www.theirm.org/training-mag

irm

Developing risk professionals

Directory

Change tomorrow with industry leading GRC software

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

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

Cost-effective technology for risk & compliance professionals

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

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

Enterprise risk management and risk analysis software

riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud based, the Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

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

Risk, audit & compliance software

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

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

Risk management software

Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while bringing new ideas and advanced features to the RMIS market. Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use, providing integrated solutions to the entire insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage total cost of risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com

Neil Scotcher
+44 (0) 16179 17740
nscotcher@origamirisk.com
www.origamirisk.com
30 Moorgate
London
EC2R 6PJ

Risk management software

In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and implementation of risk management. Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

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

Wired together

Comparing machine intelligence with human consciousness has led us up a blind alley, not least because we are already integrated with machines through our shared unconscious processes

Just over 50 years ago, the American psychologist Donald Hebb explained his highly influential assembly theory with the pithy phrase neurons that fire together wire together.

The simple meaning of this long-lasting idea is that brain cells (neurons) that are apt to respond to the same sort of stimuli connect into networks.

Subsequently when any neuron in a network is activated, the others are prompted to react too. That would explain people's often instantaneous response to the things in the world. It also provides a ready-made theory about how people remember, by activating existing networks, and learn – by building new ones.

Unconscious

Since then, theories of the cognitive unconscious have become more commonplace. Seen in that light, most of the action that Hebb describes happening in the brain acts below the surface of our everyday awareness. While readers of this article may vaguely notice, for instance, the device or paper they are holding, or the smell of coffee wafting up from their drinks, most of their active attention is (hopefully) directed towards understanding the words as they unfold.

Theories of these unconscious networks are now popular in the

psychology of risk. For example, in Richard Thaler and Cass Sunstein's highly influential 2008 book *Nudge: improving decisions about health, wealth and happiness*, the authors favour using prompts that act at a largely unconscious level to change behaviours. Replacing eye-level chocolate with fruit at a supermarket checkout is a nudge. The stimulus is meant to activate our unconscious networks and reinforce our good intentions.

Machine intelligence

More recently, machine intelligence has entered into the debate. It has taken a a lot of human ingenuity to create artificial intelligence systems to recognise human speech and images and objects in the world. But today, given the ability of those systems to respond accurately to their environments, there is little doubt that some robots and software programs exhibit intelligence.

According to the philosopher of technology N. Katherine Hayles, though, we have been thinking about such artificial intelligence in the wrong way. We have tended to measure how well machines can think in comparison with conscious human thought. But machines are already thinking in the same way that humans do because their networks of circuitry operate unconsciously in the same way as our networks of neurons.

Cyborgs redefined

In her 2017 book *Unthought: the power of the cognitive nonconscious*, Hayles argues that when human and machine intelligences work together, the whole system effectively wires together. That explains why so many people can work with and understand computer systems at an intuitive level without understanding a shred of code. The messaging between humans and machines is out of sight and out of our conscious minds.

Hayles' theory is provocative, but she is largely positive about its implications. For example, she argues that her framework can be better used to unpick the legal responsibilities and human accountabilities for drones operating in war zones. But since we join with machines at a largely unconscious level and are susceptible to being nudged, we had better hope that the software engineers and their bosses have our best interests at heart. ER

NEW

Supply Chain Risk Management Certificate

Identify, analyse & prevent

About the Supply Chain Risk Management Certificate (SCRM)

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

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

What our experts say

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

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

In collaboration with

SUPPLY CHAIN RISK MANAGEMENT CONSORTIUM™

Find out more at:

www.theirm.org/scrm-mag

Resilience, risk and recovery

irm

Developing risk professionals

The 13th annual Risk Management Awards

The pinnacle of achievement in risk management

SAVE THE DATE

3 NOVEMBER 2022

cirmagazine.com/riskmanagementawards

@CIR_MAGAZINE #RISKMANAGEMENTAWARDS