

Enterprise Risk

Spring 2021 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Cooperative resilience: APAC special / **Mind wars:** combatting intellectual property theft / **Complex manoeuvres:** managing the lifecycle of equipment / **Risk management's transformations:** IRM COVID-19 survey / **Business travel after Brexit:** new compliance requirements / **Boosting online learning:** life lessons



Global ambitions: Attitudes are changing to risk in Indo-China, as IRM ambassador to the region Saman Bandara explains

Why risk it? Get qualified

Advance your career with the global benchmark qualification in risk management



**International Certificate in
Enterprise Risk Management**



**International Certificate in Financial
Services Risk Management**

Enrolment for the IRM International Certificate qualifications is now open

Ensure you are up-to-date with international standards and best practice required to effectively mitigate risks and capitalise on opportunities to save your organisation time and money.

IRM's globally recognised International Certificates in Enterprise Risk Management and Financial Services Risk Management can help you to become an effective risk professional, and become current and competent. Both qualifications take 6-9 months to complete, the certificates are delivered by online supported distanced learning. Gain a whole new skillset from the comfort of your own home.

What our students say



Ashtar Matwani IRMCert

Enterprise Risk Management Specialist, ASYAD Group Muscat, Oman

"The IRM qualification has helped me better align my practice at my current job with industry practices and international benchmarks. I see the IRM qualification as a stepping stone to furthering anyone's career in risk management, and is also a brilliant opportunity to network with risk professionals from across the globe at the convenience of your home office!"

Find out more at:

www.theirm.org/qualifications

Resilience, risk and recovery



Developing risk professionals

Editor

Arthur Piper

Produced by

Smith de Wint

Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024

risk@sdw.co.uk

www.sdw.co.uk

Sponsorship and Advertising Sales Manager

Redactive Media

IRMSales@redactive.co.uk

Tel: +44(0)20 7324 2753

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

ISSN 2397-8848

About the IRM

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

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

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

Institute of Risk Management

2nd Floor, Sackville House, 143-149

Fenchurch Street, London, EC3M 6BN

Tel: +44 (0)20 7709 9808

Fax: +44 (0)20 7709 0716

enquiries@theirm.org

www.theirm.org

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



Developing risk professionals



MIX
Paper from
responsible sources
FSC® C017177

Editorial



Risk management: a universal language

Over the past couple of years, IRM has been deepening its global reach. As you would expect, we have reflected this trend in *Enterprise risk*. We have published issues with special focuses on IRM's work in the US, India, Africa, Latin America and, in this issue, Indo-China.

While there are obvious regional differences, the similarities in some regions are striking. For example, when IRM's global ambassador for Indo-China, Saman Bandara, talks about the growing pains of ambitious family businesses, many of the issues they face are relevant globally. The trajectory from risk-taking entrepreneurialism to risk-aware larger businesses seeking foreign investment is the same in Vietnam as it is in Argentina.

In that sense, risk management speaks a universal language. Only by understanding your threats can you fully take advantage of your opportunities.



IRM has a key role in being an educator, especially in developing countries where risk maturity can be low

IRM has a key role in being an educator, especially in developing countries where risk maturity can be low. During my interview with Bandara, he made a strong case for proper risk training and education. Not having it comes at a price.

For instance, businesses sometimes commission consultants to conduct risk assessments so that they can transform the business in a way that it will become more attractive for investors. Those reports entail months of work and come with a hefty price tag. But to take advantage of the report's content, people in the business need to turn the recommendations into action. Without a proper understanding of risk management, that is impossible.

In this issue, we also report on IRM's latest survey on how members have been affected by the COVID-19 pandemic. While the sample size is not massive, the survey suggests the type of work risk managers are doing has changed.

Almost four in ten (37 per cent) respondents said they were now providing risk advice in relation to crisis decision-making. An equal number reported that they were reviewing their organisation's risk management policies and processes as a direct result of the pandemic.

Most strikingly, almost all (96 per cent) respondents felt that the case for risk management had been strengthened by the pandemic experience. For many, that will play out in budget increases for the function.

It seems, then, that risk management is increasingly valued across the globe – from family businesses in Vietnam to governments and corporations worldwide. It is a trend that is only likely to accelerate.

Arthur Piper

Editor

The Certificate in Operational Risk Management

The ideal qualification for anyone looking to develop an understanding of international operational risk management.

Get the recognition you deserve. All CORM holders will now be able to use the post-nominals CIOR, the benefits are that it will help to raise awareness of you achieving the qualification, as well as building your professional status within the risk management community. To apply for the designation (once you've passed) you'll need to renew your IOR membership subscription annually.

The international CORM qualification provides students with an introduction to operational risk management including the tools and techniques used and how it fits into the wider risk management of the firm. The qualification is externally accredited at RQF Level 4/EQF Level 5, and is ATHE regulated by Ofqual.

Risk professionals have never been so busy and pivotal to the survival of organisations of all types globally, risk management has undoubtedly been at the heart of the global response to Covid-19. Our profession is firmly in the spotlight.

What our students say



Justine Keys

HR Risk Manager, Risk & Regulation – Human Resources at Santander UK

"The IOR CORM has given me a comprehensive view of the fundamentals of operational risk management. This has enabled me to better understand how we manage risk within my own organisation and add value in my role as a Line 1 operational risk manager in the HR function."



Ellis Williams

Consultant – Financial Crime at National Australia Bank Limited

"CORM has added real value to my self-development and potentially career opportunities by providing me with a working knowledge of a subject that I had limited prior exposure to. The course content was complemented by real-life examples to illustrate operational risk concepts providing for a much better appreciation of the subject and its implications."

Find out more at:

www.ior-institute.org/corm



10

FEATURES

APAC REGION SPECIAL:

10 Global ambitions

Attitudes are changing to risk in the rapidly developing countries of Indo-China, as IRM ambassador to the region Saman Bandara explains

14 Co-operative resilience

Working with your ecosystem of partners is the key to effective risk management

18 Mind wars

Intellectual property theft is becoming big business globally, and risk managers have a key role to play in protecting their organisations

24 Complex manoeuvres

Procurement in the Ministry of Defence demands rigorous risk management procedures at every stage of an item's life cycle

28 Risk management's transformations

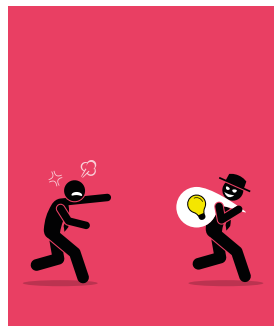
Risk managers have coped well during the pandemic and look set to enjoy an expanded role in many organisations, according to latest IRM's COVID-19 survey

30 Business travel after Brexit

The end of free movement across Europe is likely to bring new compliance risks and extra work for risk managers



14



18

REGULARS

07 IRM Viewpoint

Members of IRM and IOR are invited to collaborate more closely to strengthen their knowledge, skills and professional development

08 Trending

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

34 IRM Focus

After over a year of pandemic lockdowns across the world, IRM trainers and students find themselves in a changed landscape of online training and risk workshops

36 Directory

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

38 Toffler

Communication technologies are making us unhappy and less productive. It is time to rehumanise our digital lives



24



28



30

IRM Virtual Training

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

IRM training courses cover a wide range of risk management disciplines. We are the leading provider of risk management training based around global best practices, delivering interactive and thought-provoking content.

Our courses are delivered as practical and interactive virtual classrooms that will provide you with useful tools and techniques to help you identify, assess and manage risk.



e-Learning training
with virtual activity
packs



Learn anywhere in the
world, from the comfort
of your own home



Thought provoking,
best practice
content

- > **Fundamentals of Risk Management**
- > **Embedding Risk Management**
- > **Practical Risk Appetite & Risk Tolerance**
- > **The Risk Essentials Masterclass**
- > **Risk Reporting**
- > **Risk Culture**
- > **Choosing & Using Key Risk Indicators**
- > **Risk in the Boardroom**
- > **Managing Risk in a Digital World**
- > **Third Party & Supply Chain Risk Management**



e-Learning programs

Introduction to Enterprise Risk & Resilience

Risk and Resilience: The four main components

Fundamentals in Quantitative Risk Management & Business Simulations

Find out more at:

www.theirm.org/training-mag

irm

Developing risk professionals

Deepening ties

Members of IRM and IOR are invited to collaborate more closely to strengthen their knowledge, skills and professional development



When the Institute of Operational Risk (IOR) became part of IRM in May 2019, the intention was to leverage an already productive working relationship between the two bodies. Since then, we have increasingly pooled resources and expertise to enhance our strong educational, training and networking capabilities.

Our focus has been on harmonising our activities and processes in line with IRM while continuing our support for the operational risk community under the IOR brand. IOR's Certificate in Operational Risk Management (CORM) is available to all and upon successful completion entitles members to the CIOR post nominals. The CORM was recently recognised by the Hong Kong Monetary Authority for inclusion in its Enhanced Competency Framework for Operational Risk.

At IOR, we have also recently revised and published our series of nine Sound Practice Guidance documents on operational risk, and we will be looking to continue to add to the series. We are keen to hear any member feedback or suggestions. These can be found at bit.ly/3bgs6Tt and are also available at issuu.com/irmglobal.

Invitation

I would like to take this opportunity to invite IRM members involved in any form of operational risk activities to become involved with IOR. Since operational risk is still a relatively recent discipline, practitioners can sometimes feel isolated and disconnected from others working in the same or similar fields, even more so in the current COVID-19 climate. Coming together as a community of like-minded individuals to share experiences and provide mutual support can be a powerful tool for professional and personal development.

It is especially timely as many of the risks that our members face today have a significant operational risk dimension. COVID-19 has intensified focus on risks such as business resilience caused by lockdown rules in various countries, critical service and supply chain disruption, and impacts on business model transformation. Currently, many organisations now depend on staff working from home, which has intensified the people risk exposures and resource management challenges, including employee health and wellbeing. Other heightened operational risks include information/data protection, technology

dependence, risk of fraud, cyber-security, staff availability and IT resilience. Global regulators are also focusing on operational resilience as an outcome of effective operational risk management, which is further raising interest in the discipline.

As risk managers, we help organisations consider these threats more objectively, understand and develop their risk appetites, and respond with strategies to manage risk accordingly.




I would like to take this opportunity to invite IRM members involved in any form of operational risk activities to become involved with IOR

Coming together

IOR brings together a wide range of risk professionals to discuss and share best practice on the rapidly evolving risk landscape. By developing our frameworks and strategies to help our organisations, we both improve our effectiveness and enhance the standing of our profession.

IOR has a number of regional chapters that meet to engage in many countries around the globe including the UK, Germany, Hong Kong, Ireland, Nigeria and Thailand. Chapters are member driven and hold events and host webinars to discuss a broad range of hot topics, emerging challenges, regulatory priorities and technical aspects of operational risk management. They also provide an opportunity to network with peer practitioners.

To register interest for events, go to the IRM website [www.theirm.org], join the IOR LinkedIn group [www.linkedin.com/groups/3511716/] or, for any feedback or other ideas, contact Juliet Kamese, our member engagement manager at juliet.kamese@theirm.org 



Tony Chidwick is chair of the IOR committee and an IRM board member.

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



Who is knocking at the door?

Percentage of user accounts that are fraudulent:

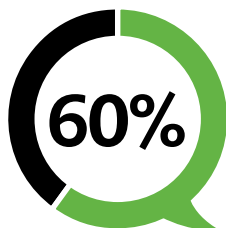
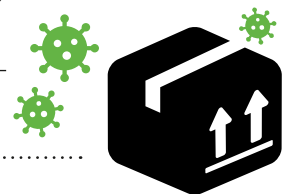


 Yet identity proofing is top challenge:

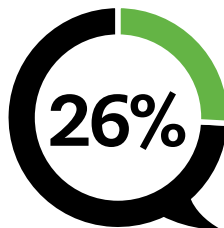


Sources: Digital fraud trends report 2021, DataVisor | Fraud trends to watch in 2021, LexisNexis Risk Solutions

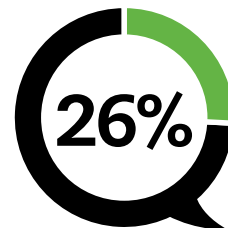
COVID-19 boosts logistics in emerging markets



Logistics executives that say pandemic has permanently changed their operations



Those saying they are more confident in operating in emerging markets



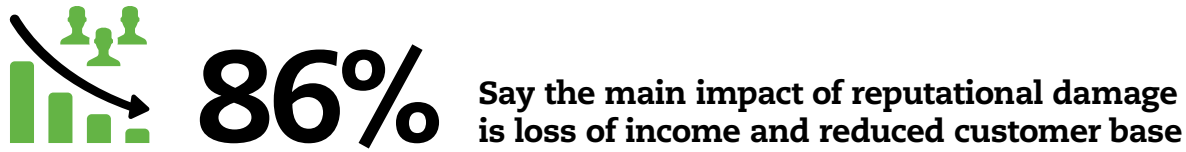
Those saying they will be renewing focus on emerging markets

Source: 2021 Agility emerging markets logistics index, Agility

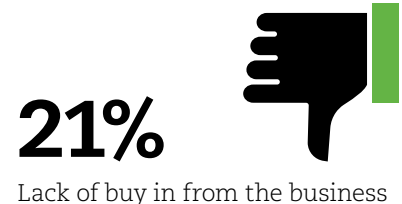
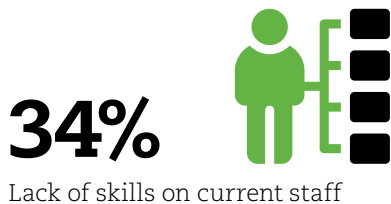
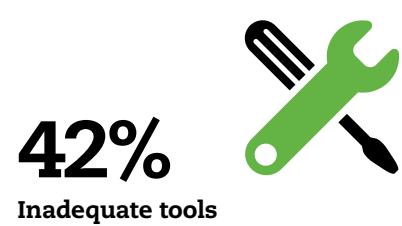
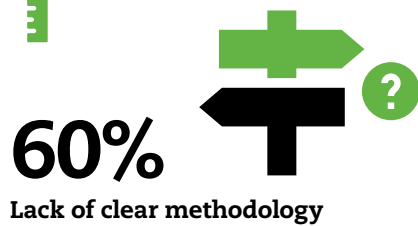
Risk managers struggle to tackle reputational threats



Over the next five years four in five risk managers expect more focus on business reputation

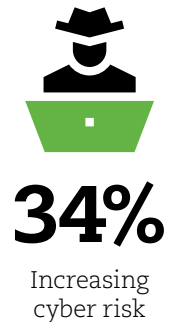
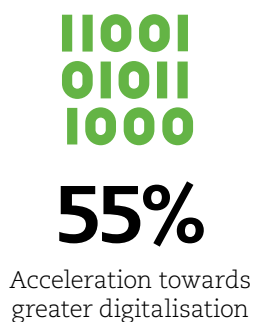


But key challenges to monitoring and measuring reputational risk remain:



Source: Global reputational risk management survey report, Willis Towers Watson

Pandemic-induced business transformations



Source: Allianz Risk Barometer 2021

Global ambitions

Attitudes are changing to risk in the rapidly developing countries of Indo-China, as IRM ambassador to the region Saman Bandara explains

..... BY ARTHUR PIPER

The Indo-China region is undergoing rapid economic and social development. The countries in the region – Cambodia, Vietnam and Laos – have transformed significantly since the mid-1980s. The World Bank, for example, has called Vietnam's 30-year reform programme remarkable. "Economic and political reforms under Đổi Mới, launched in 1986, have spurred rapid economic growth," the bank said, "transforming what was then one of the world's poorest nations into a lower middle-income country." Between 2002 and 2018, GDP per capita increased by 2.7 times.

The pandemic has hit the region, setting back economic and social reform. COVID-19 has plunged Laos into its first recession since the early 1990s. Since Cambodia relies heavily on tourism, manufacturing garments for export, and construction, it too has seen contraction. Vietnam, on the other hand, has fared better with an anticipated growth rate of about 2.8 per cent for 2020, according to the World Bank.

The US's recent spat with China has made Vietnam, in particular, more attractive to inward investment. Foxconn, for instance, is reportedly building assembly lines for Apple's iPad tablet and MacBook in Vietnam's



The US's recent spat with China has made Vietnam, in particular, more attractive to inward investment

.....





north-eastern Bac Giang province, according to Reuters news agency. It also said that Taiwanese manufacturers are looking to relocate to the countries. Japanese businesses invest heavily in Vietnam, and the European finance group Nordea has described Vietnam “as one of the most attractive countries in terms of foreign direct investment in Asia”.

Challenges

Investing in the region is not without problems, according to Saman Bandara, IRM’s ambassador to the region. As a partner at the global consultancy EY, where he heads its assurance-financial services and forensics practice, he sees the difficulties first-hand. Vietnam has a different mechanism when it comes to regulation and governance. “From a risk management perspective,

one of the main issues for foreign investors is the development of the overall legal environment,” he says. “Some of the laws and regulations are not directly comparable to the laws and regulations in neighbouring, developed economies such as Singapore and depend more on a rules-based approach to standard-setting.”

For example, Vietnam has been working to introduce International Financial Reporting Standards to replace its local accounting standards. While Vietnamese Accounting Standards are rules based, they still allow for alternative treatments through regulatory interventions in a wide range of areas, which makes the accounts difficult to interpret accurately. The situation is complicated further by limited publicly available information.

“ There can be a veneer of professionalism on the surface, but at a deeper level, personal relationships carry more weight

IRM AND APAC

The IRM APAC Regional a Group (RIG) is a network of risk and business practitioners that stretches across the Asia Pacific and Oceania region, spanning across India, the countries of South East Asia, China, Japan, Australia and New Zealand.

We are active contributors to thought leadership in risk management in the context of the APAC region, and to the IRM globally. This includes liaising with IRM Special Interest Groups and other partner organisations across the region.

Due to our geographic span, most of our work is virtual. We arrange online thought leadership events for our members, enabling them to stay abreast of global best practices, to build strong relationships and to network and share experiences, stories and good practices.

To achieve our thought leadership activities, we:

- Hold web meetings and webinars on topics of interest
- Publish an APAC newsletter
- Speak at APAC events (IRM and non-IRM)
- Run an IRM APAC LinkedIn Group
- Help assist with training

We are very excited about harnessing the potential of risk management now and into the future.

Representatives: Gareth Byatt (APAC region + Australia), Saman Bandara (Cambodia, Vietnam and Laos), Abhishek Paul (India), Hersh Shah (CEO, IRM India Affiliate) and Jason Qian (China).

To get in touch, visit: bit.ly/3sNILUr



Things are changing as the spread of risk management-type activity becomes more common

“If someone wants to invest in Vietnam, the amount of data is very limited and they may get conflicting information about the risk profiles of those businesses and sectors,” says Bandara. “There have been a lot of cases where investors have lost money because they did not dig deeper at the time of making the investment decision; there is a lack of detailed information at the point of investment.”

Small and medium-size businesses

Bandara believes the accounting reforms will boost the country’s burgeoning family business sector – many of whom want to attract overseas investment. With strong growth potential, such companies can be an attractive proposition for investors. There is a young and educated workforce. Businesses used to operating in China may find the regulatory regime less stringent, but similar in other respects. Yet while setting up a business is relatively easy, enforcement of rules around intellectual property for example, or dealing with deep-rooted family relationships, could prove more challenging.

“Directors do seek professional advice about their businesses, but professional opinion is often sidelined because the decisions have already been made and discussed in family circles,” he says. “There can be a veneer of professionalism on the surface, but at a deeper level, personal relationships carry more weight.”

There are differences between sectors. The financial services industry has become more attuned to international standards. In banking, the regulatory environment may still be a couple of decades behind countries such as Singapore and the UK, but the government is pushing for banks to meet the capital adequacy requirements under Basel II. While 13 banks were meant to have listed by the end of December last year, according to S&P Global Market Intelligence, the pandemic has slowed progress so that only the largest three have achieved those aims by the target deadline. Even so, these initiatives are beginning to raise the profile of risk management across many sectors.

Risk management

Bandara says that the culture in Vietnam – and in the region more generally – is very entrepreneurial. It is typical in developing countries, including Indo-China, for people to make money first and think about risk later. In the earlier stages of business start-ups, Bandara says, risk management is given a low priority among family business owners – they delay risk management practices until they have grown into larger enterprises. That is when they begin to understand the risks they face can be managed in a more formalised way.

Bandara ascribes this approach to a lack of understanding and education in risk management – something he believes IRM fosters in the region. Interest in IRM is gaining momentum. “Young professionals have been taking greater interest in risk management as a topic,” he says. That is partly because they are beginning to appreciate that the old style of risk management can be replaced by something more relevant and dynamic.

For example, regulated industries, such as banking and financial services companies, have risk management functions in place. But formal education in risk management is scant. “If you are not educated in the discipline, you do not have the right perspective and skills to manage risk,” Bandara says. He recalls meeting a head of risk whose background was in sales. Without having had the right training, that person was still looking at risk from a sales perspective, which favoured risk taking. In less well-regulated sectors, many directors still believe that because risk management is not mandatory, it is not worth having. “Often you will find in organisations that even the basic risk documentation does not exist,” he says, “but over time it is becoming better.”

In his role as a forensic accountant, he sees that the effects of a lack of education in risk can be far-reaching and costly. “When we ask risk management teams to implement our recommendations, they are unable to do so if they don’t have a proper understanding of the subject and its methodologies,”



Above: Hanoi, the capital of Vietnam, at night.

he says. “They can feel they are wasting time because they have paid hundreds of thousands of dollars to consultants for a report that is gathering dust on somebody’s desk.” That makes better risk management education and training vital.

Stressing the value

International consultants, the government and IRM have been working to raise the profile and explain the benefits of enterprise risk management. In the government’s attempt to foster a good growth agenda, for instance, there are initiatives that imply better risk management in such areas as corruption regulation and corporate crime. Whether directly or indirectly, things are changing as the spread of risk management-type activity becomes more common.

On the ground, the argument can be relatively easy to demonstrate. “I actually think that one of the biggest barriers to the greater take-up of risk management is the quantification of its benefits,” Bandara says. “If businesses need to bring in higher-paid employees to manage threats, they need to understand what the return on their investment will be.” Bandara’s approach is to show case studies, which has often been

enough to persuade directors to take the first steps. After that, it does not take long for those organisations to start seeing benefits, he says.

Raising the profile

COVID-19 has restricted people’s ability to go out and meet friends, and people are working from home. This has been difficult, but also a time where Bandara has been encouraging them to listen to IRM’s webinars on risk. He has been writing articles in papers and talking to universities to raise the profile of the profession in the region. As an ambassador for IRM, he has been talking to regulators. Over the past two years, he has been able to talk to many risk management teams and persuade them to get started with IRM so they can perform their roles better.

His belief in proper risk management comes directly from his own experience. Bandara trained as a chartered accountant in his home country of Sri Lanka. He was hired by a big audit firm and posted to Singapore, where he focused on auditing insurance companies. While insurers are heavily involved in managing risk for others, Bandara realised the companies they served were not actively managing their

own risks. It was something that did not make sense to him.

Bandara also started studying forensic accounting and ended up being certified in fraud investigations. After that, he moved to Vietnam to start the insurance practice for EY. That was when he sat for the IRM Certificate in Risk Management in Financial Services. It took about nine months to complete.

“It was really worth doing because currently there are so many qualifications where you can get a certificate after a couple of weeks’ study,” he says. He was impressed by the rigour and scope of IRM’s course. “IRM qualifications are more detailed and take time – they should take time because you should not just be thinking of it as an exam, but as a way of getting a deep understanding of the field linked to practical experience and knowledge,” he says.

As the profile of risk continues to rise across the region, he is keen to see more adoption of IRM qualifications and courses. The more properly qualified risk managers there are, the more the value of risk management will become apparent. And the better opportunities businesses will have for attracting crucially important foreign investment in their industries and the rapidly growing family business sector. While the full transformation of the profession in the region may be years away, it has got off to a good start. ☎



IRM qualifications are more detailed and take time

Co-operative resilience

Working with your ecosystem of partners
is the key to effective risk management

BY GARETH BYATT

In the Summer 2020 edition of *Enterprise risk*, I wrote about the need for organisations to demonstrate *purposeful resilience*. Purposeful resilience, for organisations of all sizes, is about demonstrating a good state of resilience that is coupled with a true purpose which ensures you are helping others, particularly in times of need.

Co-operative resilience takes purposeful resilience a step further. It asks us to work closely with others to ensure there is strong co-operative and purposeful resilience in place across our ecosystem and, if possible, the wider environment we operate in. This is particularly important right now, as we continue to navigate our way through the impacts and continued challenges arising from COVID-19.

This piece provides an overview of co-operative resilience, a three-point plan to set it up for success and some examples of how co-operative resilience is impacted by, and applies to, the Asia-Pacific (APAC) region (the region where I am based).

Organisational resilience is described by the ISO in the international standard 22300:2018 (Security and resilience – vocabulary) as the *ability to absorb and adapt in a changing environment* (definition 3.192). I would add “anticipate” to this definition because we need to anticipate and be ready for change.

An organisation’s state of resilience relies on the state of resilience that its ecosystem partners and collaborators



Co-operative resilience is a state of resilience that a network of organisations achieves when it is sustainable and purposeful to society



Organisms exist in complex environments in which they are linked with each other to co-exist and thrive

Build good foundations

Organisations that demonstrate a good culture and a good state of purposeful resilience have a structure in place and people who look ahead and plan, anticipate, adapt and respond effectively to change and events (good and bad). People in such an organisation are given help and support for their personal resilience. There is an innate appreciation for the velocity at which change, and events, can occur, or are already occurring, and the impacts they can have on people, societies and the broader environment. Such a culture is a solid base on which to build co-operative resilience. If we do not have “our own house in order”, we are ill-prepared to work with others to achieve co-operative resilience.

Although anticipating, avoiding and responding to negative events and situations is clearly a major focus of resilience, we should also anticipate and respond to positive change and events. For example, advances in new technology, digitisation and data analytics, and a broad appreciation about the importance of sustainability and the complexity of our environments, can be used for positive change, and positive co-operative resilience.

A practical framework for purposeful resilience must be scaled to suit the size and context of your organisation, and stitched into how it functions. Various ISO standards exist in the “22300 family” to help, including ISO 22300, 22301, 22313, 22316 plus ISO/TS (Technical Standards) 22317, 22318 and 22330, and related standards such as ISO/IEC 27001 and ISO 31000.

Various tools and techniques used for risk management, resilience, strategy and general management can be applied to co-operative resilience. Examples of such tools and techniques include scenario analysis, horizon scanning, stakeholder analysis,

across the value chain demonstrate. Combining and integrating our own resilience activities with our ecosystem collaborators, and undertaking collective actions to help our overall environment and the society and communities we serve, is the crux of co-operative resilience, which I define as *a state of resilience that a network of organisations achieves when it is sustainable and purposeful to society.*

When organisations, across the public and private sectors, implement a strategy for co-operative resilience with their ecosystem and for the overall environment they are part of, they can anticipate and adapt together to demonstrate flexibility and purpose in order to achieve objectives.

Lessons from nature

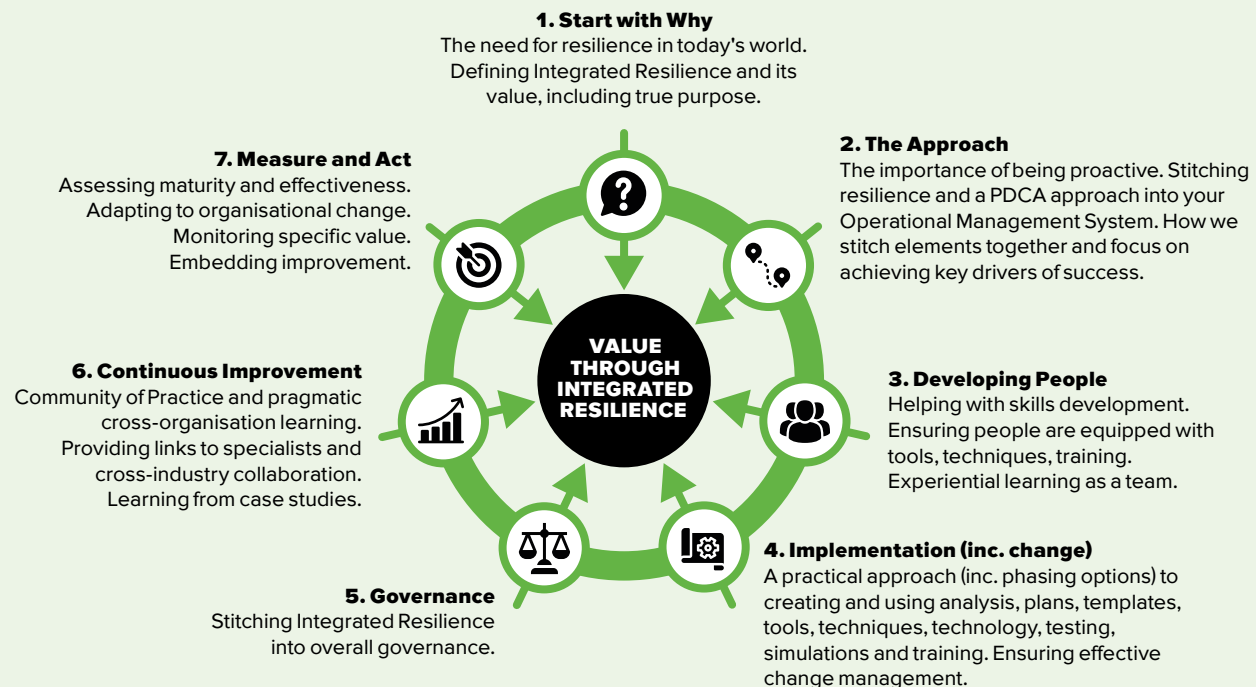
Consider the parallel of the biodiversity web we see in nature. Organisms exist in complex environments in which they are linked with each other to co-exist

and thrive. Remove one part of their ecosystem or place it in danger, and all others are impacted. This concept applies to our human-made ecosystems and environments.

The resilience built into the linkages that organisations have with each other in their ecosystems and value chains is fundamental to co-operative resilience. Think of it as links in multiple chains. An individual entity, business or location – be it a café, an office, a shop, a hospital, a factory, a mine site, a construction site, a port, an airport or any other – needs resilient linkages within its network of collaborators to thrive. And it scales: the rule applies to an organisation that has many sites/ locations, a city or a nation. If the networks and arteries between us are not resilient, or critical weaknesses are not identified and/ or addressed, problems will occur when they are put under strain.

Here are three points to consider for achieving co-operative resilience.

SEVEN ELEMENTS OF A GOOD CULTURE OF ORGANISATIONAL RESILIENCE



Source: Risk Insight Consulting



Good co-operative resilience may sometimes mean accepting or tolerating a certain amount of disruption

“What if?” decision trees, and the Business Impact Analysis (BIA) and Business Continuity Plan (BCP).

By ensuring you have a good state of resilience and are constantly working to ensure it is effective, you have a platform for a co-operative approach.

Co-operate with partners

A practical framework for resilience needs to set out how you liaise with others. Rather than assume that organisations in your ecosystem “will do their own thing”, make the time to work with them to understand

what’s critical to you all. While you may have resilience and business continuity clauses stitched into commercial contracts with suppliers, it is important to go further than legal and commercial coverage. Actively engage with your ecosystem partners to co-operate for resilience.

Discuss collaboratively how you can achieve co-operative resilience, in a way that benefits you all, the communities you serve and the overall environment. Share and discuss your resilience plans with each other and discuss critical integration and touch points. Hold collaborative workshops, tests and resilience exercises such as “hackathons” to see how you really work together under pressure. Spot gaps and improve. Many organisations have been co-operating with each other in reaction to the forces exerted upon them because of COVID-19. As the world recovers from the pandemic, we should maintain this type of focus.

Demonstrate co-operative resilience

A good state of co-operative resilience is something that needs to be

constantly nurtured. It is not a “set and forget” activity – things change. When linkages are in place and regularly tested, you will be prepared and ready to act co-operatively and in a purposeful way when change or a disruption event occurs.

Consider the example of a business anticipating extreme weather in an area where its key suppliers also have operations. If the risk of extreme weather disruption is rising, how well does the business work with its suppliers, customers, insurers, local government departments and local community organisations? Can they jointly implement proactive, cost-effective and co-operative resilience to prevent or minimise potential disruption in the most purposeful way possible?

Good co-operative resilience may sometimes mean accepting or tolerating a certain amount of disruption – which could be described in your risk appetite. At times, it may mean changing your risk appetite to lower the risk. Some organisations are reconsidering their supply chain strategies as a result of COVID-19, for example moving certain activities



Taiwan plays a pivotal role in advanced semiconductor manufacturing

and healthcare PPE. Breweries have adapted production processes to make hand sanitiser. Supermarkets and grocery retailers around the world have worked with their supply chains to keep the communities they serve fed. Restaurants have switched to take-away meals, delivered by agile delivery firms.

Through these examples, and more, we have seen how co-operative resilience can help us tackle pressing societal needs. The same applies to broader sustainability and environmental matters, as defined by the UN Sustainable Development Goals (SDGs). Co-operative resilience can help us collectively improve our readiness and response to disaster risk (including events such as extreme weather, geological disasters, cyberattacks and acts of terror).

The concept of co-operative resilience can be applied to the economic, societal and sustainability issues facing the APAC region, where I conduct much of my own work and liaise with regional IRM members to listen to their experiences and insights.

APAC considerations

The APAC region, and China in particular, is a major contributor to the global economy. Many organisations around the world continue to source supplies (be they parts, components or finished goods) from countries in APAC. Organisations around the world need to fully understand where their supplies are being sourced from, and if critical supplies are coming from APAC, to understand what this means for their resilience (among other things).

For example, the international container shipping trade has been a key focus in recent months. A shortage of containers in certain locations has led to challenges in the availability, and rising costs, of shipping freight globally. If your organisation is being affected by this situation, are there certain co-operative resilience measures that could help you to minimise its impact on your activities and operations?


In addition, the impact of COVID-19 has caused a supply shortage of semiconductors to many industries. In this complex industry, which is critical to so many products, Taiwan

plays a pivotal role in advanced semiconductor manufacturing. If your organisation is dependent on advanced semiconductors, what do the risks of a shortage (taking into account lead times) mean to your resilience, the resilience of your ecosystem and the overall impact on the societies you serve?

Across the APAC region, countries and governments have implemented strategies with their citizens to deal with the COVID-19 pandemic in a co-operative way. Taiwan is often cited as an example of a government that has implemented appropriate technology to help it to manage COVID-19. Vietnam's co-operative approach has been well documented, as has that of South Korea, Singapore, Australia and New Zealand, to name but a few. What opportunities exist for us to learn from the co-operative approaches that have been taken in much of APAC?

The APAC region is at the frontline of seeing the impact of climate change. It is a region in which many of its cities are low-lying and coastal, which makes them vulnerable to the impacts of flooding and extreme weather such as typhoons and cyclones. With an anticipated increase in heat and humidity expected across much of the region, and a rise in precipitation forecast for some areas while droughts are anticipated in others, Asian societies and economies are innovating in various ways to combat climate change. They are demonstrating co-operative resilience. With their innovation, they are learning from other regions while considering the context of their specific geographies.

As we all move forward and continue responding and adapting to the impact of COVID-19, think about how co-operative resilience can benefit your organisation, the collaborators you work with and society as a whole. Are you doing enough today to be resilient for tomorrow? 📌

 Gareth Byatt is an independent risk consultant and owner of Risk Insight Consulting. He is also an IRM global ambassador for the APAC region. He is based in Sydney, and has over 20 years' experience in international risk management and resilience.

closer to their operations sites.

As part of your ecosystem review, understand how your suppliers may also serve other sectors, and what that could mean. For example, consider the semiconductor industry. If semiconductor firms come under pressure to supply a number of industries (as has been the case during the COVID-19 pandemic), what could that mean for your needs/where would you be in the queue for deliveries? Plan ahead and conduct scenarios and exercises for such cases.

During 2020, we saw many examples of what we can collectively achieve when we set our minds to it. Whole ecosystems around the world have worked in a highly co-operative way to demonstrate co-operative resilience in response to COVID-19. Pharmaceutical businesses, biotechs and researchers have collaborated to develop vaccines for COVID-19 at unprecedented speed, backed by government funding. Mining and industrial firms have donated PPE to hospitals. Manufacturers, retailers and others have quickly retooled production lines to make ventilators

Mind wars

Intellectual property theft is becoming big business globally, and risk managers have a key role to play in protecting their organisations

..... BY ROBERT CHAPMAN

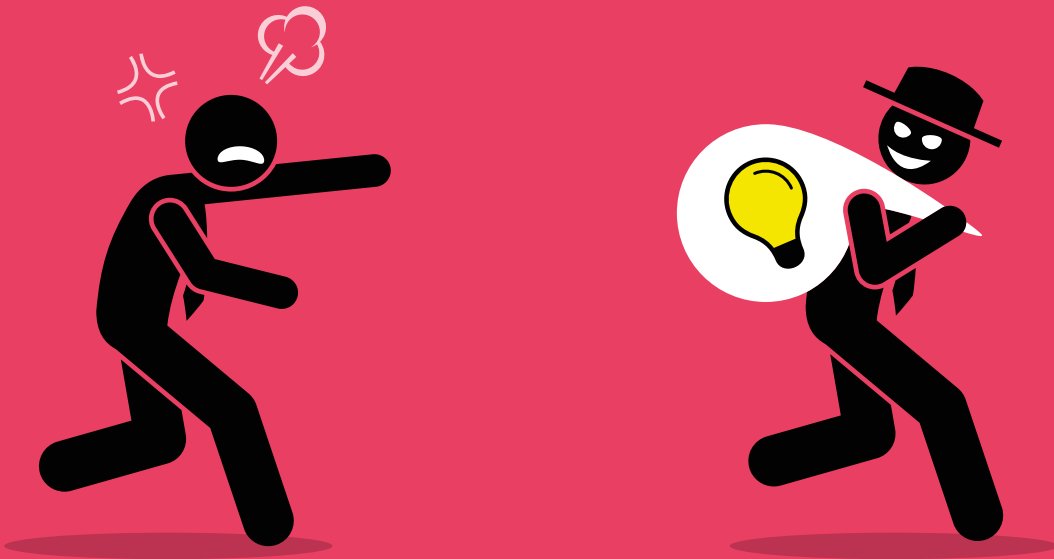
Fraud is omnipresent and highly corrosive. It is commonly recognised as among the most serious risks facing UK businesses today. Fraud is perpetrated by individuals and businesses through a variety of dishonest and illegal activities for financial gain. When conducted by individuals, these may be external threat actors or even employees. It can result in a loss of market share, customers and sales followed by a reduction in turnover and profitability. Depending on the scale of losses, it may also lead to permanent job losses. A serious fraud event can result in a business struggling to recover for years, or even lead to its eventual collapse.

It surfaces in a myriad of business functions, and its perpetrators are constantly evolving new ways to search out company vulnerabilities. The growing prominence of state-sponsored fraud is even more insidious and is often more debilitating. Fraud is a problem for all companies irrespective of size. Given the time and resources needed to minimise fraud, as a consequence of their size, small and medium-sized enterprises (SMEs) are particularly vulnerable. All businesses have to be constantly vigilant. They have to be aware of the known methods of fraud, the government agencies providing advice and the organisations to turn to in a time of crisis.



Perpetrators of IP cybercrime are seeking highly prized business secrets – not already disclosed through patents – and proprietary business information that can be quickly sold

.....



Intellectual property fraud

Of all of the types of fraud, the theft of intellectual property (IP) continues to dominate international media headlines due to the innovative blue-chip companies impacted and the potential harm that they may suffer. The UK government defines IP as something that individuals create using their minds. The definition provided by the online Cambridge Dictionary is more expansive and states “IP describes someone’s idea, invention, creation, etc., that can be protected by law from being copied by someone else”. Don Fancher, principal at Deloitte Financial Advisory Services, succinctly described IP within Deloitte’s 2016 Review (Issue 19) as “the lifeblood of many organizations” in that “it fuels innovation, growth and differentiation”.

Europol’s 2020 report on IP crime and its links to other serious crimes, states: “IP crime is often seen as ‘victimless’ crime, causing relatively ‘little’ harm. However, in addition to causing harm to the economy in general and to companies owning IP (including small and medium sized ones in particular), in many cases IP crime [...] can cause damage to the health and well-being of consumers, the environment and society”.

While IP crime is often referred to in relation to the production and sale of counterfeit goods, it also relates to the theft of technological know-how such as in the revolutionary development of electrical planes and cars. Perpetrators of IP cybercrime are seeking highly prized business secrets (not already disclosed through patents) and proprietary business information that can be quickly sold. Proprietary business

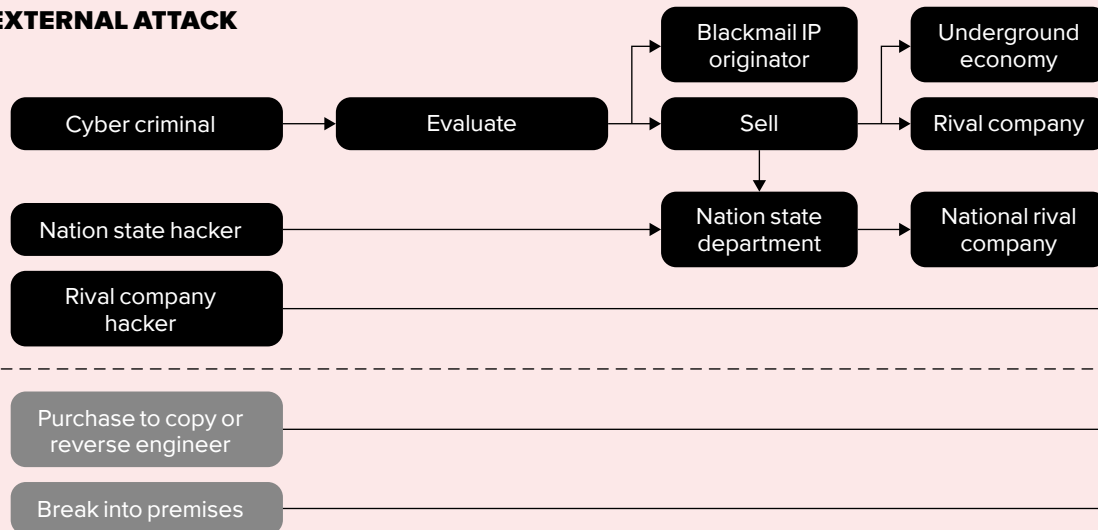
“ Nation state hackers sponsored by their own foreign intelligence service steal IP to enable the rapid accumulation of knowledge in the absence of their own country’s capability to develop it

METHODS OF ATTACK

INTERNAL ATTACK



EXTERNAL ATTACK



“ While systems and data are important, the behaviour of personnel and developing the right business culture are paramount in the fight against IP theft

information may include geological survey information on precious metals or details of mergers and acquisitions. The World Economic Forum's *The global risks report 2021* records data fraud (now grouped with cybersecurity breaches) as among the highest likelihood risks for the next ten years. Apart from organised crime groups (OCGs), IP theft is also sponsored by rival businesses and nation states seeking prized designs and technology to provide operational or technological advantage.

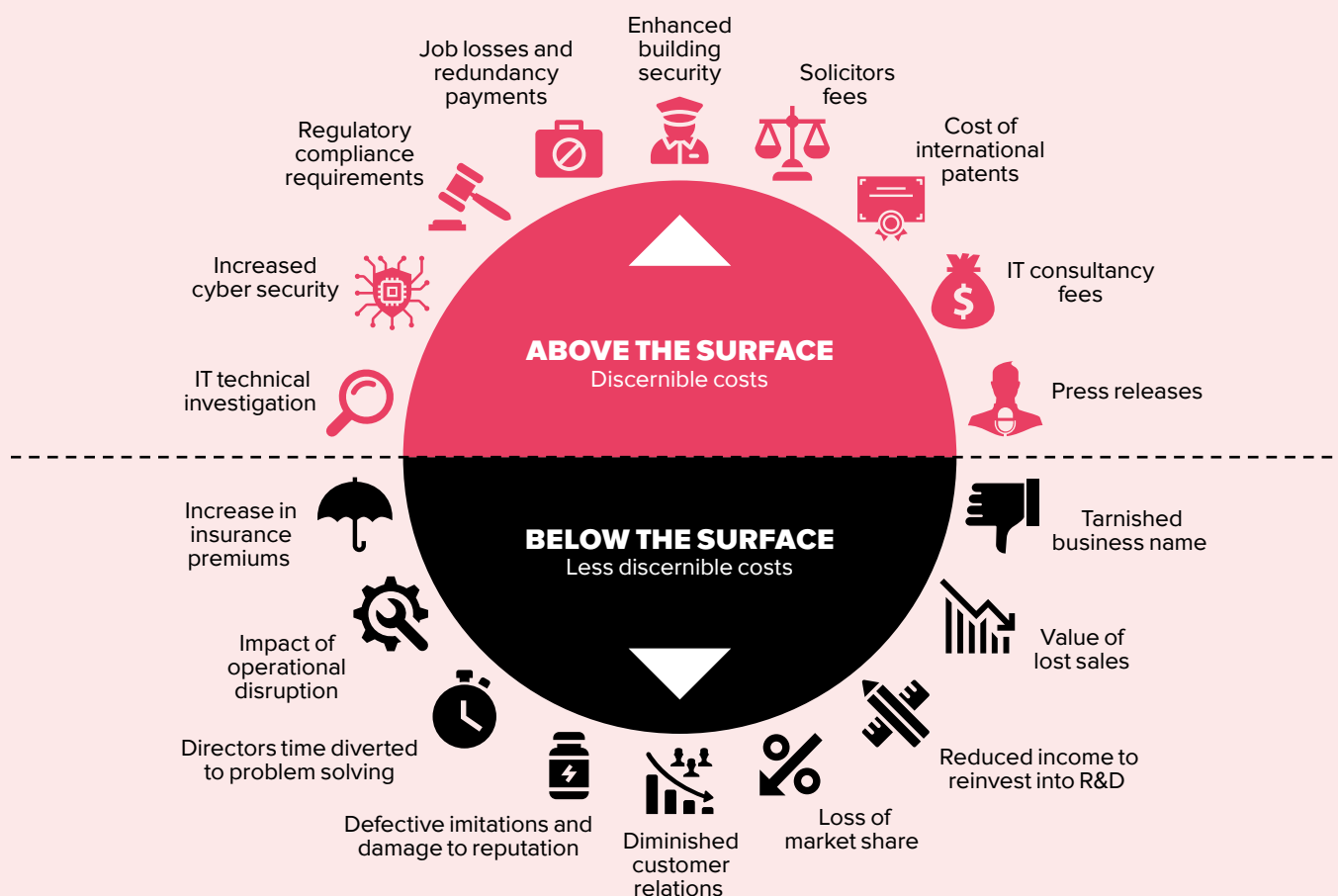
How does IP theft occur?

There are a number of scenarios whereby IP theft may occur, as illustrated in *Methods of attack*. Theft may be committed by what is commonly termed as an insider (an employee), or from outside the business (by external threat actors). Hence, it may be perpetrated by

a departing company employee with the view to use the IP to start up a new company, take it to a new employer or to sell it (on the assumption a buyer can be found). Alternatively, by an employee who already has links to an OCG, disreputable but legitimate company in the same industry or an aggressive nation state, established prior to joining the business.

Externally, it may be perpetrated by an opportunist cybercriminal who will initially evaluate the data to understand what will provide the best returns. Options may include blackmailing the owner of the IP or selling it: on the underground economy, to a rival company operating in the same market or to a nation state. Alternatively, it may be perpetrated by nation state hackers sponsored by their own foreign intelligence service to steal IP to enable the rapid accumulation

THE DISCERNIBLE AND LESS DISCERNIBLE COSTS OF A LOSS OF IP



of knowledge in the absence of their own country's capability to develop it. Their long-term goal is to make their country technologically and financially superior on the world stage. Other scenarios include a rival company hacker and theft by a competing company which buys the product or article and then reverse-engineers or copies it. The last scenario examined here is theft by a person or persons who physically break into the business premises, a company car or the home of an employee to acquire the information sought.

Insider fraud

Insider fraud is conducted by employees of a business. Given the mobility of employees combined with business's need to attract the most talented individuals to be able to succeed in highly

competitive markets, project teams are often multinational. Business vulnerabilities are then exposed to foreign nationals employed overseas who may be motivated by personal financial gain. Insider fraud perpetrated by Chinese nationals has gained overriding prominence due to the frequency and the profile of cases reported in the media and the FBI's repeated assertions over many years of the relentless pursuit of American IP by Chinese companies and individuals.

In the last couple of years, two prominent cases of alleged theft of IP were reported in the media relating to Apple and Tesla – although the disputes are ongoing and relate to individuals who may have taken secrets with them when they left the companies in question. Tesla, the electric car maker, for instance, filed a lawsuit in the US alleging that Guangzhi Cao, a former employee

Understanding IP fraud needs to be an integral element of enterprise risk management

RISK RESPONSE ACTIONS

YOUR PEOPLE	YOUR SYSTEMS	YOUR DATA
Have strict procedures for sharing IP with participating partners and suppliers outside of the company.	Consider the use of a managed service provider for managing automated backup.	Limit the number of personnel that have access to IP.
Establish a zero-tolerance culture to emphasise that fraud is completely unacceptable.	Establish a business continuity methodology and processes and test at regular intervals.	Consider disaggregating IP, such as saving different aspects of IP in different locations whereby one aspect is meaningless without the others.
Ensure the delivery of regular ongoing, comprehensive cybersecurity awareness training to all employees across all business functions, to help employees be alert, wary and vigilant.	Know where company information resides, know what applications and networks store and process that information, and build security into and around these.	Validate that any partners or suppliers involved in collaborating in the creation of IP have taken the same cybersecurity measures and are in sync in terms of the protections adopted.
Motivate those generating and processing IP to exercise security awareness and observe data management policies and processes on a day-to-day basis.	Maintain inventories of hardware and software assets to know what is in play and at risk from attack.	Agree processes for the movement and storage of IP information, particularly between active and back-up files.
Prepare and issue an anti-fraud policy to communicate a strong fraud prevention message to staff providing clear guidelines for preventing, detecting and dealing with fraud.	Put in place appropriate measures for general user and restricted access across the organisation: privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce multi-factor authentication where appropriate.	Conduct regular data audits to understand whether file structures are adequate and whether IP data is being saved in accordance with the business file structure, to avoid any unnecessary vulnerabilities or incomplete backups.
Carry out pre-employment checks for new recruits, follow up on two independent references and verify personal information and background details.	Identify valuable assets and reduce the chances of those assets being defrauded or stolen by rogue employees.	Establish managerial oversight to ensure that one person cannot transfer high-value assets by themselves or without sign-off.
Get to know your people and what motivates them. Look for signs that may indicate that they are unsettled, disgruntled or dissatisfied with their role in the business.	Conduct a scenario analysis with very carefully selected attendees, where the scenario examines a member of staff deciding to go and work for a competitor and deciding to take whatever IP he/she can access with them.	Consider using a specialist third party/contractor to look for a trail of digital IP theft by way of a USB memory stick, portable hard drive, email attachments and cloud storage (such as Google Drive or Dropbox).



Above: US and Chinese companies are in dispute over alleged IP breaches in the motor industry

“ Time and energy need to be expended to understand the complete picture of the business’s desired IP protection

of Tesla, stole key details from their self-driving car project and took them to Guangzhou-based Xpeng Motors, a Chinese electric vehicle start-up. Tesla says Cao uploaded a complete copy of the company’s self-driving source code to his personal Apple iCloud account (amounting to more than 300,000 files and directories) with the intent to share them. Xpeng replied that it was investigating the issue and that it “has by no means caused or attempted to cause Mr. Cao to misappropriate trade secrets, confidential and proprietary information of Tesla,” and that it was “not aware of any alleged misconduct by Mr. Cao.”

In cases where there has been proven IP theft, companies have found the markets they operate in flooded by cheaper products resulting in a drastic shrinking of their order books and the need to make very extensive redundancies. Alleged theft of IP by Chinese individuals is not confined to the US but has impacted companies across Europe as well. Such practices are prevalent globally, which is why UK businesses need to be alert to the threat and constantly vigilant to protect against IP theft.

Risk assessment


When conducting a risk assessment of the potential impact of the loss of IP, there are subjects which


immediately spring to mind, such as the discernible costs associated with a technical IT investigation into how the IP theft occurred during a cyberattack and the increased cybersecurity measures that have to be put in place to remedy the identified shortfalls. However, there are a myriad of other less discernible costs arising from a loss of IP which are not so readily quantified as they commonly emerge over time. They are labelled costs; however, they commonly relate to a loss of revenue due to a loss of market share followed by a fall in sales reducing the funds available for reinvestment in research and development. This reduced reinvestment is the start of a vicious cycle whereby the business’s ability to differentiate its products from its competitors is reduced leading to a fall in market share.

Risk response measures

Time and energy need to be expended to understand the complete picture of the business’s desired IP protection and the individual pieces of the puzzle that are already in place and those that are missing and need to be added. As a minimum, there needs to be an understanding of the elements of people, systems and data. While systems and data are important, the behaviour of personnel and developing the right

business culture are paramount in the fight against IP theft. Included here is a small sample of the risk response actions that businesses should consider implementing to protect against theft of IP.

Understanding IP fraud needs to be an integral element of enterprise risk management. Risk managers need to ensure that tackling fraud is undertaken in a collaborative way across all of the business departments and professions affected from (for instance) human resources to cybersecurity, data management, business continuity planning, crisis management, regulatory compliance, media management, patents and insurance. Fraud risk management is a good example of where an integrated risk management approach is a must and silo risk management would be ruinous. 

 Robert Chapman is a director of Dr Chapman and Associates Limited. He is the author of *Simple tools and techniques for enterprise risk management, 2nd Edition*, which is recommended reading by the IRM. A discount of 30% can be obtained for the hardback version through the publishers John Wiley and Sons using the promotional code RMD30 and the URL: bit.ly/2NGSJS6. Select country of residence in the tool bar. The discount is available globally until February 28, 2022.

Complex manoeuvres

Procurement in the Ministry of Defence demands rigorous risk management procedures at every stage of an item's life cycle

..... BY TOM CLARE

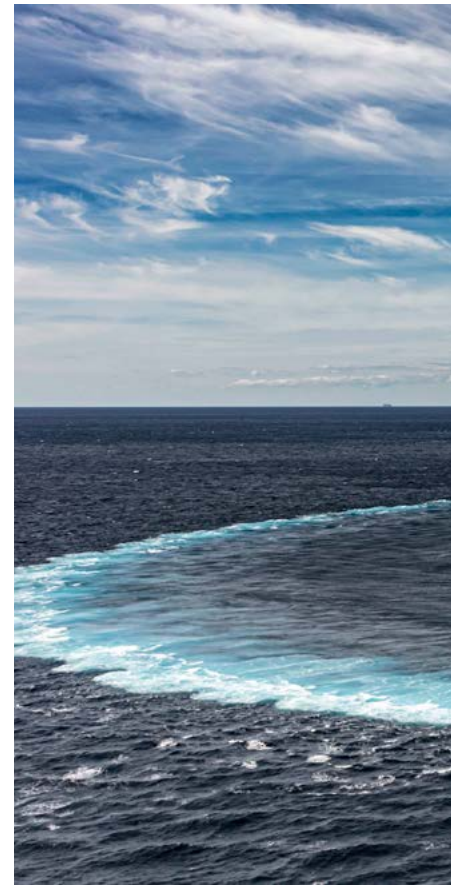
Defence Equipment and Support (DE&S) is a highly specialised part of the Ministry of Defence. From the procurement of clothes to carriers, rations to rifles, we ensure the UK armed forces – the Royal Navy, the British Army and the Royal Air Force – have the equipment and support they need to carry out their duties. Employing over 11,500 civil servants, military personnel and private contractors, operating with an annual budget of circa £10 billion, there is an active risk management community of about 130 individuals to support the delivery of these complex projects, programmes and portfolios of work.

The CADMID Cycle

.....

The delivery of equipment for the armed forces is a complex task requiring a clear understanding and expectation from how an idea is formed, through to its approval, delivery, use by the customer and eventual disposal. One way in which equipment is delivered in the organisation is through a series of phases called the CADMID Cycle – Concept, Assessment, Demonstration and Manufacture, In Service and Disposal – with each stage requiring the risk manager to adapt their approach (See diagram on page 26).

Large-scale projects, like the Queen Elizabeth class carriers, can remain in one stage of the life cycle for years owing to the complexity of the design, and a risk manager could spend their entire time in that team in one phase. In contrast, some projects could progress in much shorter timelines, owing to the operational need or



A project can remain in one stage of the life cycle for years owing to the complexity of the design

.....



Above: HMS Queen Elizabeth (with Merlin helicopters and F-35B jets on the flight deck) performing a hard turn whilst on Exercise WESTLANT 19.

comparative simplicity of the project.

The challenges for the risk manager in each stage can vary, requiring consideration as to how to work with leadership teams and risk owners in the most effective way at each stage to maximise the likely benefits that effective risk management can bring to a project's delivery.

Concept and assessment

In the *concept phase*, there is an idea that we are seeking to develop. This could be a new class of armoured vehicle, or a new fighter jet for example. In this stage, a delivery team is formed, and the organisation is seeking to develop user requirements – how this equipment needs to perform – involve industry, identify potential technological and procurement options and set out the process in terms of funding as to how this could be achieved.

At the end of this phase, a business case is submitted for approval outlining the progress to date and planned next steps, with cost, time and performance considerations – a

project's "Initial Gate". Assuming approved, the team then moves to the *assessment phase*. Here we establish further detail on how the equipment needs to perform, understanding the systems that are required to meet this to maximise achievement of the user requirements while ensuring value for money for the taxpayer. This is developed into a full business case, proposing approval for the delivery of equipment split over phases within tightly defined performance, time and cost boundaries at its "Main Gate".

Considerations for risk managers one

For a risk manager at this stage, there can be significant challenges in such uncertainty. The idea may have never been considered before – what risks are associated with the available technology? Is there a likely supplier base? How clear are we on the requirements of the idea?

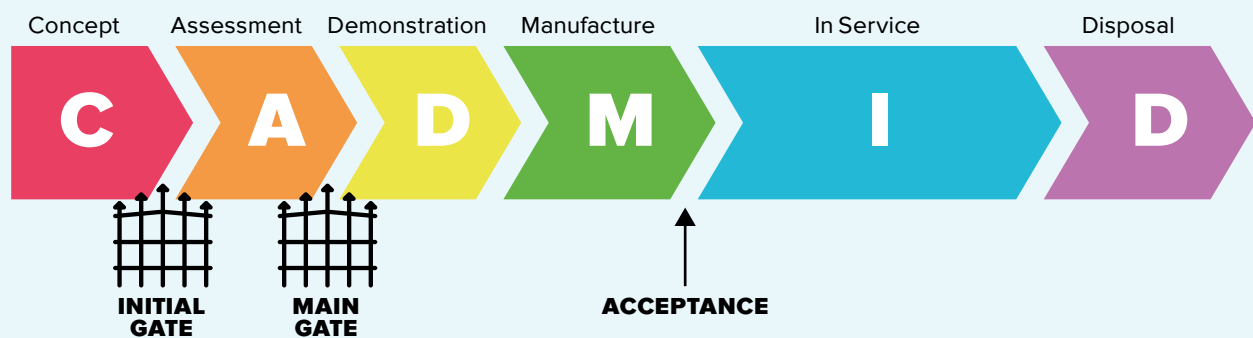
A risk manager could consider the standard toolset of prompt lists, checklists, workshops and interviews across the members of the team.

These, however, may result in risks that feel too broad to be useful – a risk around "Technology available to deliver the equipment" may result in a "so what?" response at senior levels if not articulated appropriately. If we consider risk management to be at its best a tool to make more effective decisions, the risk manager could prove their value by encouraging the development of more engaging risks during these uncertain phases.

Individuals enjoy sharing their experience and advice. Rather than delving through all too often stale "Lessons Learnt" logs, an interactive session with relevant owners to highlight how something was completed from different but comparable projects in size, cost or complexity could be a rich source of information in the absence of harder data to get their first understanding of a risk register for the new project.

The risk manager can then support the team through the development of appropriate assumptions and dependencies to generate more detailed, useful risks that help navigate

THE CADMID CYCLE



“ It is key for a risk manager to open up their approach and be confident in interacting with industry partners, not only to share information and knowledge, but to be able to provide constructive challenge

this stage. It may, for example, highlight the need for studies to understand a concept through scientific research, or prototypes to understand how the delivery of the equipment could be achieved.

Demonstration and manufacture

In the *demonstration phase*, DE&S moves to its first steps of delivery. The team seeks to progressively de-risk potential threats to manufacture, to test the design and understand how the expected systems are working and whether they are likely to deliver the requirements we need. At this point, contracts may be set up with suppliers after a competitive process has been held, and interaction will begin with likely industry partners to further understand the equipment's anticipated delivery. At the demonstration phase, the team and supplier may seek to potentially provide prototypes of the equipment, or a limited manufacture run to start understanding the reality of delivering the equipment.

As the equipment moves into its *manufacture phase*, larger-scale

production is now in flow as we seek to deliver within the time and cost limits set out in the Main Gate business case at the end of the assessment phase. This phase may be broken into tranches of delivery, with milestones of Initial Operating Capability (IOC) as the equipment passes acceptance trials and becomes available for use by the customer, eventually leading to Full Operating Capability (FOC) as an agreed quantity of equipment is now performing as desired.

Considerations for risk managers two

It is key for a risk manager to open up their approach and be confident in interacting with industry partners, not only to share information and knowledge, but to be able to provide constructive challenge to them to ensure they are assisting the delivery team seek the best value for money possible for the taxpayer.

The supplier should not be the foe, rather an integral partner to delivery with a positive, collaborative relationship in place. These times will undoubtedly have challenges. Testing may not go as planned,

unforeseen challenges may emerge, but key to the successful resolution of these between our organisation and the supplier is this relationship.

The risk manager must take steps to do this – visit your supplier if you can to develop a professional relationship and be honest in terms of risk register content, within any commercially sensitive or legal considerations, to share and resolve problems together.

In doing so, the risk manager has the opportunity to conduct highly valuable joint assurance activities such as a combined schedule risk analysis, where you can find a realistic confidence level of when key milestones may be achieved and have the opportunity to ensure effective risk interventions can be made to maximise the likelihood of delivery when desired.

In-service and disposal

Through rigorous trials and acceptance periods, the equipment has been accepted and the user is able to benefit from this new capability from the team, and we move into the *in-service phase*.

The team's job is to now maintain this equipment to ensure the user continues to have an appropriate quantity for operations. This could be ensuring a certain percentage of a helicopter fleet is available, or there are an appropriate number of items at readiness to be deployed. The in-service phase can be relatively short to meet an urgent requirement, or for significant periods of time, such

as the Queen Elizabeth class aircraft carrier, which is anticipated to be in service for the next 50 years.

At the disposal phase, the equipment has come to the end of its operational life. This may be through a long length of service – for example, the Sea King helicopter, retired in September 2018 after nearly 50 years of service. Alternatively, it may now be surplus to operational need, or no longer practical to operate. There are typical two routes at this stage – either safe and effective dismantling and disposal of the equipment, or where practical, DE&S may seek to get a return to the taxpayer by arranging its sale to partner nations.

Considerations for risk managers three

During the in-service phase, a team will often be in an issues-management frame of mind – as and when items may break, or need replacing, the team must have the right arrangements in place with suppliers to ensure the user continues to have access to the equipment.

This may feel like the risk manager could be side lined, but at this time the consideration of the controls in place to enable the smooth operations of the contract is essential. There may be fewer tangible milestones in a plan to define a risk event, but it is vital there is confidence in a supplier's ability to manage demands placed on them, such as a surge capacity for repairs, or impacts of major external events, providing assurance that they can continue to perform the vital role required of them to maintain the capability to ensure required quality and quantity.

At the disposal phase, consideration of the legacy of the equipment is essential. If the equipment has been in service for years, are there environmental considerations in its safe disposal? Do we have the confidence and assurance that the appropriate controls can be in place to dispose of it in line with all relevant legislation and societal expectations?

If we are seeking to sell the equipment, are there uncertainties around the quality or condition of it? Perhaps mitigation plans are required to ensure the equipment remains fit for purpose to enable

a sale. Alternatively, with the age, original equipment suppliers may no longer be available for spare parts. Are there risks around obsolescence issues that also need to be considered to ensure an effective disposal?


Wider applications


Although this article focuses on a very specific sector, many organisations will adopt a similar life cycle/phased approach to delivering their outputs and services, and a risk manager is likely to see comparisons in their industries across the board.


The complexity of a risk manager's role in defence equipment procurement is varied, and the assumption that one approach fits all phases would not help maximise the opportunity to deliver to performance cost and time parameters and demonstrate how the risk management profession can aid effective project delivery.

It is vital that in their practice a risk manager considers the phase of a project they are working in. Have the confidence to utilise a range of skills and techniques, adapting your message accordingly – there isn't one size fits all to gain that all-important engagement in the process with team members and other stakeholders.

Although a useful foundation, a risk manager should not just rely on the age-old staples of checklists, prompt sheets and forms to perform their role from afar. They should be an advocate for the risk profession – partnering up to the business,

applying their skill set in new and creative ways and utilising people skills to get the information needed to provide the risk management service their business or delivery organisation can truly benefit from. 

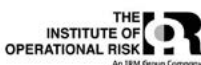
 Tom Clare CFIRM, is a senior risk manager for Defence Equipment & Support, an organisation within UK Ministry of Defence responsible for procuring and supporting defence equipment for the UK armed forces. For further information on this organisation, please visit www.des.mod.uk

 There isn't one size fits all to gain that all-important engagement in the process with team members and other stakeholders

Is a career in risk management in your sights?

The Institute of Operational Risk's Certificate in Operational Risk Management (CORM) has now been approved for ELCAS funding.

This Level 5 course is a self-study workbook supplemented with workplace reflection and learning activities, providing candidates with a foundation in operational risk management. Increase your earning potential and chances of career progression.



To find out more, please visit:

www.ior-institute.org



Risk management's transformations

Risk managers have coped well during the pandemic and look set to enjoy an expanded role in many organisations, according to latest IRM's COVID-19 survey

..... BY CAROLYN WILLIAMS

It is just over a year since the UK experienced its first lockdown in an attempt to stem the impact of COVID-19. An early IRM poll of risk managers (see "Risk management in the global crisis", *Enterprise risk*, Summer 2020), showed that 98 per cent were still in post and working effectively at home. Most organisations (89 per cent) said they were either very satisfied or satisfied with their responses to the crisis.

A year on and opinions have shifted, but not significantly. The number of businesses saying that they were satisfied with their response has dropped by about 7 per cent, according to the most recent IRM poll. Those reporting to be very satisfied has fallen from 36 per cent to 25 per cent, suggesting that more operational snags have arisen between April 2020 and December 2020 when the surveys were conducted.

Working well

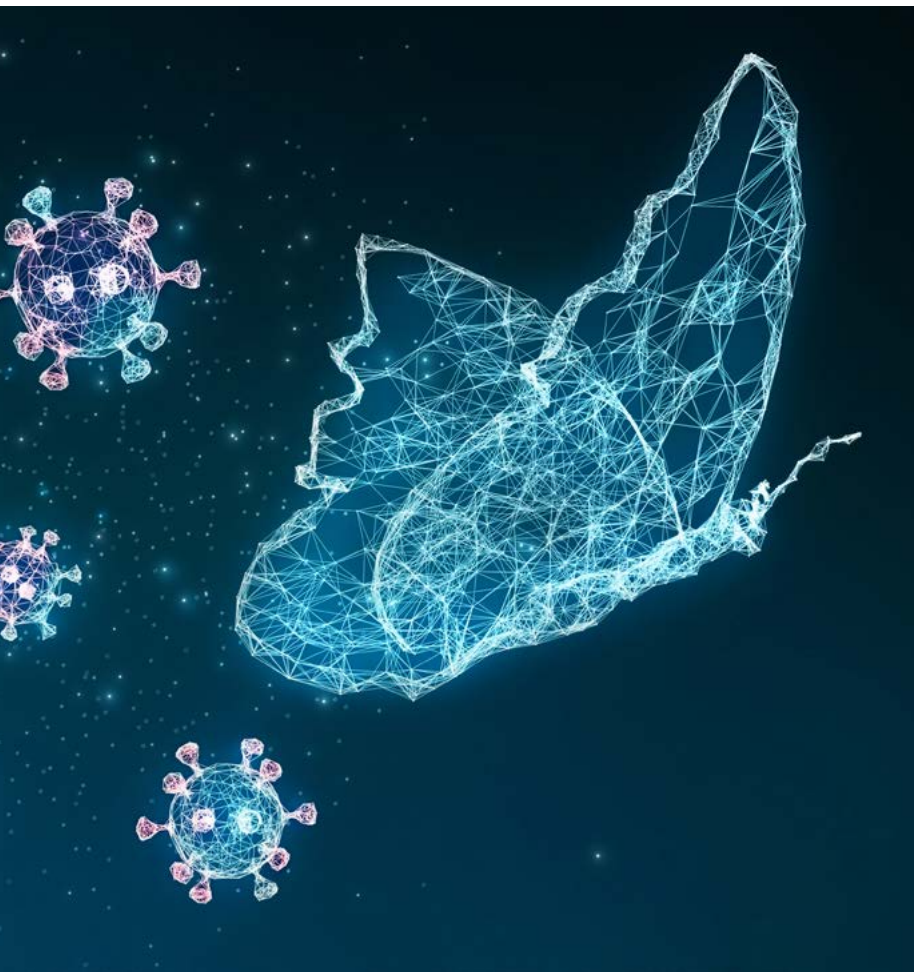
.....
"Our survey research indicates that although only a small proportion of firms had precisely anticipated and planned for pandemic risk, their more generic business continuity and crisis management plans generally worked well," Iain Wright, CFIRM IRM chair, says.

"Whatever the crisis that presents itself, a conscious combination of great leadership, great communications and great IT support helps firms both manage the risks



Although only a small proportion of firms had precisely anticipated and planned for pandemic risk, their more generic business continuity and crisis management plans generally worked well





45 per cent said of respondents said they planned to take qualifications in risk management

.....

Respondents said that robust continuity plans and work done on resilience were helpful factors in responding to the crisis. In fact, greater focus on building operational resilience is the highest pandemic-driven change in risk management for 93 per cent of respondents, followed by greater board-level interest in strategic risks at 86 per cent and integration of business continuity planning into ERM at 78 per cent. Finally, 83 per cent of respondents said they would be undertaking a review of their strategic plans and risks in response to the crisis (a similar figure to the April 2020 survey).


Stronger

.....

Most (96 per cent) of respondents felt that the case for risk management had been strengthened by the pandemic experience. That is reflected in over half (56 per cent) saying that they expected their risk management budgets to increase – with 17 per cent of those expecting a greater than 10 per cent increase.

The pandemic is likely to leave a long-lasting legacy – and risk managers in the survey shared their future expectations. Most said they expected to continue working from home (73 per cent). Education was also high on the agenda: 45 per cent said they planned to take qualifications in risk management, and 38 per cent said they would take other forms of qualifications to improve their skills and marketability. Those aspirations point to the increasing professionalisation of the risk sector. 📖

.....

 Carolyn Williams is IRM's director of corporate relations. The full survey will be published on the IRM's website by the end of March.

and exploit the opportunities.”

Organisations seem to have coped better with the second lockdown, according to anecdotal comments from the poll. Working from home had never been tried on such a scale in the UK and has generally been considered an innovation that has worked well so far. In addition, communication improved.

“There was a lack of information and clarity during the first phase of the crisis as we all (central government and our organisation) were defining [things] as we went so were largely reactive in response,” said one respondent. “The second lockdown in August was much calmer as we knew what to do and had successfully responded earlier.”

Another said: “The plans worked well but only because of a concerted effort across functions and senior management. If the pandemic had affected working age people more than it did, we (and others) would have found it harder

to implement and adapt plans.”

Some businesses have taken this new model of home-working seriously enough to begin reviewing their property portfolios with a view to ditching expensive city-centre office space. But the stresses of homeworking and risk of longer-term mental health issues have not yet been properly risk assessed in most businesses (see *Mail chump*, page 38).

Reviewing risks

.....

Four in ten risk managers reported no change to their roles because of COVID-19. But 37 per cent said they were now providing risk advice in relation to crisis decision-making. An equal number reported that they were reviewing their organisation's risk management policies and processes as a direct result of the pandemic. Some 28 per cent of risk professionals expect the changes to their roles as a result of COVID-19 to be permanent.

Business travel after Brexit

The end of free movement across Europe is likely to bring new compliance risks and extra work for risk managers

..... BY ELAINE MCILROY

The end of the Brexit transition period has had many impacts for business. Some multinational businesses operating across the UK and the EU may not have fully anticipated the need to give far greater thought and planning to international business travel and visa requirements. The end of free movement has also given rise to new business risks as employers now have to consider and navigate the immigration requirements applicable in each member state within the EU before sending staff to work or for business trips. Ensuring compliance in this area is likely to result in increased costs as businesses may need to take local legal advice in order to ensure that they comply with local laws. It may also give rise to civil and criminal liabilities as well as reputational risk if businesses do not comply with immigration requirements across different jurisdictions. That is the case whether businesses send staff to Europe from the UK or vice versa.

The new rules

.....

Before the Brexit transition period ended, resulting in the end of freedom of movement, UK, EEA and Swiss citizens could travel across the EEA and Switzerland for



The end of free movement has given rise to new business risks

.....





business trips or for the purposes of work without the need to apply for any sort of work permit. They could stay for unlimited periods of time, and there were no restrictions on the sorts of activities that they could do. That was the case whether someone was engaged on a self-employed basis or as an employee. That has now all changed.

Freedom of movement ended at 11pm on December 31, 2020. From that point on, EEA and Swiss citizens coming to the UK for business visits will have to comply with the requirements in the UK immigration rules on business visits. They will have to take care to ensure that only permitted activities are undertaken and that no work or other prohibited activities are performed unless the person has some sort of work visa.

Similarly, businesses sending UK citizens to the EEA and Switzerland

for business trips will now have to comply with the rules on short-term business visitors in the country being visited. That will involve ensuring that any activities to be undertaken comply with local requirements. In addition, it will also involve limiting the amount of time spent to ensure that the rules on visa-free travel are complied with.

The new Trade and Co-operation Agreement (TCA) that was entered into late in December 2020 included reciprocal provisions relating to short-term business visitors to the UK and the EU. The European Union (Future Relationship Act) brought the relevant parts of the TCA into UK law with effect from January 1, 2021. On the EU side, the agreement is being applied provisionally pending ratification. Some aspects of the arrangements on visa-free travel between the UK and the EU had already been agreed even



The TCA contains some exceptions to the general rules, which specific member states have negotiated

.....



Any business trips are likely to require planning and will in some cases require legal advice

PERMITTED BUSINESS ACTIVITIES

- 1 Meetings, conferences or consultations with business associates;
- 2 Certain research (including market research) and design activities;
- 3 Training seminars (providing the training covers “techniques and work practices which are utilised by companies or organisations in the territory being visited”; and the training complies with the conditions in the rules);
- 4 Trade fairs and exhibitions for promoting company products or services;
- 5 Certain limited sales activities, such as taking orders or negotiating the sale of services or goods; entering into agreements to sell services or goods. However, delivering goods or supplying services is not permitted;
- 6 Purchasing goods or services for an enterprise;
- 7 Certain after-sales or after-lease services essential to a contractual obligation or pursuant to a warranty or other service contract incidental to the sale or lease of commercial or industrial equipment or machinery, including computer software;
- 8 Commercial transaction activity: management and supervisory personnel and financial services personnel (including insurers, bankers and investment brokers) engaging in commercial transactions;
- 9 Tourism personnel attending or participating in conventions or accompanying a tour that has begun in the UK;
- 10 Translation or interpretation services provided by employees of a UK organisation.

before the TCA was agreed. Having these business visitor provisions as part of the TCA is useful for international businesses as it should provide some consistency across the UK and the EEA and Switzerland in relation to business visits and certain other types of specialist work permits which are provided for in it. However, This can make it difficult for businesses to understand what is permitted in each location. For that reason, local legal advice may be needed in some cases which can be costly – especially for businesses that operate in multiple jurisdictions.

Visa-free travel

The new arrangements permit British citizens to travel to the EU, Iceland, Liechtenstein, Norway and Switzerland for short visits of up to 90 days within any 180-day period without requiring a visa. In most cases, what is relevant is the total amount of time spent across all of

the countries concerned. There are separate 90-day limits for Bulgaria, Croatia, Cyprus and Romania. No prior travel into EU countries before January 1, 2021, will be considered towards the above periods.

British citizens who wish to stay for longer than 90 days, or intend to carry out certain activities that are not permitted under the short-term visit rules (including working), will need to comply with the EU immigration requirements that apply to non-EU nationals (third-country nationals), as well as the national laws of the relevant member state. That may involve obtaining a work permit under local laws.

Short-term visitors

The TCA specifies that British citizens who are travelling for business are permitted to stay in the EU for a period of up to 90 days in any six-month period. However, whether or not a work visa will be required will

depend on the rules of the country being visited and the type of business activity being carried out. Below are business activities that are generally permitted under the TCA. However, there are some exceptions included for specific countries which makes the rules more complex. It should be noted that British citizens will require to have a minimum of six months left on their passports to travel to the EU.

Permitted business activities

There are defined types of business activities that are generally permitted during short-term visits to the EU in the TCA (see Permitted business activities).

There are restrictions in place to prevent business travellers selling goods and services to the public, receiving remuneration locally and engaging in the supply of a service in a contract with a consumer if the business is not established in that country. Business travellers seeking

to carry out these activities are likely to require a work permit from the country that they will be visiting.

Additional provisions

The TCA contains some specific provisions about those setting up a business in another country. If business travellers are visiting for “establishment purposes” – to set up a business in another territory – they will not generally need a work permit for entry and temporary stay of up to 90 days within any six-month period. This is only applicable to those travellers in a senior position. During this time, the business visitor must not offer or provide services or engage in any economic activity other than that required for establishment purposes, and they must not receive remuneration from a source located within the EU. There are also specific rules in the TCA relating to contractual service providers and independent professionals.

The TCA also includes provisions that deal with the circumstances in which certain employees of multinational businesses can obtain an intra-corporate transferee permit. Managers or specialists which fall under the definition in the TCA will usually be permitted to stay within the EU for up to three years, and trainee-level employees will be permitted to stay for up to one year.

In-bound visits to the UK

EEA and Swiss nationals travelling to the UK can participate in a variety of business activities without a visa including attending meetings, events and conferences. In the majority of cases, they will be permitted to stay for up to six months, but in practice business visits will usually be far shorter – a longer trip may indicate that the person is working, which is prohibited by the rules. During that six-month period, they will be able to enter the UK multiple times, but they must not live in the UK by means of successive visits.

Certain types of business activity are not permitted as a visitor including (1) carrying out paid or unpaid work for a UK company or as a self-employed person; (2) carrying out a work placement or internship;

or (3) selling directly to the public or providing goods and services.

Challenges and implications

The end of freedom of movement between the UK and the EU has given rise to a number of challenges for businesses operating across Europe. Previously, there was a single set of rules which were simple to understand for EU citizens – they could live and work in any country for as long as they wanted to. Business travel across the EEA and Switzerland had no limits in terms of the amount of time an employee could spend or the activities they could do. No advance planning was required for a business trip, and local legal advice was unlikely to be required. There was little or no paperwork required to work in other jurisdictions.


The challenges that have arisen as a result of the end of freedom of movement are considerable. There is no longer a consistent approach across the EU to UK business travel. Although there are standard rules applicable in terms of the amount of time that someone can spend on a visit, the list of activities which are permitted can vary. In this sense, the rules have become more complicated. Any business trips are likely to require planning and will in some cases require legal advice. In some cases, the activities may not be permitted under the visit rules, in which case a work permit may be required.

Consequently, seeking local advice in relation to business travel into an EU country may be required as not all EU countries adopt the same rules as to what travel is permitted without a work visa or permit. This will present a cost to employers, particularly if more than one country or type of business activity is concerned.


At the moment, with coronavirus and travel restrictions in place, this is an added complexity for business travel. While many travel plans have been on hold due to COVID-19, it is likely that the real impact of the end of the Brexit transition period will be felt once international travel for business purposes resumes.

Minimising risks

It will now be important for businesses to ensure that their

employees who are travelling for work to the EU keep track of the time that they spend there. Monitoring will be important to be able to plan business travel to ensure compliance with the rules. It will also be important to understand the rules of the country that will be visited and to ensure that there is time to seek advice where necessary. Employers should also consider their insurance provisions for business travel such as travel insurance, health insurance or any other work-related insurance. 

 Elaine McIlroy is a partner at Brodies LLP Solicitors. She heads Brodies' immigration offering and acts for employers across the UK. She regularly advises on the implications of Brexit.

 **Monitoring will be important to be able to plan business travel to ensure compliance with the rules**

Boosting online learning

After over a year of pandemic lockdowns across the world, IRM trainers and students find themselves in a changed landscape of online training and risk workshops

..... BY JOHN CRAWLEY

From the beginning of the pandemic lockdowns in 2020, I and my fellow risk management colleagues put in place a model for online training for IRM events. This model has been refined and perfected over the many training sessions held during the year and has been universally embraced by participants. So, what are the tips and lessons learnt?

Lead differently

.....

All presenters – both trainers and risk meeting facilitators – have needed to learn how to lead differently. The biggest change from face-to-face interactions to the online environment is the loss of non-verbal cues. A huge percentage of our communication is non-verbal. This is a significant loss to any presenter and needs to be replaced with alternative methods of checking in with participants to ensure that the content and messages are understood.

The simplest and most effective way to do this is verbally to check in with participants frequently. Train the Trainer expert Annie Clarke, of Annie's Training Company, says: "You need to regularly (and by regularly I mean every five minutes) engage your [participants]. Speaking at them doesn't cut it in this new virtual world."

We have found the use of two presenters to be very powerful. You can open up two lines of communication with your participants: one presenting while the other answers



The biggest change from face-to-face interactions to the online environment is the loss of non-verbal cues

.....





Online training is much less of an intrusion into participants' personal time

.....

much less of an intrusion into their personal time. Another positive consequence has been the increased diversity in training rooms across different cultures and nationalities.


Online generally means training and meetings are attended from home. This brings its own challenges. A year ago, we thought it was amusing when a BBC presenter's children entered the room while he was broadcasting. Today, it is normal to see children, small animals and other household members on screen. We need to allow for this in how training and meetings are structured. Shorter, more intensive periods of learning interspersed with more breaks have worked best for participants.

It is important to remember, particularly in these stressful times, that fun and laughter are by far the best ways to maximise participant engagement. There is no end to the creative potential here from impromptu dance breaks if a specific song is played, to a requirement that any small animal that wanders by be introduced to the group.

An ice-breaker exercise that we find extremely useful at the beginning of a session is to ask participants to run around their house while some upbeat music is played and bring back two items that begin with the first letter of their name. The participants are then challenged to use these items to introduce themselves and explain what they wish to get out of the training.

Ultimately, a successful move from face-to-face to online interaction is about using all the tools at your disposal to create the right communication and learning environment for the participants. 🎧

.....

 **John Crawley, IRMCert, is the lead partner in Expert Partners, a boutique consulting and advisory practice in the area of organisational risk, strategy and turnaround. He is also one of the IRM's principal trainers.**

questions using the chat facility. Polls and thumbs-up-or-down reaction buttons are very useful complementary tools, when used correctly.

Content and agendas

.....

Training and meeting facilitation is a fundamentally different prospect when being delivered online. Do not dust down your PowerPoint slides from an in-person training course or workshop and expect them to work online. Periods of engagement need to be shorter and more bite sized. There needs to be much stronger signposting so that your participants do not get lost.

Every participant has a much better view of the screen than was possible from the middle or back of a classroom or meeting room. This does mean you can deal with more complex diagrams and infographics. However, it is important to remember that even though participants may be able to see the slides more

clearly, it is not acceptable to fill the screen with too much text.

For online training, an accompanying workbook or journal is an invaluable way for participants to reinforce their learning and capture the course content for later use. Presenters need to think about different ways of dealing with content. Can it be dealt with through song or dance? Can it be physical action activities? Or can it be small-group discussions that you previously had around a table that you now do in a virtual breakout room?

Participants

.....

From a participant's perspective, one of the greatest advantages of online training is increased accessibility. Participants no longer have the time-consuming and sometimes costly inconvenience of travelling to a training centre, which for some made accessing training an impossibility. The feedback from participants has been that online training is

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

Governance, risk management, and compliance software



OneTrust GRC enables risk, compliance and audit professionals to identify, measure, and remediate risk across their business to comply with internal rules and external regulations. With OneTrust GRC, companies can seamlessly integrate risk management into their day to day activities. OneTrust GRC is a part of OneTrust, the #1 most widely used privacy, security and third-party risk

platform trusted by more than 6,000 customers and powered by 100 awarded patents. To learn more, visit OneTrustGRC.com or connect on LinkedIn.

 **Scott Bridgen**
 **+44 (0) 7554 515 343**
 **sbridgen@onetrust.com**
 **www.onetrustgrc.com**
 **Dixon House**
1 Lloyd's Avenue
London
EC3N 3DQ

Reporting and compliance software solutions



Workiva Inc. (NYSE:WK), provider of the world's leading connected reporting and compliance platform, is used by thousands of enterprises across 180 countries, including 75 percent of Fortune 500® companies, and by government agencies. Our customers have linked over five billion data elements to trust their data, reduce risk and save time.

 **Tim Le Mare**
 **+44 (0) 203 868 0550**
 **info@workiva.com**
 **www.workiva.com/uk**
 **14 Gray's Inn Road**
London
WC1X 8HN
United Kingdom

Risk management software



Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while bringing new ideas and advanced features to the RMIS market. Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use, providing integrated solutions to the entire

insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage total cost of risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com

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

Risk management software



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

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

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

Risk management training



As the world's leading enterprise risk management institute, we know what great risk management looks like, and what risk management professionals need to know, do and deliver to succeed. What's more, we understand how training works and we are experts in designing and delivering courses that provide the tools and motivation to

make change happen. Our short courses and tailored in-house learning and development solutions support hundreds of organisations every year, both in the UK and internationally. Some courses, like the Fundamentals of Risk Management, cover the broad range of ERM skills, whilst others take an in-depth look at specific topics, e.g. Risk Analysis, Risk Appetite and Tolerance, Managing Risk Culture, and Identifying Key Risk Indicators. Members can also benefit from a new suite of e-learning courses, which are now available on our website.

 **Sanjay Himatsingani**
 **+44 (0) 20 7709 4114**
 **sanjay.himatsingani@theirm.org**
 **www.theirm.org/training**
 **IRM Training
Sackville House,
143-149 Fenchurch Street,
London, EC3M 6BN**

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

Mail chump

Communication technologies are making us unhappy and less productive. It is time to rehumanise our digital lives

In Philip K Dick's 1969 novel *UBIK*, Joe Chip walks into a chemist to buy a spray can of *UBIK*. Applied liberally, the contents of the can prevent objects from regressing to a prior technological form of development in a world travelling backwards in time. For example, spray some *UBIK* on an electric car to prevent it becoming petrol-driven, and on that car to prevent it becoming a horse and cart.

Except, by the time he arrives at the store, the spray can has become a tin can containing powder. When Chip goes to pay with his credit card, the cashier asks: "What is a 'credit card'?"

Nightmare vision

Dick's technologies evolve historically through a series of steps and come closer each time to a kind of ideal form. But homeworkers today may dream wistfully about his entropic nightmare of disappearing gadgets – without the *UBIK*. That is because trends identified by a new slew of research show that the way we communicate in an online world creates too much anxiety and self-evaluation. The pandemic has intensified such side-effects.

Videoconferencing, for instance, has been a boon to organising collaborating remotely over the past year. But seeing yourself on screen and having "excessive amounts of eye contact" can be extremely fatiguing, according to Stanford Virtual Human Interaction Lab professor Jeremy Bailenson.

He likens the experience of using platforms such as Zoom to public speaking: "Social anxiety of public speaking is one of the biggest phobias that exist in our population. When you're standing up there and everybody's staring at you, that's a stressful experience." Similarly, many people



“ The longer one spends on email in [a given] hour the higher one's stress is for that hour

.....

do not like looking at themselves in a mirror – which is the same as seeing your image on screen, potentially for hours on end. "There are negative emotional consequences," he says.


Under fire

Email has also come under fire. "The longer one spends on email in [a given] hour the higher one's stress is for that hour," researchers at the University of California, Irvine, found. It shows, according to the tech writer Cal Newport, that "email is making us miserable."

In his forthcoming book, *A world*

without email, he argues that the problem is not the technology itself, but the way too many organisations have used it to create an always-on work culture. The pleasure of going on holiday, for instance, can be almost negated by the thought of a burgeoning inbox waiting at home.

Newport calls much of this behaviour "unstructured communication". Organisations should look for better ways of using their tools. Basecamp, a software development company, gave technical experts office hours. That meant co-workers could not send an email outside of those times. Workers did not seem to mind waiting, and the technical crew's productivity increased.

Such studies remind us that it is important to rehumanise our digital interactions. Technology does not evolve from good to better automatically, as Dick implied, but needs reconfiguring and restructuring – or even replacing with something less stressful. Wouldn't it be nice if an intern of the future could ask, "what is an email?" 

IRM specialised risk management certificates

Study with us to develop your career, knowledge and network



Digital Risk Management Certificate



Supply Chain Risk Management Certificate

Enrol onto a specialised IRM risk management certificate

Effective risk management is crucial to every organisation's viability and reaching objectives spanning cyber, financial, operational, supply chain, people and reputation risk to name just a few. Cyber risk and supply chain risk are vital components to maintaining an organisation's risk resilience.

What our students say



Robert Luu

Director of Customer Success, Galvanize, Singapore

"Whether you're directly in risk management practice or not, it is a great program 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."



Emma Duggan

Risk Manager, Experian, United Kingdom

"The IRM's Digital Risk Management Certificate is extremely relevant to my role and I would urge risk professionals to consider it. It is very relevant for anyone working in technological development, as risk is everyone's responsibility."

Find out more at:

www.theirm.org/qualifications

Resilience, risk and recovery



Developing risk professionals

IRM's revised International Diploma in Risk Management

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



About the International Diploma in Risk Management

For 30 years, IRM's International Diploma in Risk Management has been the global choice of qualification with risk professionals and their employers. The IRM has revised the syllabus for the International Diploma to ensure our students are informed of the best practices in risk management. Students will benefit from our new online learning platform, the Virtual Learning Environment (VLE). The VLE supports students step-by-step through the modules and provides activities and quizzes to help master the subject matter. Students can submit their assignments when they are ready, no more exam centres.

Benefits of the International Diploma

- Gold standard in ERM qualifications
- Global recognition
- Master's level equivalent qualification
- GradIRM designation with option to apply for CMIRM
- Designed to ensure you are current and competent

What's new about the International Diploma

- Students can enrol at any time
- Learn from anywhere in the world via the VLE
- Access the learning platform via PC, tablet or mobile phone
- Assessed through practical work-based assignments that can be submitted online at any time
- Quicker (provisional) results on marked assignments
- Potentially shorter study time more suited to those who are working

What our students say



Helen Hunter-Jones, CMIRM
Chief Risk Officer, Pay.UK, United Kingdom

"I took the International Diploma in Risk Management and could not have got to the position I have without it. The IRM can provide access to many other practitioners and help build your professional network."

Find out more at:

www.theirm.org/diploma-mag

Resilience, risk and recovery

