Reputation matters
Damage to corporate reputation from cyber liability is front of mind

Book reviews
Digital transformation and anti-bribery procedures

Industry Awards
The winners of the 2017 Risk Management Awards

cirmagazine.com

January 2018

CIR

CONTINUITY INSURANCE & RISK

thinking resilience

The year ahead *CIR speaks to industry experts to find out what's in store for resilience professionals in 2018*

Digital enabler *Daisy's Andy Dunn talks to CIR about developments at the company and in business continuity*

Software Report *CIR's report examines some of the best ways to gather risk data from across the entire organisation*

Tomorrow's world

Shifting gears in risk

Industry view: "Employers must take care of staff safety and avoid exposing them to unnecessary risk"

Comment

Earlier this month, infrastructure contractor Carillion went into liquidation, after extended rescue talks with lenders and the government failed.

The UK's second biggest infrastructure company hit trouble after losing money on a number of large contracts and running up significant debts.

Within days of the collapse, the impact was already being felt. The firm employed 43,000 people worldwide, of which 20,000 were based in the UK.

Some 30,000 small firms that were working on Carillion projects in the private sector suddenly face problems as a result of the bankruptcy. The company is said to owe these businesses approximately £1bn in unpaid costs; and there is growing alarm that much of this money will be lost, leaving many more firms at risk of financial collapse.

Meanwhile, the company's 19,500 staff in public sector jobs will continue to be paid – at a potential cost to the taxpayer of hundreds of millions of pounds.

While we are yet to fully understand precisely what might have averted Carillion's collapse, there are a number of questions being asked about its management, as well as about the government's reliance on a small number of huge outsourcing firms, which poses a dangerous risk to national economic stability.

The UK's procurement regime is stacked against small firms. As chairman of the Federation of Small Businesses, Mike Cherry, points out, providing small businesses and the self-employed with more opportunities to secure public contracts would not only mean less risk, but a better return for the taxpayer.

At the very least, he says, we should see the reinstatement of the target date for achieving 33 per cent of all public sector procurement with smaller businesses to 2020.

Responding to the announcement of overdraft extensions, payment holidays and fee waivers from a number of banks for small firms impacted by Carillion's liquidation, the FSB says the emergency measures put in place by banks for customers hit by the collapse will provide some respite at a desperate time for hundreds of small firms. "Many hundreds more are still yet to feel the knock-on impacts of the giant's demise. It's critical that they also receive support in the months ahead," the small business group warned.

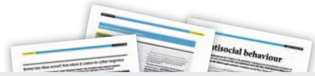
The Electrical Contractors' Association and the Building Engineering Services Association have issued a five-point action plan following the collapse, which includes a call for SME contractors already working on Carillion projects to be allowed to continue on these projects and be paid directly; a call for major public sector suppliers like Carillion to be precluded from winning any further contracts unless it can prove it pays its supply chain promptly; and a suggestion that public sector suppliers like Carillion worthy of their own government account managers and who rely on SME supply chains for successful delivery must be made to implement transparent supply chain payment systems, statutory public sector payment requirements, project bank accounts and no retentions, throughout the supply chain. It also calls for the government to monitor and enforce the public sector 30 day payment supply chain model as opposed to Carillion's own 126-day payment terms, which leaves thousands of SMEs struggling for cash flow to pay staff and suppliers.

Deborah Ritchie, Editor

Tomorrow's world 14

Shifting gears in risk

PERSPECTIVE PUBLISHING
PPA Publisher Member
abc Audit Bureau of Circulations Member
recycle When you have finished with this magazine please recycle it.



News, views & regulars

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

Editor
Deborah Ritchie
deborah.ritchie@cirmagazine.com
Tel: +44 (0)20 7562 2412

Associate publisher
Steve Turner
steve.turner@cirmagazine.com
Tel: +44 (0)20 7562 2434

Design & production manager
Matt Mills
matt.mills@cirmagazine.com
Tel: +44 (0)20 7562 2406

Publishing director
Mark Evans
Tel: +44 (0)20 7562 2418

Publisher
John Woods
Tel: +44 (0)20 7562 2421

Contributing writers
David Adams
Martin Allen-Smith
Graham Buck

Accounts
Marilou Tait
Tel: +44 (0)20 7562 2432
Fax: +44 (0)20 7374 2701

Subscriptions
Tel: +44 (0)1635 588 861
perspectivesubs@dynamail.co.uk

£189 pa in the UK
£199 pa in the EU
£209 pa elsewhere

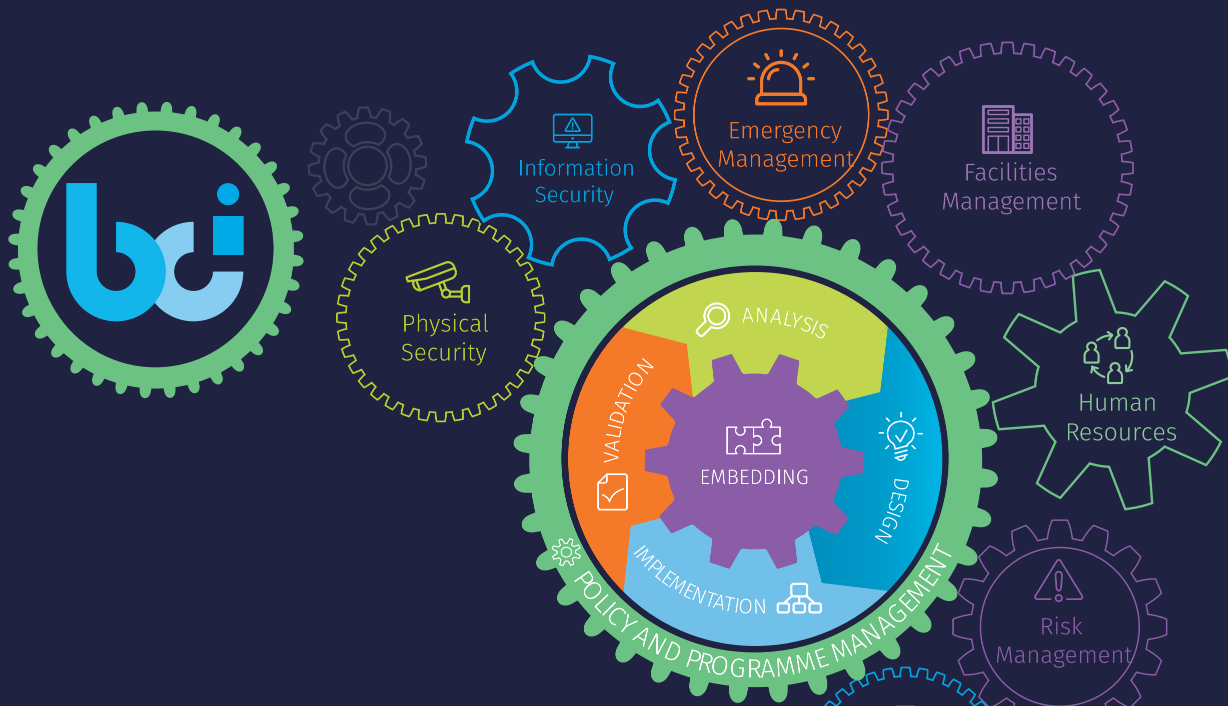
Cheques must be made payable to Perspective Publishing Limited and addressed to the Circulation Dept.

CIR Magazine is published by:

Perspective Publishing
6th Floor
3 London Wall Buildings
London Wall
London, EC2M 5PD
UK

Tel: +44 (0)20 7562 2400

ISSN 1479-862X
cirmagazine.com



New BCI CBCI Certification Course

2018 Edition

The BCI Good Practice Guidelines 2018 Edition is here, and we've got a brand new course to go along with it. The BCI CBCI Certification Course and Exam is designed specifically to prepare you for the CBCI examination, one of the main gateways to BCI Membership, and it's fully aligned with GPG 2018.

Visit www.continuityshop.com/certification for details

And introducing our new range of BCI Courses

- BCI Policy and Programme Management
- BCI Designing Business Continuity Solutions
- BCI Supply Chain Resilience
- BCI Validating your BCM Programme

Discount for readers of CIR Magazine

Quote the code CIR001 when booking to receive 10% off the course fee. More information on all our courses can be found at our website at www.continuityshop.com, or call us on (+44) 0161 743 3555.

CONTINUITY SHOP

Innovation Forum, Salford, UK M6 6FP T: +44 (0) 161 743 3555
E: info@continuityshop.com www.continuityshop.com

bci AWARDS Hall of Fame

Business Continuity Institute
Licensed Training Partner

Government launches new product safety office

The government has opened a new office for Product Safety and Standards, aimed at enhancing the UK's product safety system and providing higher levels of protection for consumers. Deborah Ritchie reports

The government has announced the creation of a new national oversight body tasked with identifying consumer risks and managing responses to large-scale product recalls and repairs. The new office is also tasked with ensuring the UK carries out appropriate border checks on imported products once it leaves the European Union.

The announcement comes as part of the government's response to the Working Group on Product Recalls and Safety. Established in October 2016 by former consumer minister Margot James, the group of product and fire safety experts was brought together to build on the recommendations made by Lynn Faulds Wood in her independent review into consumer product recalls.

According to Business Minister Andrew Griffiths, the new Office for Product Safety and Standards will "strengthen the UK's already tough product safety regime and will allow consumers to continue to buy secure in the knowledge there is an effective system in place if products need to be repaired or replaced". It is hoped that the new office will help enable the UK to meet the evolving challenges of product safety by responding to expanding international trade, the growth in online shopping and the increasing rate of product innovation.

Based in the Department for Business, Energy and Industrial Strategy (BEIS) and expected to have a budget of around £12m a year, the Office for Product Safety and Standards will cover general (non-food) consumer product safety. It will not cover vehicles, medicines and medical devices, or workplace equipment, which are already covered by other agencies. Nor does the remit of the body cover construction products, which are currently subject to a separate review being led by Dame Judith Hackitt.

Other activities forming part of the government's response to the Working Group include collaboration with the British Standards Institute to provide guidance on product recalls and corrective action; conducting research to help manufacturers and retailers develop technological solutions to product marking and identification; and researching consumer behaviour to identify the best way to drive up the number of consumers registering appliances with manufacturers.

The new body is also expected to represent an expert panel to bring together trade associations, consumer and enforcement representatives to advise on product safety issues as they arise; advice which may include conducting risk assessments and analysing what risks are present for businesses.

Written by Deborah Ritchie

Essential reading for resilience professionals

ISO 37001: An Introduction to Anti-Bribery Management Systems

Alan Field, IT Governance Publishing, 2017. Reviewed by Deborah Ritchie, Editor, CIR

itgovernance.co.uk

Under the Bribery Act 2010, a maximum of ten years' imprisonment and an unlimited fine may be imposed for offering, promising, giving, requesting, agreeing, receiving or accepting bribes. The Ministry of Justice's quick start guide to the Bribery Act makes it clear that there is a full defence "if you can show you had adequate procedures in place to prevent bribery". Legal obligations aside, an ethical approach to business is a contributory factor in effective reputation management.

ISO 37001:2016 is the international standard for anti-bribery management systems. Some readers will be familiar with its predecessor, BS 10500:2011, the British Standard, with which the former has many similarities, albeit with some important nuances. The new ISO specifies a number of anti-bribery policies and procedures that organisations can put in place to prevent bribery from occurring and to help effectively identify and deal with any instances where it does occur.

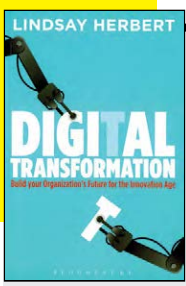
Published as part of a series on governance, risk and compliance (in which readers may also find the GDPR pocket guide of interest), these books are keenly priced at £9.95 and aim to be an introduction to what might be a new topic for some or a quick reference guide for others.

Author Alan Field has many years' experience with

"Some readers will be familiar with the ISO's predecessor, the British Standard BS 10500:2011, with which the former has many similarities, albeit with some important nuances"

quality and integrated management systems in the legal, financial, property services and project management sectors, and in auditing, assessment and gap analysis roles. He also has experience in third-party assessment of anti-bribery management systems to BS 10500 and ISO 37001 requirements, and counter-fraud systems in the public sector.

This little pocket guide may provide useful guidance on the importance of clearly defining policies; logging gifts and hospitality in auditable records; ensuring a consistent approach across the organisation; controls for contractors; facilitation payments; and charitable and political donations.



Digital Transformation: Build your Organisation's Future for the Innovation Age

Lindsay Herbert, Bloombsury Business, 2017. Reviewed by Deborah Ritchie, Editor, CIR

bloomsbury.com

Digital transformation is a term increasingly heard in the business environment yet often misunderstood. And confusion surrounding what it is, how it works and what it means for processes and jobs has, in a lot of cases, led to many companies failing to embrace it. From the get-go, this book sets about dispelling some of the misconceptions about digital transformation – to lift the veil and help pave the way for organisations that are serious about getting to grips with it.

Among these misunderstandings, according to author Lindsay Herbert, is the widely held assumption that everyone is on the same page when it comes to digital transformation. In reality, the term means very different things to different stakeholders. As Herbert outlines, the CEO considers its impact on revenue and investors; the CMO looks at it in terms of spending more on digital marketing; the CFO meanwhile may see an opportunity to shift low-skilled work offshore.

With this book, Herbert demystifies the 'black art' of digital transformation, offering a model for business leaders and consultants alike, and recognising that the challenge of successful digital transformation is not the tools but the culture of a business.

Herself a digital transformation leader with IBM, the author has been overseeing digitally transformative programmes of work for large scale international businesses and charities for over a decade.

"This book sets about dispelling some of the misconceptions about digital transformation and to help pave the way for organisations that are serious about getting to grips with it"

"The truth about digital transformation is actually not about adapting to new technology at all – it's about directing an organisation to be more adaptive to change itself," she writes, and goes on to explain through countless examples that the companies that succeed in this area are the ones that adopt a new mindset and new ways of working, not just to meet the changed needs of their customers – but instead to become future-proof.

News in brief

The latest news for business resilience and insurance professionals

A collision involving an unmanned ship as a result of a cyber attack would trigger difficult questions about liability, according to global marine industry executives. Confusion surrounding the regulation of unmanned vessels and available insurance cover are together confounding concerns in this arena, according to a report published by global law firm Clyde & Co and the Institute of Marine Engineering, Science & Technology (IMarEST).

Half of UK consumers don't believe commercial organisations care about their privacy, and many are prepared to take legal action against businesses that don't comply with GDPR, according to a study. Businesses, meanwhile, are concerned the new data privacy regulations will have a negative impact on operations and international relations.

Law firm Clyde & Co has completed a study into the legal and regulatory considerations that arise as they are increasingly used in insurance. The report draws on insights from Clyde & Co's global network of insurance lawyers, explores the growth of parametric insurance and considers the important role it has to play in building resilience to natural catastrophes.

Security flaws in the vast majority of devices were exposed in January. Researchers discovered gaps in security in the CPUs from most of the major manufacturers: Intel, ARM and AMD. The vulnerability leaves devices using these chips – including PCs, mobiles and servers open to attack.

The role of today's chief risk officer has shifted from technical expert to business advisor, and has propelled CROs into a world of complex stakeholder relationships, business navigation and regulatory expectations. According to a new study, this poses significant challenges for aspiring CROs in maximising the effectiveness of businesses risk functions.

Careless disposal of antibiotics could lead to 'ferocious superbugs', according to United Nations experts. Growing antimicrobial resistance linked to the discharge of drugs and some chemicals into the environment is one of the most worrying health threats today, according to new research from the UN which highlights emerging challenges and solutions in the environment.

Arc Legal Assistance has launched a dedicated Personal Cyber Support policy providing household insurance customers with access to support, restoration services and cover for cyber attacks. Designed to provide immediate assistance for individuals and families in the event of a cyber attack on personal electronic devices, cover can be either embedded in an underlying home insurance policy or provided as part of a legal expenses insurance (LEI) policy. Cover is underwritten by AmTrust Europe.

A growing number of small businesses say they are looking to interact with their insurers online according to a survey of small firms around the world, with UK companies among the most 'digitally savvy'. The PwC survey of 2,100 small businesses suggests that the insurance market for SMEs is likely to completely transform to match the digital transformation seen personal insurance over the past decade.

Around 200,000 residents have now been evacuated amid the latest California wildfires as crews battle to fight the latest blaze. More than 5,000 firefighters have been battling four brushfires that have damaged 150 buildings in the south of the state. The development is a major blow to a region that was still counting the cost of October's wildfires, which are believed to have been the costliest in the US state's history.

For more information on these stories and other industry news and views, visit **cirmagazine.com**

photo by: Casimiro PT / Shutterstock.com

A partnership between Pool Re and Cranfield University has seen the appointment of Professor Andrew Silke as the professor of terrorism risk management and resilience at the university. The role– a new position which will be co-funded by Pool Re and Cranfield University – is for an initial five-year period, starting on 31 January 2018.

Analysis by the Confederation of British Industry suggests a rise in the number of people who believe businesses in the UK have a good reputation. The research, comparing perceptions of businesses between May and November 2017, reveals 2 in 3 people think UK businesses have a good reputation, up 7% in 6 months.

Pool Re has announced plans to extend its cover to include material damage and direct business interruption caused by acts of terrorism using a cyber trigger. The cover, effective from April 2018, which will exclude intangible assets, will be offered as standard to all policyholders purchasing terrorism insurance from Pool Re members.

Product-related risk is one of the biggest perils facing businesses today, with recall exposures having increased significantly over the past decade, bringing the potential for larger and more complex losses than ever before, according to Allianz.

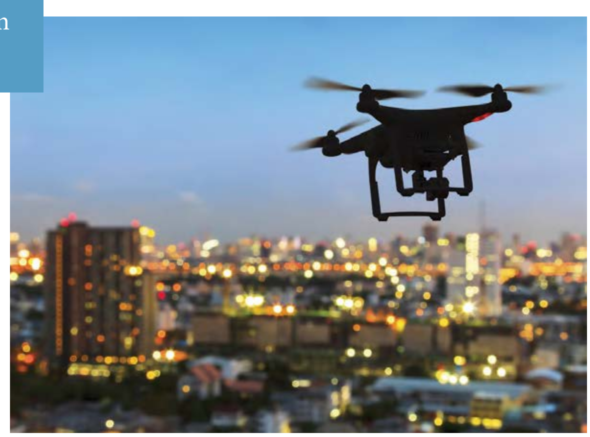
More than a third of IT professionals (35%) see themselves as the biggest internal security risk to networks within their organisation, according to research from IT security firm Balabit.

Sungard Availability Services has launched a fully-managed cloud recovery solution on Amazon Web Services, through which they can now offer SLA-backed recovery for users on AWS or on premises, delivering the level of resiliency required for business-critical applications. Users can expect to achieve sub one-hour RTOs and RPOs for their x86 workloads.

Supermarket chain Morrisons has been found liable for a data leak involving financial and personal data of almost 100,000 members of staff following a trial in the High Court. Information including salaries, national insurance numbers, dates of birth and bank account numbers were among the details leaked by a former disgruntled employee – Andrew Skelton – in 2014. Skelton was jailed in 2015 for his crime.

Research suggests only five per cent of IT decision makers have all the necessary data governance strategies in place to be compliant ahead of the introduction of the European Union General Data Protection Regulation (GDPR) deadline on 25 May 2018.

Legislative proposals, due to be finalised in spring 2018, look set to place new responsibilities on owners of drones weighing 250g or more. These rules include mandatory registration of the individual and the requirement to take a safety awareness test. The proposed legislation could also see drones banned from flight near airports, or above 400ft, in an effort to reduce unsafe flying. Police may also be given authority to seize and ground drones which may have been used in criminal activity.



Digital enabler

Deborah Ritchie speaks to availability services director at Daisy Corporate Services, Andy Dunn about developments at the company and in the business continuity market

Andy Dunn is availability services director at Daisy Corporate Services, the Lancashire-based end-to-end communications and IT services provider. Prior to holding this position, Dunn was regional head of sales, having worked for what was Phoenix since 2015. Since taking the helm in April, Dunn has been tasked with repositioning business continuity and recovery services in the cloud focused IT arena.

You've been at the helm at Daisy for several months now. How are plans coming along?

We're executing really quite well against a backdrop of quite a lot of change both within business continuity and the business as a whole! Since I took on the role in April, my remit extended in October to include not just the business continuity business, but also public sector within Daisy Corporate Services (DCS). Along with James Pickering, and Louise Newbury Smith, we look after the entire go to market strategy. This involves rolling out what's worked in business continuity across the public sector team, but the primary focus is to bring Daisy Availability Services (DAS) into the heart of everything we deliver within DCS.

I understand Daisy is planning a new launch for April. Can you reveal anything about what the market might be able to expect?

I can't say too much about this! But I can tell you that cloud will feature heavily in our new DAS offerings. The bridge for that is the new backup solutions we have developed.

There are two ways of looking at the impact of cloud on business continuity. On the one hand, the move to the cloud has been eroding our revenue for years... the outsourcing of cloud IaaS has hit our traditional ITDR services quite hard. Reactively, we pushed against it instead of trying to understand the drivers behind it; but since then we have begun to consider where the dials might be tuned – to work with the tide instead of against it – and from this perspective you can start to see the upsides.

As part of this, we've been doing a lot of work looking at cloud to cloud recovery – examining ways we can cross-provide in our own cloud or public to public. There is still a lot of work to do on that, as some of the complexities are huge when you consider what infrastructure customers have in place – particularly when it comes to any legacy systems they may have.

We've also been looking at the risk of a customer losing access to public cloud services. We've had hard invocations where customers have invoked into work area for cyber events, so that's another important focus for us at.

So are customers coming back full circle to work area recovery when cloud access fails?

Yes, in a sense I guess they are. Our Safe Haven, while there is no mention of work area recovery under this offering, it is part of the cyber resilience solution. What we call Flexplace basically means customers can use the area for anything they need to – be it systems testing or staff training. This really means work area recovery becomes a more holistic business enabler.

So that area of the business is returning to growth, as we are seeing a very clear upturn in the interest around newly defined services. And you can see why – it's the ultimate backstop. Even the more nimble starts-ups appreciate the need for a clean environment when it all goes pear-shaped.

The global shift to cloud recovery has been unnerving the business continuity providers in the UK. But despite this we've renewed all our major customers this year. Notably, a number of major financial institutions have been really proactive in that resign process.

How are you as a service provider affected by and prepared for GDPR?

The biggest manifestation of the GDPR problem is currently nervousness around how the new rules will be applied.

We have examples of contracts where we have been happily coexisting on the contract for ten years with a clear risk on DPA. But the question raised by the new rules is around whether you are a processor or a controller when a customer invokes with you.

It's a difficult conversation to have for obvious reasons. Customers want to pass it to service providers, and service providers want to limit their liability.

However, all the Daisy services

Andy Dunn, Availability Services Director, Daisy Corporate Services

that support or enable GDPR for businesses have a clear alignment so customers understand which elements of GDPR can be covered with a particular service. So as a provider we are clear on our service value under GDPR.

What has been the impact of Brexit thus far on the way Daisy does business?
We have seen some customers look for a Brexit clause in their agreement, just in case their UK entity may later no longer be viable. This is mostly among the smaller, European-owned financial institutions.

But that aside, there have been a number of cases where we have used it to our advantage. All of us were chasing long-term contracts – mainly consisting of work area recovery, a significant amount of seats and in the region of £1m a year – which is a big commitment. But instead we are offering alternative terms and complimentary Daisy services on contracts, whereby we will take the risk if Brexit is a problem. You pay a premium for that level of agility, but the model works and can be applied to other risks on the register.

What other issues are your customers dealing with, and how are you helping them to address those issues?
Brexit and GDPR are keeping all our customers busy – across all the verticals we serve – though we are probably seeing the most demand for contract flex in financial services and retail. The retailers are uncertain. The traditional undercurrent of driving value in that sector, is more prevalent than ever.

What's your view on the competitive landscape in the business continuity space given how much it's changed over the last 5 to 10 years, and how is the market collaborating to ensure its future ahead?
There are some obvious shifts – mostly that there are fewer providers investing in property to deliver the heritage business continuity services. We are in conversation with some of the major providers about what the next five years look like for our sector and are making progress with a number of exciting plans in that regard. We think it's important to collaborate with our competitors to maintain excellence in service delivery for all customers.

What's next for Daisy?
As the fourth largest UK telco in the business to business arena and the UK's third largest VAR, we are ideally placed to ensure our customers can link converged IT and communications solutions and still benefit from our 30-year heritage of business resilience and recovery.

Interview by Deborah Ritchie

- Uncertainty surrounding global trade and political risk correctly forecast in early 2017 is ongoing, with some sectors harder hit than others
- At the same time, a growing economic recovery presents business and political leaders with an opportunity to grapple with the important issues
- By far the greatest concern raised by experts this year was the environment, with a focus on extreme weather events in particular

Tomorrow's world

The last 12 months have provided resilience professionals with a wide ranging array of risks , and as the new year risk forecasts flood in, Deborah Ritchie suggests that this year will be no less challenging

Twelve months ago, analysts at Control Risks forecast a difficult year ahead for business risk professionals. CEO Richard Fenning said the unexpected results of the US election and EU referendum would make "one of the most difficult years for business' strategic decision-making since the end of the Cold War". The challenges to globalisation and trade highlighted by these two major events on both sides of the Pond did indeed make for a year of heightened strategic uncertainty in 2017; and that uncertainty prevailed as we rung in a new year.

The very catalysts to international business – geopolitical stability, trade and investment liberalisation and democratisation, have undergone varying degrees of erosion over the past year, making the commercial landscape among government, private sector and non-state actors ever more complex. Such instability is a mixed blessing for risk professionals: high levels of complexity and uncertainty have forced boards to undertake comprehensive reviews of their approaches to risk management. Demand for risk expertise – practitioners and consultants alike understandably increases at times like this.

But, despite the national headlines, it has not all been doom and gloom. Fears that Britain would slide into a post-referendum recession did not transpire, with economic data confounding the apocalyptic forecasts, and with the year ending with low unemployment, strong consumer spending, a steady housing market and a buoyant stock market.

The further prospect of strong economic growth globally in 2018 presents leaders with an opportunity to address signs of severe weakness across societies, economies, international relations and the environment.

This was indeed among the headline messages of the World Economic Forum's (WEF) annual report on the global risk landscape, published earlier this month, and the culmination of the WEF's deep-dive into the most pressing risks we face.

"A widening economic recovery presents us with an opportunity that we cannot afford to squander, to tackle the fractures that we have allowed to weaken the world's institutions, societies and environment," says Professor Klaus Schwab, founder and executive chairman of the WEF. "We must take seriously the risk of a global systems breakdown. Together we have the resources and the new scientific and technological knowledge to prevent this. Above all, the challenge is to find the will and momentum to work together for a shared future."

But while this key statement from the WEF's anticipated study had positive overtones, its authors also issued a number of warnings for business leaders this year.

A generally deteriorating geopolitical landscape is a cause for great concern across the coming year, with a staggering 93 per cent of respondents to its annual risk report said to be expecting political or economic confrontations between major powers to worsen and nearly 80 per cent expecting an increase in risks associated with war involving major powers.

This sentiment was echoed by the Control Risks analysts, which points more specifically to the increasingly personalised and assertive style of national leadership that it believes will contribute to a profoundly uncertain business environment across the coming year. Company CEO Fenning says that despite the most positive global economic outlook since the end of the financial crisis, we are entering a year of geopolitical fragility that has the potential to trigger shockwaves to global stability and business confidence.

"The biggest risk is that the next world order will be imposed, not agreed, set off by further nuclear brinksmanship between the US and North Korea, or wide scale destabilisation in the Middle East because of escalating Iran-Saudi Arabia rivalry," he warns. "While these events are unlikely, what is certain is that global dynamics and perceptions of risk are being shaped by a more robust, personalised and unpredictable style of political leadership in many parts of the world, making business planning very difficult."

He says that despite all this political turbulence, global businesses must go into the year with a cool head. "Trying to understand the motivations of global leaders and the potential impact of their actions will be critical to making the right strategic business decisions," he advises.

Key risks facing businesses in 2018

North Korea escalation - War on the Korean peninsula is unlikely, but while the paths of escalation are clear, de-escalation is harder to plot. The search is on for the least bad option. The risks of miscalculation and accidental escalation are the highest they've been since North Korean leader Kim Jong-un assumed power.

Large-scale cyber attacks against infrastructure - 2017 was the year of major but random disruptive attacks. 2018 could see the likes of WannaCry, NotPetya and BadRabbit recur, but in a more powerful, targeted and disruptive manner. National infrastructure systems are particularly at risk. Such attacks will target primarily countries in regions of heightened security and military tension. Attacks on the UK will be unlikely due to factors including a lack of significant international conflict involving the UK and a strong cyber defence posture from UK agencies.

US gets protectionist - Low likelihood, high impact, but the threat is there: in a year of mid-term elections, NAFTA negotiations fail to make enough headway, Donald Trump pulls the US out of NAFTA and the WTO, and goes after China on trade, causing profound disruption to international commerce.

Regional rivalries in the Middle East – Ambitious Saudi Arabia and assertive Iran will not go to war, but across the region their rivalry will inform and inflame conflicts and enmities in Syria, Lebanon, Iraq and Yemen and between Israel and the Palestinian Territories.

Personalised leadership – Astride the business risk landscape is a collection of assertive world leaders who rely heavily on nationalism and, to varying degrees, populism. Prone to capricious decision-making, they find foreign companies convenient targets. More than ever, knowing the mind of the person at the top is essential.

Source: Control Risks

A transformational time

Strategic decision-making is top of the agenda at this month's World Economic Forum meetings in Davos, ahead of which the aforementioned Global Risks Report serves to allow

participants to grapple with some of the most pressing challenges. In a new addition to the report this year, the organisation urges business leaders to prepare for "sudden and dramatic disruptions". It makes clear that these are not predictions, but rather potential stories that underline the value of running through a variety of scenarios that might fundamentally upend operations.

These include global food supply failures, democratic collapse, artificial intelligence "weeds", ongoing bilateral trade disputes and insufficient response, advanced protectionism, advanced civil conflict and state-on-state cyber attacks. Depending on your imagination, some of these scenarios might seem far-fetched, but, as the report states, while some are more speculative; others extrapolate from risks that have already begun to crystallise.

Among them, technological risks, and our struggle to keep up with an accelerating pace of change in this arena. And, as concern surrounding cyber risks intensified in 2017, worry overtook optimism for respondents to this year's report, as cyber attacks and massive data fraud both appear in the list of the top five global risks by perceived likelihood. Large-scale attacks now rank third in terms of likelihood, while rising cyber dependency is considered the second most significant driver shaping the global risks landscape over the next 10 years.

By far the greatest concern raised by experts this year, however (and for the second year running) was the environment, with extreme weather events seen as the single most prominent risk. All five risks in the environmental category were ranked higher than average for both likelihood and impact over a 10-year horizon. This follows a year characterised by high-impact hurricanes, extreme temperatures and the first rise in CO_2 emissions for four years.

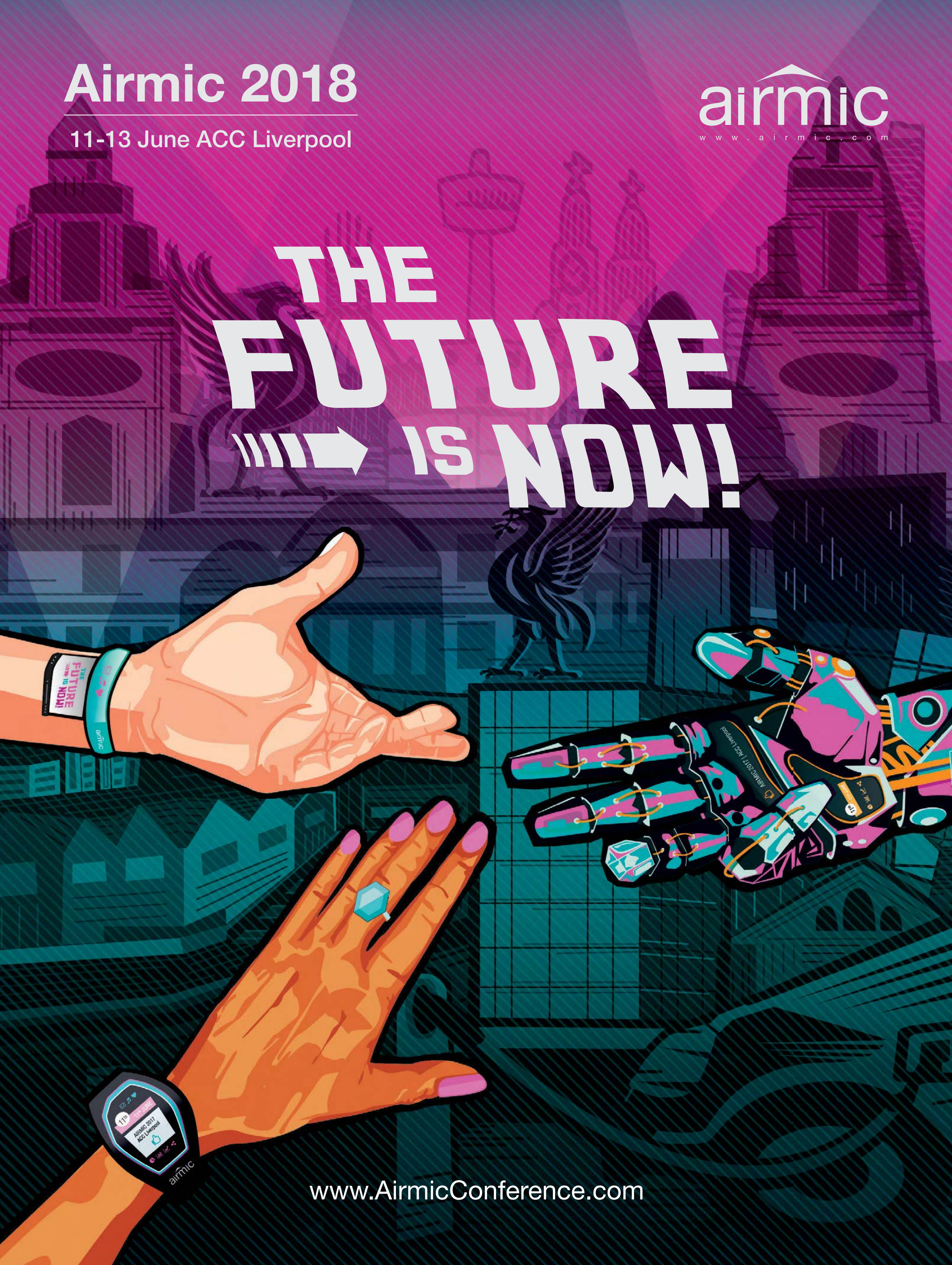
"We have been pushing our planet to the brink and the damage is becoming increasingly clear," the report's authors write. "Biodiversity is being lost at mass-extinction rates, agricultural systems are under strain and pollution of the air and sea has become an increasingly pressing threat to human health." They add that a trend towards nation-state unilateralism may make it more difficult to sustain the long-term, and that multilateral responses are required to counter global warming and the degradation of the global environment.

There is something somewhat paradoxical about the risk and opportunity horizon as we begin this new year. As the authors of this report point out, our generation enjoys unprecedented technological, scientific and financial resources, and yet, ours is perhaps the first generation to take the world to the brink of a systems breakdown.

The need to for nations and leaders to shift up and gear and collaborate to tackle these systemic risks is clearly apparent.

Let's hope that in January 2019, we are looking back on a year when the opportunity was seized to allow this to happen.

Deborah Ritchie is editor of CIR


Airmic 2018
11-13 June ACC Liverpool
airmic
www.airmic.com
THE FUTURE IS NOW!
www.AirmicConference.com

Risk views

As a new year begins, CIR speaks to an array of industry experts to find out what's in store for resilience professionals over the coming 12 months and beyond – from D&O and demographic shifts to political risk and wargaming

Shifting risk landscape spells change in D&O

Criminal investigations and prosecutions of both entities and their directors are likely to increase in the UK and across Europe in 2018. Strict liability offences under the UK Criminal Finances Act 2017, which came into force at the end of September, now make companies and partnerships criminally liable if they fail to prevent tax evasion by an employee or associated person, and could herald a raft of new prosecutions next year.

The penalties for these new offences are tough. They include an unlimited financial penalty and possibly ancillary orders, including confiscation or serious crime prevention orders. In addition, the conviction will be on public record. If the furore surrounding the Paradise Papers is any indication of the national mood – where the important distinction between (legal) avoidance and evasion is often blurred – any company in the spotlight is likely to suffer considerable reputational damage whether involved in or associated with legitimate tax avoidance or illegal evasion.

The UK government also looks set to further tighten corporate governance regulations, with the proposed extension of the Senior Managers and Certification Regime to all authorised firms, due this year

It has also been suggested that further "failure to prevent" and other forms of economic criminal offences, may also be introduced, as the government seeks to make it easier to hold corporate bodies, and their directors and officers, accountable.

The broadening of corporate criminal offences inevitably has an impact on directors and officers, who may increasingly find themselves at odds with the company when wrongdoing is alleged. Deferred prosecution agreements (DPAs), with their strong emphasis on cooperation, may provide regulators with much-needed information to pursue individuals as a price of potentially allowing the corporate to defer, or escape prosecution itself, leading to a heightened risk of individual prosecutions.

With businesses becoming more and more global, the chance increases that an organisation may find itself subject to multiple prosecutions for any wrongdoing. The importance of strong global processes cannot be underestimated, nor can the need for adequate insurance to meet the costs of defending criminal investigations and prosecutions, which otherwise can be on the business-critical scale.

Will increased corporate scrutiny and regulation, changing public attitudes to corporate governance and the risk of reputational damage linked to leaked documents be the perfect storm that turns the D&O market? We will find out this year...

Mark Sutton, Partner, Clyde & Co

Perilous security landscape prevails

Security and recovery will rise further up the agenda in 2018. Malware and ransomware attacks will continue to dominate, with devastating consequences for affected businesses. With the widespread adoption of the Internet of Things (IoT), we will also see an increase in the number and complexity of endpoints, which could in turn lead to an increase in zero attacks.
Chris Ducker, Senior Director, Sungard Availability Services

Digital transformation gets serious

Digital has so far been about pace and urgency. The race to embrace the fourth industrial revolution is still being run – but this year expect the early front-runners to ease up a little. Digital transformation is a marathon, not a sprint. And that's good because it gives business continuity professionals the time to identify and mitigate the new risks that the digital revolution presents.
Andy Dunn, Availability Services Director, Daisy Group

GDPR will help crystallise the importance of securing visual data

As the May 2018 deadline for GDPR approaches, some organisations are working hard to ensure compliance. One element of these preparations that cannot be overlooked is that of visual data collected by surveillance cameras. There are millions of cameras in the UK, across all kinds of organisations – from hospitals and GP surgeries to schools and colleges, from shops and offices to transport hubs and open spaces. Wherever they are, those responsible for the visual data that cameras generate will be subject to the provisions of GDPR.
James Wickes, CEO, Cloudview

The role of wargaming in combatting inevitable global cyber attacks

While recent commentary has focused on issues such as the recent increase in DDoS attacks due to IoT devices and the rampant and pernicious ubiquity of ransomware, a bigger potential storm has been brewing throughout 2017, of which the clearest warning sign has already been seen in WannaCry.
Dr Danny Steed, Head of Strategy, ReSolve Cyber

Adaptability is the key to sustainable business

The regulator seems set to maintain the pace of consultations, with a key focus on ensuring great customer outcomes and ensuring personal accountability of leaders. We'll need to filter through these voluminous documents and work through the details to identify the critical issues and provide compelling arguments and evidence to shape any future rule changes. Throughout 2017, we've read lots about InsurTech, with new entrants threatening to be disruptors. But given agile development and flexibility of digital platforms – enabling integration with legacy platforms, 2018 could be the year that traditional players bring technological change to their core business.

Tom Woolgrove, CEO, Premium Credit

The innovative insurer becomes the norm, not the exception

Digital technologies will continue to transform the insurance industry and will do so at an increased pace this year. While insurers compete to leverage digital technologies to improve the customer experience, a wave of technological innovation will continue to disrupt the entire value chain. Drones, IoT devices and sensors are forging new and powerful connections between insurers and the risks they cover – changing underwriting, claims, risk selection and pricing and even insurance products themselves.

Seth Rachlin, executive vice-president, P&C Insurance Leader, Capgemini

Oil and gas predictions

Major Accident Risks

As ever, catastrophic major accident potential and physical asset integrity will, and needs to, remain a major focus in the industry. Such events must always be front of mind given their impact on people, the environment and the business of the industry. With the lower oil price era continuing, producers have needed to look at ways of limiting their costs. While they have done this with the aim of not impacting on major accident risk, the impacts of the changed ways of working on the integrity of assets and hence on major accident events are likely take time to materialise. Some aspects that illustrate this are:

- With an increased use of floating production systems, there has been a drive to accept marine standards for hydrocarbon systems with a potential de-specification in safety factors. Marine and oil and gas are very different risks types and need to be managed using their own standards.
- Ownership changes within mature oil and gas fields is resulting in some transferred assets being managed by new operators/licensees who have lower engineering capacity; and having lack of clarity between licensee and operator (dutyholder) over responsibility for risk management. (Company X as the licensee asks Company Y to operate the asset under the management system of Company Y)
- Onshore assets (refineries and petrochemical) being run harder and for longer between shutdowns, to take advantage of cheap feedstock prices.

It is therefore important to continually manage and monitor these risks in case there is an unintended upturn.

Rising risk of decommissioning

There has been a trend of postponing decommissioning over the last few years to avoid the costs in the immediate term, however decommissioning will occur more frequently in the coming years. With decommissioning of oil and gas facilities there is the challenge of plugging and abandoning wells with the challenge of the ongoing assurance of their status in perpetuity. This is a possible emerging risk where there is a concern that the integrity of older wells is not achieved, with the occurrence of adverse events in the future. Postponing decommissioning has also had the impact of further extending the life of several assets that were already beyond their design life.

Other emerging risks

Based on current forecasts, oil and gas will continue to be a key source of energy for some time to come. There is, however, drive for increased use of low carbon energy sources. The safe operation of older assets during the energy transition needs to be maintained and the change could take focus off older oil and gas assets. As we move to a lower carbon / new energy sources future, new risks will emerge. For example, risks associated with:

- Hydrogen
- Biogas/Syngas
- Biomass
- Batteries / transformers

For instance, the potential of hydrogen being used for heating homes raises a number of issues: it burns with a colourless flame, requires changes to heaters/boilers, and must be able to pass through a grid developed for natural gas. The generation of hydrogen needs to be cost-effective and if generated from natural gas would require carbon capture and storage – a technology yet to be commercially proven on a large scale.

The transition also raises supply security and continuity risks. The change needs to bring in the new energy sources at a rate to replace the old sources and in a form that can be taken up by the end users, at an acceptable cost.

Finally – as for many sectors – the greater application of IT technology for oil and gas operations is raising the issue of cyber risk. This is a growing concern for the industry with greater use of such technology to; for example, allow remote operations and monitoring of platforms, subsea and remote facilities. Recent claims in related industries have also illustrated the potential magnitude of impact were a major event to hit an oil and gas organisation.

Mark Boult, CFIRM, Director, DNV GL Ltd

Political risk hotspots continue to change extraordinarily quickly

Political risk has long been a concern for companies operating and trading in or with jurisdictions described as developing countries, including South America, Africa, Eastern Europe and some countries in Asia. The richness of these countries in terms of natural resources and other commercial interests continues to make them attractive investment options, however.
Graham Denny, Partner, EC3 Legal

Demographic shift will be a precursor for change in the insurance industry

By December 2018, 25 per cent of the people employed in the insurance industry in 2015 will have retired, a trend which is set to accelerate over the coming decade. It should be no surprise therefore, that there has been an influx of investment into risk management innovation as the industry seeks creative solutions to fill this gap.

To date, the main focus of InsurTech has been on product distribution but there is increasing attention on the breadth of the value chain. Demographic shifts are likely to enhance focus on those elements of the supply chain which, because of procedural intensity or data complexity, will suffer most from a scarcity of human resource

The current 'first wave' of InsurTech businesses have for the most part been supporting incumbents and not disrupting them. These first movers have faced a kind of industry that their successors will not, and cultural changes will provide fertile ground for the disruption of legacy systems throughout this year and beyond.

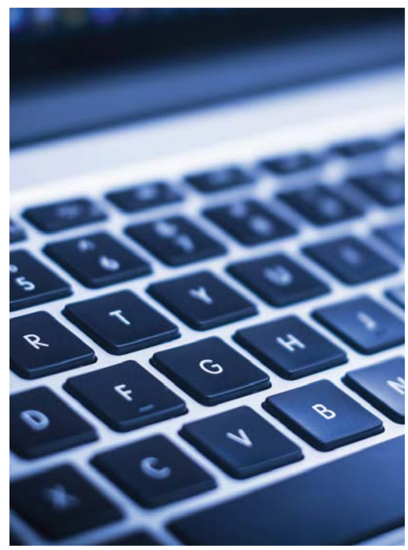
The market will see increasing innovation in claims and underwriting, with analytics and artificial intelligence (AI) playing an enhanced role, as the significance of personal relationships wanes. Here, the impact of technology driven risk assessment on underwriting is worth mention, particularly in human vehicular piloting.

By way of illustration, motor insurance faces disruption on two major fronts. Firstly, autonomous vehicles and the resultant reduction in the risk of accident caused by human error. Secondly, the ability to adjust premiums on a real-time basis by using feedback from the vehicle about the condition of its driver. Considered with AI's capacity to manipulate and provide insights from data, these advances highlight the ever-decreasing need for human involvement in the profiling of risk.

With the implementation of GDPR this year, the legislative underpinnings of a framework for advanced data process management will be in place. Data is already the most valuable asset available to a business, easily outstripping other commodities and GDPR will provide an obvious point of coalescence for so called RegTech advances with general relevance to the management of risk.

What does all this mean? In the medium to long term, lower premiums, a more streamlined customer journey and reductions in the complexity of risk management. In 2018, it will call for continued refinement by incumbents as they face challenges to their operating models and their bottom lines and they seek to integrate InsurTech while staving off its competitive challenge.

John Small, Solicitor, EC3 Legal



Social engineering attacks set to soar

The conditions are in place for a further rapid rise in social engineering attacks in 2018, with more and more organisations falling victim to these scams. During the first nine months of 2017, Beazley saw a nine-fold increase in the number of social engineering incidents reported by clients compared to the same period in 2016. Most affected were professional service firms, financial institutions and higher education establishments.
Raf Sanchez, International Breach Response Service Manager, Beazley

Reputation matters

While reputational risk covers an increasingly wide range, damage to corporate reputation from cyber liability has moved top of the agenda, reports Graham Buck

- There was no shortage of high-profile reputational casualties in 2017: Pepsi's Kendall Jenner advert, United Airlines and Bell Pottinger among them
- Underlying issues driving reputational risk are steadily becoming less about money and capital, and more about relationships and trust
- Risk management requires asking how stakeholders feel about an issue so they have a chance to identify the threats and vulnerabilities that matter most

"Reputation is an idle and most false imposition; oft got without merit, and lost without deserving." Shakespeare gave this line to Iago 400 years ago and today's corporates are still grappling with the capricious nature of reputational risk.

There was no shortage of high-profile casualties in 2017, such as Pepsi's misjudged Kendall Jenner advert, United Airlines forcibly removing a passenger from an overbooked flight, McDonald's first UK strike and revelations about Bell Pottinger's activities in South Africa that triggered the PR firm's demise.

"Each of these crises relates to poor corporate governance, whether it was in the way businesses viewed and treated customers, workers or the wider society," says James Bickford, managing director of research and advisory specialist the Reputation Institute. "All had a profound financial impact."

What's more, episodes from previous years continue to reverberate, such as Tesco's £250m accounting 'black hole' from misreporting and tax avoidance strategies employed by US giants including Amazon and Starbucks.

However, while such episodes might have impacted on the stakeholders of these corporates, their clientele wasn't directly affected. Companies mishandling risks involving their customers or workforce can suffer both financial and reputational damage; no more so than when hackers are able to infiltrate personal data.

US retailer Target became the "poster child for major data breaches" in 2013, reports James Burns, cyber product leader at CFC Underwriting. As Christmas approached, the company reported that 70m credit/debit card numbers and records of customers' personal information had been stolen.

"Target suffered a 20 to 30 per cent drop in profit in the quarter following the breach; its perceived lack of customer involvement impacting very negatively," says Burns. "While sales eventually recovered, it wasn't enough to recoup losses suffered in the aftermath."

Subsequent resulting pay-outs included US$10m to settle consumer lawsuits, nearly US$40m to US banks and credit unions for resulting losses and a further US$18.5m to state enforcement agencies last May. Added to this was a US$200m plus bill for credit card unions that reissued affected cards.

UK supermarket chain William Morrison was recently found liable for the actions of disgruntled employee Andrew Skelton, who in 2014 posted the payroll data – including names, addresses, bank account details and salaries – of nearly 100,000 employees.

The court's decision to hold Morrison's liable for the breach, despite it being the victim of criminal activity by a trusted employee, promises to have implications for other businesses. They include ride-sharing pioneer Uber, which concealed a hack affecting 57 million customers and drivers.

Diverse responses

Burns says companies learned much from high-profile data breach cases in 2015, involving telecoms group TalkTalk and retailer Carphone Warehouse.

"Although both incidents were similar in nature, the companies' respective responses were very different."

Dido Harding, then TalkTalk's CEO, promptly set out on what aimed to be a damage limitation exercise. Unfortunately this was done without the company "first getting its ducks in a row" as it emerged that around 157,000 customers had been affected by the breach rather than TalkTalk's entire customer base of around four million.

"Carphone Warehouse actually suffered a bigger breach, but managed to handle it more adeptly," adds Burns. "While TalkTalk's breach led to a parliamentary enquiry, Carphone Warehouse was able to limit the media attention received. Damage to its share price was short-lived and the

Photo by: Shutterstock.com

company lost only a small number of customers."

In the aftermath of a cyber incident, companies can usually deploy considerable PR resource to help manage reputational impact," says Nicholas Hartley, head of business improvement and innovation at specialist insurer Ecclesiastical. However, charities and not-for-profit organisations often lack the same level of resource or expertise to deal with the fallout.

"The damage that might be caused following a cyber incident could be far reaching and have an impact on future fundraising, as well as eroding public trust in the organisation," he adds. "Charities are often held to a higher standard by the public than large corporations and research by The Charity Commission revealed that one in three people said their trust in charities had fallen between 2014 and 2016."

Changing priorities

Airmic's CEO, John Ludlow, believes that underlying issues driving reputational risk are steadily becoming less about money and capital, and more about relationships and trust.

"Modern technology, social media and the way that news is now communicated all mean that both issues and bad news travel even faster," he observes. Social media not only spreads messages quickly but enables the impact of an event on a corporate to be gauged via Facebook and LinkedIn.

The way that people feel about issues has also become more important, with customers increasingly no longer prepared to put up with poor service. "There's always the option to take their custom and support elsewhere," Ludlow says. "Stakeholders not only have more power; in addition companies and organisations also have a whole plethora of different stakeholders."

He says that corporate risk managers have to identify the threats and vulnerabilities that matter most. "To understand that first involves understanding the stakeholders. The traditionally-held assumption that 'if it's legal, it's OK' no longer works.

"Risk management requires asking how stakeholders feel about an issue. For example, it might be perfectly legitimate for a company to exploit the advantages of a tax haven, but how do stakeholders feel about it?"

The Institute of Business Ethics (IBE) annually canvasses public opinion of business behaviour and the issues considered important. Its latest survey, issued last month, found that just over half (52 per cent) of respondents believe business behaves ethically; better than the 48 per cent recorded in December but still down on the figure of 59 per cent two years ago.

Corporate tax avoidance has been a major gripe since 2012, with 38 per cent of respondents citing it as an issue that needs to be addressed, against 43 per cent last year. Publication of the Paradise Papers in November, following on revelations in the Panama Papers, means that the issue is likely to continue in the spotlight.

Second comes excessive executive pay, rising from 28 per cent to 30 per cent. "Although there has been some movement on this issue by companies, as past shareholder approved policies take effect, it will still take time to move the dial," says IBE director Philippa Foster Back. "Naturally the public perception is that the changes are not quick enough." Exploitative labour – companies offering poor pay and working conditions – maintains third place at 27 per cent.

Photo by: Shutterstock.com

Future shocks
Biggest corporate casualty of 2017 could ultimately prove to be US film studio The Weinstein Company, with a stream of sleaze allegations directed at co-founder Harvey Weinstein. "Sexual misconduct and inappropriate behaviour has certainly become as damaging, if not more damaging, to corporates than financial impropriety," says Bickford.

Data gathered by Reputation Institute shows corporate governance – perceptions of fairness, ethics and transparency – has a more significant impact on reputation than ever.

"Governance now counts for 17.2 per cent of overall reputation, second only to perceptions of products and services," adds Bickford. "The public want to be able to trust the businesses they spend their money with, and the alleged behaviour seen at Weinstein puts that trust at most risk."

Looking ahead, as more companies introduce artificial intelligence and robotics any resulting redundancies will be news and carries a potential reputational risk. "AI strips out costs and increases returns, which is good for shareholders but destroys jobs and is therefore less popular with consumers," notes Lyndsey Bauer, a partner at Paragon International Brokers. "It can create, and fail to meet, consumer expectations over performance, physical safety, privacy or ethics."

The change will have to be carefully managed if a backlash is to be averted, which will involve retraining and reskilling affected workers where possible.

Reputational risk and crisis management insurance is available for companies seeking additional protection for their reputation and brand value, with a number of products such as AIG's ReputationGuard. Other leaders include Tokio Marine Kiln, the Liberty syndicate at Lloyd's and Novae Insurance (now part of Axis); however, Bauer reports that the market is relatively limited, offering capacity of £50m to £100m.

"Insurers approach reputational risk on the basis that if the loss is calculable, definite and derives from a fortuitous event then it can be insured," says Bauer. "However, as underwriters and buyers often place differing values on reputation it can be challenging to agree an amount acceptable to both parties. For the underwriter, revenue directly reflects the company's reputation, enabling them to measure loss arising from a specific event.

The company's risk/insurance manager will be invited to specify issues they regard as the biggest reputational threats. "This is important, given that views on corporate ethics and behaviour are regularly changing," adds Bauer. Once identified, the underwriter will ask why each issue is a matter of concern and a little more detail on the reputational threat posed.

"This is essential so that the company knows exactly what reputational risk coverage it wants, the scope of the insurance being purchased and the self-insured retention it is willing to bear."

The cover aims to ensure the company can financially survive a reputational risk event that impacts on its net profit and continue to meet its costs. It extends to the cost of employing a PR agency to devise a crisis communications plan. That plan, says Bauer means everyone should have a role that is tested, which includes communicating with customers, investors, employees and the general public respectively.

She cites Marks & Spencer as an example of adept crisis response. "When M&S suffered a data breach in October 2015 it owned up to it early on, demonstrated that it cared and assured customers that it was investigating the issue."

Graham Buck is a freelance journalist

Structural integrity

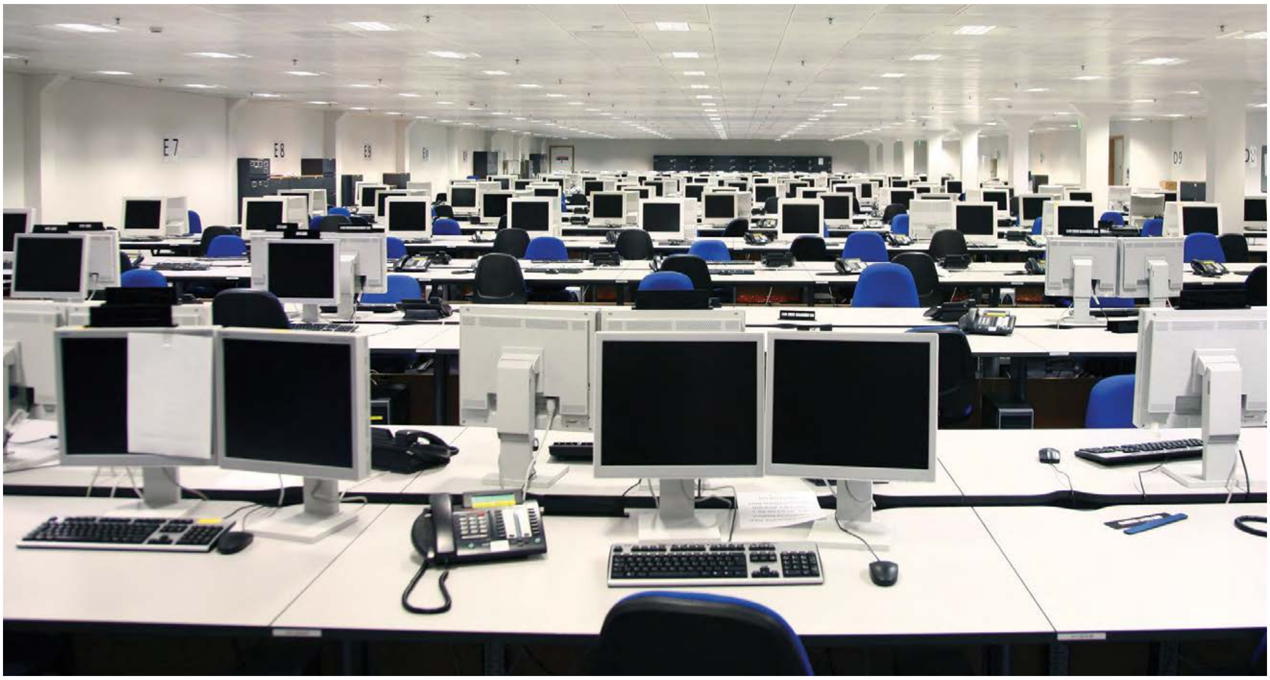
Martin Allen-Smith examines how continuity professionals can ensure that plans go beyond the theoretical to achieve true resilience in the face of an evolving threat

- The task of maintaining 'business as usual' remains a tough one, with a wide range of issues driving the corporate approach to business continuity
- The gap between principle and practice can be perilous for those who just tick the boxes without making the links to realities within the business
- Risks, technologies and expectations have shiften in recent years, which is having an impact on approaches to business continuity management

Headline-grabbing incidents during 2017 did much to help keep corporate eyes on the need for strong and stable resilience measures. But whether the risk is high-profile cyber or terror attacks affecting part of the operation, or a seemingly more low-key but sometimes just as disruptive incident such as a supply chain issue, the task of maintaining 'business as usual' remains a tough one requiring careful planning throughout the organisation.

There are a number of issues currently driving the corporate approach to business continuity programmes and policies. Managing director of European operations at Fusion Risk Management, Richard Cooper, believes that a primary issue is the need to 'operationalise' risk management. He sees his clients attempting to integrate risk management practises with business resilience to achieve a comprehensive and manageable programme. "Traditional GRC approaches have essentially failed to... accomplish this objective, given the level of dissatisfaction we find in the marketplace among practitioners and executives."

Cooper says legacy approaches in business continuity planning



have also failed to deliver true business resilience. "Along with other planning-oriented approaches, such as disaster recovery planning, and crisis response planning, legacy business continuity programmes have struggled to incorporate risk-based perspectives given the focus on delivering plan documents. It has fallen short in matching executive expectations for business resilience to the reality of an organisation's actual capabilities to respond and recover from disruptive events."

He says Fusions sees organisations beginning to work through these challenges, however, and many are recognising that too little value has been gained from the efforts and investments into achieving this goal.

The gap between principle and practice can be a perilous one for any organisation tempted to chase the aim of ticking the boxes without linking these ticks to the day-to-day reality of the business. Cooper says: "A key gap we find is the lack of a manageable 'information foundation' about business risks, business dependencies, and business impacts.

So what measures do businesses need to take to give the theory the necessarily reality check – and what are the obstacles potentially holding organisations back? For Cooper, this is to take a risk-based approach to business resilience which brings together risks, dependencies and impacts across all categories of business disruption.

"Next, organisations must understand not only their risk tolerances across myriad risks but more specifically their tolerance for disruption, as well as their capabilities for response and recovery. This can be complicated or fairly straightforward depending on the approach."

Another approach

Suggesting that the principal gap is caused by the disconnect between theory and a practical solution that can applied across the organisation, ClearView Continuity's chief executive Charles Boffin says that while business continuity teams will generally have a very good idea of what needs to be done, but the 'how' in many large organisations is often not so easy to define.

He believes this frustration has a number of drivers. Firstly, internal reprioritisation of investment in the business continuity process at corporate level, for which – as with all major initiatives – cost pressures and headcount reductions provide significant challenges. Secondly, embedding business continuity as part of 'business as usual' is a key challenge. Technology can help here says Boffin, but, ultimately, business continuity teams have to actively engage their business counterparts in the process on a 'hearts and minds' level.

Thirdly, a big requirement is corporate willingness to make it happen at all levels of the organisation, with executives who understand and accept that business continuity is a corporate imperative, and are prepared to create a culture which recognises the need for continuity throughout the business.

Boffin says that the solutions are very much the antithesis of the problem areas: "Investments in business continuity, using smart technology as an enabler, driving a culture that recognises business continuity as an important foundation and good governance process in place, driven by active recognition at board level, not just a tick in the box."

At the programme management level, new technologies are enabling the transition of business continuity tools from document-management systems to data-management systems, to reduce work effort and achieve more timely information, These technologies are enabling better connection of risks, dependencies, impacts, and response/recovery capabilities, for a more comprehensive understanding of the risk profile of the enterprise, which can results in a better matching of risk tolerances to investments in mitigation and resilience.

Fusion's Cooper suggests that, going forward, these technologies should enable more effective activation of response and recovery capabilities, and more comprehensive recovery orchestration across all the workstreams of activities to minimise business impact and accelerate recovery, with greater confidence and less execution risk.

New technologies are also coming into play to broadly engage employees throughout the enterprise with purpose-built software tools that make it easy to receive and acknowledge alerts, provide situation reports, and participate in the incident response process as needed. In addition, organisations are now recognising the need for flexible solutions that can keep pace with changing business requirements, and avoid becoming constrained by rigid systems that will not easily adapt to the organisation's programme needs.

Looking ahead

Technology clearly has a key part to play in a more resilient future, and has the potential to achieve this in a number of important ways. It can help attain resilience of operations through the growing robustness of IT infrastructure and 'always on' solutions. It can also support processes for resilience – including software, mobile access, and multiple communications channels – which all provide a technology framework to supports the development, maintenance and effectiveness of plans.

While there are huge opportunities to come, the challenges remain sizable, however. ClearView's Boffin says planning for the unexpected will of course remain at the heart: "Business continuity plans focus, quite rightly, on risk, impact and continuity, but there is a growing range of ad-hoc threats that may lead to the need for different solutions.

"Cyber threats cast their shadow wider than core IT systems. Terrorist incidents create wide-scale physical events that had previously not appeared on the organisational radar. These events are often hard to foresee; 'traditional' responses may not always be sufficient, and organisations have the dual challenge of structured responses to events that can be forecasted – such as inclement weather for example – and those that appear with little or no warning."

Expectations too have shifted in recent years. Organisations have had to react to the commercial pressures from clients, shareholders and other stakeholders for 'always available' services. Boffin adds: "Continuity becomes the expected state and, thus, organisations that cannot or do not deliver on this expectation are faced with the ultimate threat – their very survival."

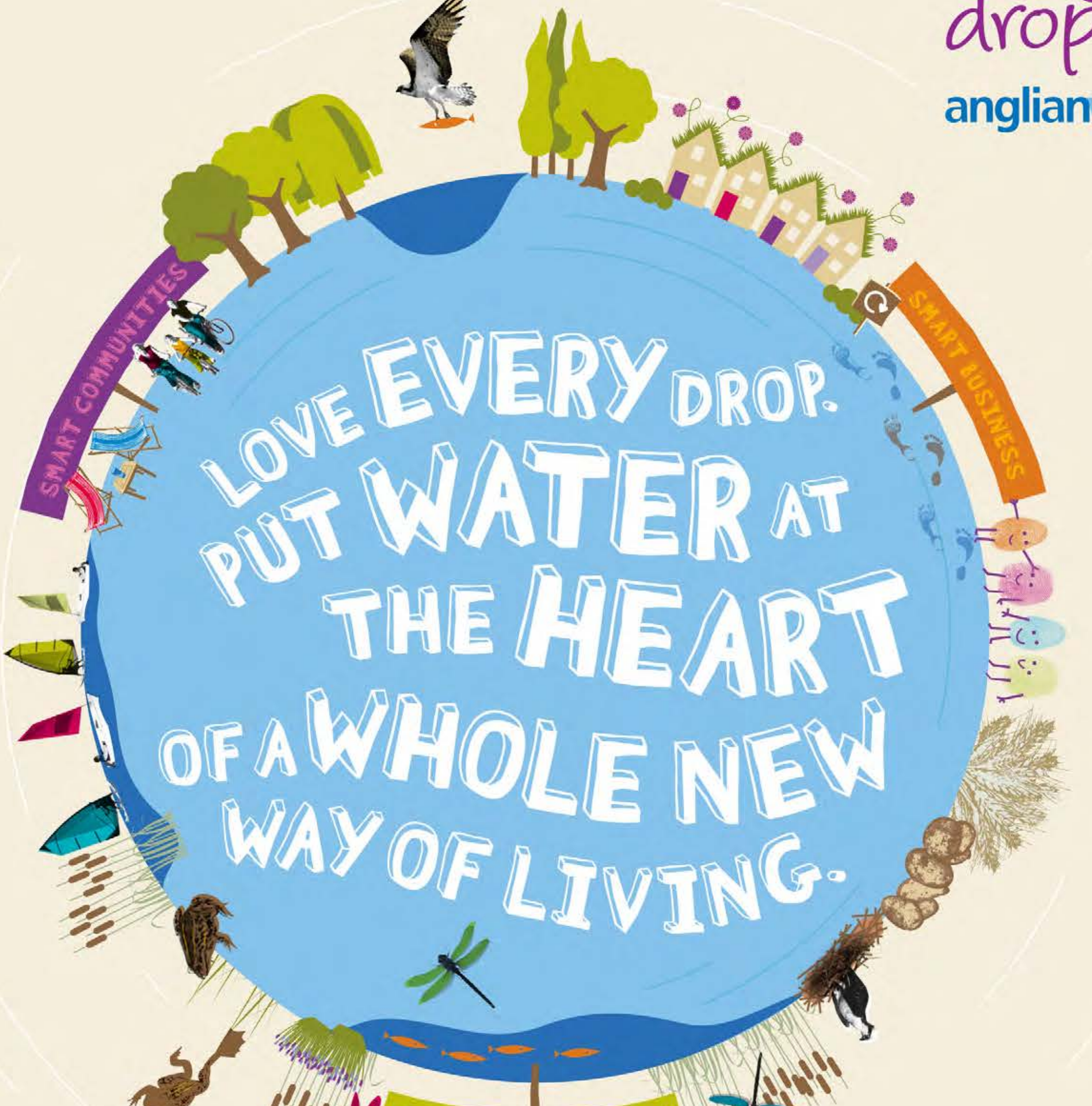
Andrew Lawton, founder and CEO of Fortress Availability Services, suggests the next stages of business continuity planning will depend on how we manage events using technology. "Our AlertSense tool not only enables crisis communication [with] staff or resources but also provides a platform for two-way communication. This, crucially, also gives the crisis management team the ability to [communicate] tasks to staff and track the completion of those tasks through an inbuilt task manager. This activity is completely integrated into the current tool such as RSA Archer or Fusion, taking tasks and allocating them to resources as defined in the plans or developed 'on the fly' to cope with the actual event. This means that crisis managers have far greater controllable resources available to them to get crises under control and the recovery underway."

There are a host of new challenges on the horizon that will have a bearing on the likely success of a programme's implementation and execution. Although the nature and diversity of the threats to an organisation may change over time – and the specific measures needed to address them – at the core of the approach to countering them are some tried and tested principles. Fusion's Cooper says: "One of the biggest obstacles remains the mindset of 'planning' and 'compliance'-oriented programmes. Documents and checkmarks can create the illusion of business resilience, when actual capabilities to understand risks and respond effectively to disruptive events can remain significantly lacking."

He adds that these mindsets also miss the strategic opportunity of business resilience as the basis for competitive advantage. As Cooper says, an organisation's ability to tolerate disruption, through effective business resilience, can change the risk profile of an organisation and change the strategic decisions about which risks to avoid, which to transfer, and which to accept.

Martin Allen-Smith is a journalist

love every drop.
anglianwater



TOMORROWS FORECAST IS FOR MORE PEOPLE AND LESS RAIN.

CIR Risk Management AWARDS 2017

WINNERS' REVIEW

The 8th annual Risk Management Awards

Celebrating success within the practice of risk management

The winners and highlights

cirmagazine.com/riskmanagementawards

Sponsored by

love every drop anglianwater

In association with

airmic alarm Chartered Insurance Institute iirsm THE INSTITUTE OF OPERATIONAL RISK

CIR | Risk Management AWARDS 2017

This year's winners are

Risk Management Innovation of the Year
WINNER: Costain Group

Best Use of Technology in Risk Management
WINNER: Neural Technologies

Cyber Security Product/Partnership of the Year
Product WINNER: ZoneFox
Partnership WINNER: Crises Control/ThreatSpike

Risk Management Specialist Company of the Year
WINNER: Aviva Risk Management Solutions
Highly commended: Ventiv Technology

Risk Management Product of the Year
WINNER: International SOS

International Risk Management Award
WINNER: Horizonscan

ERM Strategy of the Year
WINNER: Vodafone

Operational Risk Initiative of the Year
WINNER: Argo Group

Public Sector Risk Management Award
WINNER: Alarm

Major Capital Projects Award
WINNER: Network Rail - Northern Hub Alliance

Risk Management Programme of the Year
WINNER: Severn Trent

Risk Management Team of the Year
WINNER: National Operational Guidance Programme

Newcomer of the Year
WINNER: Pauline McNulty, Liberty Specialty Markets

Risk Manager of the Year
WINNER: Rich Williams, Office for National Statistics



cirmagazine.com/riskmanagementawards

Risk Management Specialist Company of the Year

Chris Andrews, head of Aviva Risk Management Solutions, pictured with Risk Management Awards judge and head of operational risk and regulatory advisory at Credit Suisse, Andrew Sheen and host Lucy Porter

Winner Aviva Risk Management Solutions

The judges said: With so many worthy contenders, the specialist category was particularly closely fought in 2017. This year's winning organisation was able to demonstrate how successfully it leverages in-house skills, expertise and knowledge to build a suite of services that protect the things that are most important to its clients, having considerably expanded its range of services over the last 12 months.

Aviva is the UK's largest insurer, with 33 million customers worldwide. It paid out £34.4 billion in benefits and claims to its customers in 2016. It has a strong international presence in selected insurance markets across North America, Europe and Asia.

Historically, insurance business has been somewhat transactional, but Aviva recognises that increasingly, supporting clients is more than just paying claims. As such, the company has built, and is expanding, a range of risk management solutions that can mitigate against losses on a day to day basis, its solutions designed to suit the needs of all clients – from sole traders in the construction industry to multinational conglomerates.

Over the years Aviva Risk Management Solutions has shared its wealth of knowledge with brokers and customers and it continues to develop innovative and cost effective solutions for its customers in the commercial market.

"Within Aviva Risk Management Solutions (ARMS), we recognise that our client's needs in managing risks within their business are constantly evolving," comments head of ARMS, Chris Andrews. "With our team of over 100 risk consultants we aim to always offer the right solutions, be innovative in our approach and always put our client's needs first. With an average experience of 22 years for our consultants, our use of prevention technologies and our extended network of risk management partners we have a suite of solutions to meet the complex risks that our clients face. That's why our approach is tailored, bespoke to the businesses we help protect to reduce the risk of loss.

"We're extremely proud that our hard work, our breadth of risk management services and our dedication to doing what's right for our clients has been recognised," Chris adds. "We're now working on developing our expertise and our suite of solutions further to ensure we continue to be market leading."

aviva.co.uk/risksolutions

AVIVA

CIR Risk Management AWARDS 2017

winner

Risk Management Specialist Company of the Year

International Risk Management Award

The Horizonscan team pictured with Risk Management Awards judge, Edward Sankey and host Lucy Porter

Winner Horizonscan

The judges said: The clear winner in this year's category, this company offers a unique solution for stress testing crisis readiness that provides a lens into areas of resilience, as well as vulnerabilities that need to be strengthened.

The winning entry: Horizonscan Ltd provides a global consultancy service that includes running crisis-scenario simulations with clients across many sectors and geographies.

Protecting key and critical assets is a vital part of any risk management programme. Founded in 1919, Cummins is a global power leader that designs, manufactures, distributes and services diesel and natural gas engines and engine-related component products. The company currently employs over 55,000 people. Cummins is a global business with varied operations and complex internal and external supply chains. Its core values are integrity, trust and dependability; a commitment to all of its stakeholders permeates throughout the organisation, and is fundamental to, and consistent with, Cummins' risk philosophy, risk appetite and risk mitigation strategies / programmes.

Following an extreme weather event and business interruption loss, Cummins committed itself to engaging all 'key and critical' locations to make itself more resilient to crisis events. Analysis and evaluation highlighted facilities on all five continents, deemed to be key and critical and therefore within scope of a new, global, stress-test simulation programme.

As a consultancy specialising in crisis-simulation exercises, Horizonscan was selected as the business partner to undertake delivery of the project. Many of the staff within Horizonscan were time-served senior officers from the police and fire service, with many years of crisis command to draw from.

"The Horizonscan team is really proud to have its work recognised by CIR Magazine's Risk Management Award," says Horizonscan's Russ Timpson. "We have worked hard with this particular client for the past three years to develop its annual stress test programme and it's now being rolled out around the world with noticeable improvements in their resilience. We are now using what we've learnt to help our other customers, but adapting it to their particular sectors and individual business requirements. 2018 is looking very positive for us as a company as we continue to build our team of experienced practitioners who can support our clients with the changing risk landscape."

horizonscanbcp.com

HORIZONSCAN

RISK - RESILIENCE - READINESS

CIR Risk Management AWARDS 2017 winner

International Risk Management Award

CIR Risk Management AWARDS 2017

Best Use of Technology in Risk Management

Eugene O'Reilly and Paul Cox, Neural Technologies, pictured with Wayne Rigby, Insurance Manager at Doncaster Council & Director at Alarm and host Lucy Porter

Winner Neural Technologies

The judges said: Referred to by the judges as representing a 'quantum leap forward', there was one clear winner in this dynamic category.

The winning entry: The winning entry in this year's Best Use of Technology in Risk Management category was focused on the use of the Optimus Fraud Management and Anti-Money Laundering solution by telecommunications company Safaricom. Based in Kenya, the company deployed the solution to complement their globally renowned mobile money solution M-PESA.

The rapid rise of services and subscribers offered through M-PESA comes with a plethora of new scenarios relating to money laundering, financial crime, and terrorism.

Neural Technologies was selected to address these risks by providing a powerful, future proof anti-fraud solution, thus aiding Safaricom invaluably in their risk management and resilience functions.

Neural's innovative solution now enables Safaricom to verify the identity of applicants to mitigate fraud and money laundering.

Neural Technologies exists to bring accord and insight to enterprise data. Founded in 1990, the company has a global presence with customers in 45 countries. Neural Technologies' Optimus Platform helps users transform their businesses by delivering smarter insights, better decisions and faster actions to support digital transformation strategies. This product arms users with the capabilities to deliver new business models faster, enhance customer loyalty and improve operational efficiency.

By using the Optimus Platform, enterprises can ingest and organise their data records to ensure they bring accord and insight to their data. By applying the relevant microservices to such data records, enterprises can interpret, act and present significant insights and facilitate informed business decisions. Whether it be fraud management or mediation, all Optimus solutions are agnostic and unique in their ability to connect enterprises to all of their data records. Open source scripting language delivers high flexibility and allows any user to develop new solutions with ease.

neuralt.com

Neural Technologies

CIR Risk Management AWARDS 2017 winner

Best use of technology in risk management

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

RISK SOFTWARE REPORT 2018

The big picture *The ability to gather risk data from across the whole organisation and to keep it in one central repository makes the job of managing enterprise risk more cost-effective and reliable. David Adams reports on developments in risk software* p38

The Risk Software Report 2018 *Your annual guide to products and features in the global risk software market* p40

Market analysis • Products • Product features • Supplier Directory

The big picture

The ability to gather risk data from across the whole organisation and to keep it in one central repository makes the job of managing enterprise risk more cost-effective and reliable. David Adams reports on developments in risk software

The language of risk management is everywhere: in organisations of every kind you will find sections of annual reports or executives' presentations dedicated to it. While adoption of sophisticated risk management technologies is still spreading slowly, it is increasing, across all industry sectors, as more organisations recognise the value of these technologies, as a means of improving understanding of risks, thereby protecting the organisation and delivering efficiency and cost savings.

Adoption is also driven by the need to ensure compliance with various regulatory requirements: at present, many organisations are focusing on the EU Global Data Protection Regulation (GDPR), which comes into force in May 2018. Technology vendors are responding to the growing variety of end user needs by developing more innovative risk management technology.

As one might expect, use of these technologies is particularly widespread in the insurance sector. Since 2016 the Belgian insurance broker ADD has been using technology provided by risk software specialist Origami to collect and analyse risk and insurance data relating to its clients. It also uses the technology when collaborating with other insurers and brokers through the Worldwide Broker Network. Matthew Serck, commercial manager in the international department at ADD, cites the ability for both broker and client to access the same data, improved data quality and enhanced reporting and scheduling capabilities as the most important attributes of the system. "[The] technology has proved to enable all parties to work more efficiently," he says. "This has been a resounding success."

The market for these technologies is still divided into organisations using Risk Management Information Systems (RMIS) primarily as a means of gathering data for insurance purposes and to manage the total cost of insurable risk; and those seeking to take a broader approach to risk management. Origami's Neil Scotcher believes the latter approach is becoming more widespread, as organisations of all kinds use risk information to inform business decisions.

The decision to invest in these technologies is determined in part by the industry or sector in which an organisation operates. In sectors like energy or mineral extraction, technology purchasing decisions are driven by the operational risks these businesses face; in the financial services sector the key risks may relate to compliance, vendor risks, or data management and security.

But cyber and digital risks demand more attention in almost every organisation, in part because of the increased use of online and cloud technologies, and software as a service (SaaS) solutions. The ever-evolving nature of digital and cyber risks also means there is a need for solutions flexible enough to be adapted as circumstances demand.

Gisle Bråstein, global product manager, enterprise risk management solutions, at Norway-based risk

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

technology provider DNV GL, says the growth of the Internet of Things means data collection and analysis processes are becoming more complex. Many DNV GL clients work in the maritime, oil and gas and energy/utility sectors, so there is a need to collect risk-related data from a wide range of systems, facilities and both physical and digital assets, from power stations, oil rigs and pipeline infrastructures to operational systems on ships and in ports.

The need to gather data on risks from every part of any organisation makes it essential that risk management technologies are user-friendly, so they can be used by risk owners across an organisation, often via mobile devices, so that non-specialists become an organisation's "eyes and ears when it comes to identifying and monitoring risks", as Fusion's Andy Mercker puts it.

Risk information then needs to be analysed effectively. Ventiv's technology aims to put predictive data analytics that might previously have required a team of data scientists in the hands of risk managers, according to global product manager Angus Rhodes. His colleague, David Thomas, director at Webrisk (a RMIS acquired by Ventiv from Effisoft 2017), believes analytics capability will become the most important differentiator for risk management technologies.

Another differentiator is ease of integration. That can mean integration of tools delivering different forms of risk management, to create an ERM solution; or integration between risk management software and other business systems.

Some organisations want to integrate risk management capabilities with other solutions to create comprehensive governance, risk and compliance (GRC) capabilities. The aim is to ensure organisations have access to a single version of the truth when assessing risk and compliance status.

Bram den Boer, principal business analyst, market technology, at Nasdaq BWise, says the ability to access this kind of integrated overview forms an important part of the business case for these technologies. "That's where they see the benefit, because they don't have that overview at the moment," he says. "For them it's a case of 'I would like to see all my risk issues, and who is taking action to mitigate those risks.'"

Nasdaq BWise provides organisations with complete GRC capabilities; and offers support to help align audit, compliance and risk management capabilities within the organisation. Its GRC platform includes solutions for internal audit, information security and sustainable performance management, alongside compliance management and its comprehensive risk management solution. Businesses using the platform include Orange, Roche and Swiss Life.

Any GRC platform stands or falls on the quality of the data it holds. Coca Cola European Partners (CCEP) is the largest independent Coca Cola bottler in the world. Created through a merger of three bottling businesses in 2016, it is a €12 billion business that operates in 13 territories and employs over 24,000 people. A RMIS solution supplied by Riskonnect and originally implemented in 2013 is now complemented with a Riskonnect GRC platform rolled out in 2017.

Risk analyst at the company, Joseph Tunstall is using the solution to aggregate risk data relating to the operations of the company and its predecessors going back 15 years, alongside new risk data captured from across the business: everything from liability claim schedules to employee and product data.

"The most important thing we're trying to do with this system is to report on the total cost of risk," Tunstall tells me. "Utopia for us would be to have all of our risk data in a central repository. I don't view this process as something that will ever be completed: it's about the continual aggregation of data. Off the back of that will come all the things we should be doing with that data: analysis, reporting, understanding where we should have more of a focus."

There is also a growing trend for integration of risk management capabilities with business continuity and crisis management tools such as mass notification, according to Fusion's Andy Mercker. His company describes itself as a "provider of business continuity risk management".

"We find that this term really captures this confluence of not only the risk agendas but also, if any of these risks were to occur, of how organisations go about responding to and recovering from them," Mercker explains.

All these capabilities may sound very attractive in theory, but there is always a need to gain buy-in at the top of an organisation for investment in them. For Ventiv's David Thomas enhanced analytics capabilities, providing real time insights to the board, are of paramount importance. "It becomes easier to make a business case when you're able to deliver real time analytics to help decision-making," he says.

Mercker believes that while there may be many reasons why organisations choose to invest in these technologies, for a growing number it has simply become essential to be able to understand the risks that could disrupt their operations and the potential consequences of that disruption. Executives need to know that in the event of a major incident they can stand up in front of employees, customers, shareholders and the media and explain that all necessary precautions had been identified and taken, says Mercker. As he says: "Not having a clear understanding of risk and resilience is no longer acceptable."

ACTIVE RISK MANAGER
SWORD ACTIVE RISK

Sword Active Risk supplies enterprise risk management (ERM) software that aims to drive business performance by providing management and the board with information that supports more informed decision-making. The Sword Active Risk approach to ERM enables a single view of risk across the organisation, linking the risk management process with business planning activities. From managing project and programme risk through to strategic business planning, Active Risk Manager (ARM) helps organisations identify, analyse, control, monitor, mitigate and report on risk across the enterprise. ARM addresses the risk management needs of the entire organisation, covering four key areas: operational risk management; project risk management; governance and compliance; and opportunity management. The latest version, ARM 10, delivers additional collaborative working functionality in support of ARM's Mobile First and cross-platform strategies. The full solution portfolio comprises ARM Core, ARM Risk Express, ARM Risk Performance Manager (RPM), ARM Risk Connectivity, ARM SNAPPit, ARM Apps, ARM Unplugged, and ARM Cloud. ARM Risk Express provides an intuitive interface for business users that replaces spreadsheets. It presents risk information in an editable grid format, with dials and filters enabling users to update information quickly and easily within seconds. Risk Express is fully integrated with the ARM core platform, maintaining data integrity, and full governance and transparency. ARM SNAPPit, which is downloadable from app stores, enables business users to record details of incidents, accidents, hazards, concerns and observations on the spot. It updates ARM in real time so that investigations and mitigations can begin immediately. ARM is supplied with a library of standard reports and analysis tools including ARM Visualizer and bowtie analytics. Risk Performance Manager (RPM) provides the ability to create dashboards, tables, charts and matrices without the need for specialised IT or report writing knowledge.

sword-activerisk.com

BARNOWL
IDI TECHNOLOGY SOLUTIONS

BarnOwl is a fully integrated risk management, compliance and audit software solution supporting best-practice frameworks. BarnOwl Risk and Compliance offers end-to-end GRC management including compliance management (third party regulatory content), incident management, performance management (KPIs, KRIs, KCIs), workshop voting and online updating of action plans, surveys and checklists, risk and control self-assessments supported by automated email notifications, reminders and escalation. BarnOwl Audit supports end-to-end risk and control based auditing.

barnowl.co.za

EXONAUT
4C STRATEGIES

This ERM tool is designed to help users take control of their risk management activities in accordance with ISO 31000. Features include risk identification, analysis and treatment, fully configurable risk categorisation and classification, enterprise user management allowing full control of rights and privileges. It is designed to allow the optimisation of financial reserves and economic capital across the portfolio of organisational units and projects. Work flow management is driven by assignment of responsibilities and risk ownership, and real-time monitoring of current risk exposure and ongoing risk treatment activities is available. This product aims to deliver transparency of risk exposure to all those who need to know. It also serves to improve understanding of the financial budgeting required to protect organisation and reduces the time spent inputting, consolidating and gathering risk data.

4cstrategies.com

FIGTREE SYSTEMS
NTT DATA FIGTREE SYSTEMS

NTT DaTa
NTT DATA Figtree Systems

This system is used globally for incident and OH&S management, claims management, corporate insurance and employee benefits management, fleet and asset management and ERM. System features include workflow automation, document management and creation, reports and dashboards, smartphone and web-based data capture and email notifications. The configurability of the system ensures that variations in business processes are catered for. The system is available in the traditional client server model as well as a SaaS model from ISO 27001 compliant datacentres. Incident and OH&S management provides an easy way to log an incident or hazard from either a mobile device or a web browser. An initial incident notification only requires that some basic details be filled in. Configurable workflow rules notify relevant personnel to review forms. Claims management processes, including first notification of loss, reserve-setting, payments and recoveries are comprehensively covered by the system. Loss adjusters and insurers can also collaborate in this process.

All types of claim, including motor, property, life and disability, liability and workers compensation claims, can be managed using this system. This tool performs corporate insurance management functions including maintaining local and master policies with aggregate, deductible and excess values, maintaining country-wide asset and exposure lists, generating certificates and invoices and performing annual renewals. Credit risk claims, employee benefit covers, policies and master agreements can also be managed. The ERM process of risk assessment, risk treatment, risk monitoring and risk reporting can also be performed using this product. A graphical matrix of severity and impact gives a summary of risks at business unit levels, as well as the enterprise level.

figtreesystems.com

FUSION FRAMEWORK CONTINUITY RISK MANAGEMENT SYSTEM
FUSION RISK MANAGEMENT

Fusion Framework software is designed to deliver an integrated risk management programme across operational risk and business resilience including business continuity, disaster recovery, crisis/incident management, third party / vendor risk, cyber and IT risk and facilities risk. It is designed to carry out risk and impact assessment, contingency planning, exercises and simulations, crisis/incident management, as well as reporting, analytics, dashboards, workflows, approvals, enterprise collaboration and mobile. Flexible and configurable, the software is designed to help users keep pace with changing needs and programme evolution. Fusion Framework Enterprise Community is designed to engage all employees for incident management, response, safety and physical security through a simplified mobile and desktop platform.

fusionrm.com

GUARDIANERM
INCONSULT

GuardianERM is a web-based integrated governance and risk management system, available hosted or as SaaS. It is designed to integrate, automate and streamline important management activities that support corporate governance. GuardianERM supports ISO 31000 and allows documentation of action plans, business continuity and recovery strategies on a risk-by-risk basis. It has a number of interactive dashboards and graphical reports to assist management in the analysis of the various forms of data. Standard reports with extensive filter options and user-defined reporting function provide information as required. GuardianERM is fully scalable, from one user to enterprise-wide. Users can also opt to purchase individual modules.

guardianerm.com

HAWKSIGHT SOFTWARE
HAWKSIGHT SRM

This software is designed to enable organisations to take an enterprise-wide approach to security risk management. Reporting tools give full visibility of the threats and issues impacting projects, calculating risk based on ISO 31000 and associated Australian standards. The latest version of this software includes mapping dashboard interface and live incident data feed options, global-to-local scalable mapping overview, project locations colour coded by risk level, incorporation of selectable satellite tracking layer and comprehensive security risk assessment functionality. An operational risk management toolkit is combined with a risk modelling and simulation capability. It also provides risk management legacy information. Upcoming developments for 2018 include a broader range of tools to interrogate and chart incident data within a specified geographic area; linear and multiple location risk analysis to assess risk between two or more points, or across multiple locations which can be assessed under one project; the development of a collector app to enable offline data collection and report builder functionality for both Word and PowerPoint. Available as a hosted service or on a bespoke delivery basis.

hawksightsrm.com

JCAD LACHS
JC APPLICATIONS DEVELOPMENT

JC Applications Development has been a market leader in the development and implementation of software for risk management and claims processing for over a quarter of a century, and has a large client base of over 200 organisations from a diverse range of industries and the public sector. JCAD LACHS is a claims handling system that aims to enhance efficiency and streamline the claims handling process. The way in which claims are handled is constantly changing, and this provider continually develops its products to comply with changing market needs. This product is designed to help users efficiently process claims in-house; view data and generate reports easily; reduce claims and insurance premiums; maintain historic data; enable powerful and flexible reporting and improve efficiency and productivity. Features include a range of additional modules and central data management. This off-the-shelf system is designed to be scalable and intuitive.

jcad.co.uk

JCAD CORE
JC APPLICATIONS DEVELOPMENT

JCAD CORE is offered as a simple to implement and cost-effective solution for risk and compliance management. Simple to use, all stakeholders are able to participate in the risk management process. This product is designed to help users proactively identify, monitor and mitigate risk; ensure corporate governance; capitalise on new opportunities; drive effective business strategy and improve efficiency. Features of JCAD CORE include multiple registers; performance metrics; interactive dashboards; configurability and automated alerts. As a web-based solution it is suitable for both small and large organisations.

jcad.com

KNOWRISK
CORPROFIT SYSTEMS

KnowRisk supports a well-defined risk management corporate governance framework. This product covers ISO 31000 risk management, compliance, project risks, audit and safety management.

corprofit.com

MACLEAR EGRC SUITE
MACLEAR

The Maclear eGRC Suite is a proprietary solution for capturing, monitoring, measuring and managing integrated risk and compliance across the enterprise, and is designed to help strengthen corporate governance processes, facilitate effective risk and compliance management and convert data elements into actionable data. The product is a modular, scalable solution that helps enable continuous monitoring and provide transparency into enterprise-wide risk posture. Maclear eGRC Suite enables businesses to address immediate pain points, mitigate risks and successfully manage the complexity of the dynamic modern regulatory and compliance environment. The Maclear software solution enables effective monitoring in the form of dashboards, macro-level analysis and automated workflows for reporting, assessments and remediation management. The solution also provides for operational support through configurable controls, access automation, testing and integration with third party tools. Designed as a modular suite of products that integrate to provide a complete solution; modules can either be implemented individually or collectively – based on an organisation's needs.

maclear-grc.com

MAGIQUE GALILEO
MAGIQUE GALILEO

Magique Galileo is a fully integrated web-based system for ERM and internal audit. Magique is a web-based risk management tool is designed to help organisations record, evaluate and manage their risks. In addition to the risk register and an emerging risks register, there are options for loss events/incident management, for scenario analysis, a questionnaire system for control self assessment, a policy compliance system to monitor compliance with regulatory requirements and an action tracking system for recording and tracking of further required actions from any part of the system. Galileo is the optional internal audit module covering risk-based auditing, audit management, resource scheduling, work papers, compliance questionnaires, issue tracking and extensive KPI/MI reporting. Magique and Galileo can be used independently or fully integrated to support a risk-based audit methodology. Both systems can be configured to the user client's chosen terminology and methodology.

magiquegalileo.com

MARSH CLEARSIGHT
MARSH CLEARSIGHT

The Marsh ClearSight platform is designed to be quick to learn and easy to use with features that are intuitive. Access to this system is available from almost any device – tablet, laptop, or desktop. This product was designed to seamlessly integrate data from multiple internal and external data sources, including carriers and third-party vendors, as well as HR and finance departments.

marshclearsight.com

METRICSTREAM RISK MANAGEMENT SOLUTION
METRICSTREAM

This product provides an integrated and flexible framework for documenting and assessing risks, defining controls, identifying issues and implementing remediation plans. It is not designed to support or process insurance claims, policy and premium management and renewals. The solution is used for managing enterprise, operational, compliance, IT risks, vendor, reputational risks.

This tool provides in-depth, realtime insights into changing business conditions and risks that could impact a business. The M7 platform delivers an improved user experience, high configurability, mobility, powerful analytics, and a future-ready architecture for GRC. The MetricStream integration framework has the capability of integrating with external systems using its data integration engine. Available on-premise or in the cloud, technical support is available 24/7 from support centres around the globe.

MetricStream's commercial models are based on the number of application modules and number of users. The primary model is subscription-based with some exceptions on perpetual licencing.

metricstream.com

ORIGAMI
ORIGAMI RISK

Origami Risk's RMIS, Claims Management System and Policy Management System were designed to offer speed, flexibility, automation, data import and export tools, claims management tools, analysis and reporting tools. Users deploy this product to carry out property values collection; claims administration and incident intake; policy/programme management; claims, internal and safety audits' governance risk and compliance; captive management; reporting and analytics; and asset and fleet management. This product has the versatility to interface with multiple systems, including those of TPAs, insurance carriers, brokers, agents, banks and payroll providers. Users can capture, import and analyse information from various external and internal sources, databases and spreadsheets to understand and analyse loss trends, pinpoint cost drivers and identify best practices. Origami Risk's data export features enable clients to share timely information internally and with key providers to promote safety, and allocate costs to operating units and individual cost centres. Other features enable clients to manage documentation, contracts and insurance policies more effectively.

origamirisk.com

PREDICT!
RISK DECISIONS

Predict! Risk Controller is a risk management tool designed to help users quickly identify which risks and, most importantly, which actions need their attention. Message-driven prompts encourage users to engage in managing risks and actions. Bespoke visual reporting, and fully integrated risk analysis provide up-to-date contingency and confidence information. Key features include entering and editing risk and action information; threat, issues, opportunity and action (mitigation and fallback) management; single page for quickly updating a risk and its actions; bulk updating of multiple risks in one go; and rapid access to risks and actions. With this product, users can easily create lists of risks based on criteria and chosen columns. Quick, simple reporting and exporting is available directly from core screens. A customisable reporting capability, including trends and visualisations, is also available, along with MS Excel upload/download capability.

riskdecisions.com

QUANTATE
QUANTATE

Quantate's products are delivered in a secure SaaS environment, accessible via a personal dashboard. Dashboards show configurable information such as key responsibilities, tasks to perform, their reports, and issues raised or escalated for their attention as well as jump off points to the relevant parts of each application. Quantate Risk provides a platform that enables organisations to record information and monitor activities that are consistent with the principles and guidelines of ISO 31000. Quantate Compliance is a web application that provides a platform for the management and monitoring of obligations. Quantate Project has been designed specifically to support the management of project risk. It uses Monte Carlo techniques to quantify project risk, both cost and schedule. By aggregating this information across a portfolio of projects users can predict when the peaks and troughs of risk exposure occur. Safety Kit fulfils the requirements of a best practice health and safety framework. It has been developed specifically to suit the needs of small to medium businesses. Licencing is generally offered on an enterprise-wide basis and is independent of number of users.

quantate.com

RISKCONSOLE ADVANCE
VENTIV TECHNOLOGY

Recent improvements of this popular platform include enhanced system performance and a more modern, clean design and intuitive layout. RCA ensures high-quality data consistency with features including required fields, in-situ validation, customisable look-ups and full audit and roll-back functionality. Its embedded interactive dashboards provide real-time data visualisations that help risk managers make evidence-based decisions on where to focus their efforts. A wide range of configuration options include integrated mapping and map search features and a powerful global search function. Search results can be refined using Boolean strings to deliver results quickly. Users can also take their configuration offline from the production system and move it into a sandbox, where they can safely make changes to that configuration and then reimport their changes back into the production system. A completely open architecture means users can create unlimited tables and fields.

ventivtech.com

RISKHIVE ENTERPRISE RISK MANAGER
RISKHIVE SOFTWARE SOLUTIONS

This is a cloud risk database that helps manage, control, and report on risk, opportunity and assumptions. It can quickly import, consolidate and maintain risk registers to deliver a simple and cost-effective way of centralising risk data into an analysable organisational risk portfolio.
ERM has advanced visualisation and modelling including interactive risk bowtie graphics in which users can build and manage risk scenarios that incorporate the controls, responses and fallbacks associated with risk management. Causes can be triggered by failed assumptions or KRIs. ERM also has horizon-scanning risk-radars that show what risks are potentially coming from where and when using an add-on KRI monitoring service and feeds a configurable dashboard that displays both internal and external KRI status, delivering effective pre-emptive analytics. KRI data can be supplied to corporate dashboards or linked directly to ERM risk causes to automatically prompt emerging issues and trigger responses. Links to objectives, assets and insurance policies assist in understanding value at risk, and novel techniques for decomposing and reclassifying risks by management processes can significantly alter and improve the risk profile whilst demonstrating the effectiveness of risk management. ERM can use multiple currencies and languages simultaneously and display any fields, interfaces, user controls or reports in any combination of languages and currencies. ERM is used on major capital projects globally and is available on SaaS and cloud or internal installation.

riskhive.com

RISKONNECT
RISKONNECT

Riskonnect allows organisations to understand, manage and control risks. Its fully integrated risk management solutions are configured to meet a user's specific workflow, processes and reporting needs. A centralised database and analytics system provides for a secure, online reporting environment with a simple user interface that allows clients to create, modify and manage all workflow rules, custom data fields, screen designs, user security, and other system configurations necessary for important daily operations.

Riskonnect RMIS is designed to manage incidents, claims, litigation, exposure, property, including COPE, policy management and asset management. Riskonnect's Compliance and Regulatory Management solutions are designed to instil a culture of risk management, while optimising internal controls and improving compliance. The Audit Management solutions are designed to allow users to easily identify an audit subject, develop an audit plan, documentation of the audit, agreement on any audit finding, oversight of finding remediation, and reporting to an audit committee.

The provider's Health and Safety Management solutions aims to give risk managers and safety professionals the ability to provide actionable business intelligence to senior management and key stakeholders. Riskonnect ERM is designed to bring together all the significant risks of an organisation in a way that enables the organisation to most effectively manage those risks. Riskonnect's Vendor Risk Management solutions provide the ability identify the risks every vendor introduces with each engagement with an organisation and monitor them. The Business Continuity Management solutions allow for a consistent global approach with automatic updates to source data if contact details change and efficient single storage place for all data. Riskonnect Healthcare solutions enable the handling of healthcare risk management, quality of care, patient safety, and employee management.

riskonnect.com

RISKSOLVED
RISKSOLVED

This cloud-based risk management solution is designed to help insurers, brokers and MGAs actively manage their exposure to policyholders' risks. The solution consists of portals for every member of the insurance value chain, from policyholder to broker to insurer, allowing collaboration over identification of risks across all classes of insurance, automatically identifying how to mitigate those risks and reduce the costs of risk transfer. This product is designed to mimic physical building risk assessments but eliminate the need for expensive visits to site, by leveraging big data supplemented with self-assessments by local site managers.

risksolved.com

RISKWARE
PAN SOFTWARE

Riskware supports AS/NZS/ISO 31000: 2009 to break down silos by integrating all areas of risk to provide a true picture of enterprise risk and performance in a user-friendly single consolidated environment.

riskware.com.au

SCAIR
INTERSYS

This tool is enables manufacturing companies to quantify financial losses resulting from supply chain failures by visualising their end-to-end supply chains; data which can then be used to formulate continuity plans. SCAIR quantifies the accumulated exposure of a company's portfolio of products to each critical supply point, based on existing internal planning information and profit predictions. An intuitive flowchart-driven interface allows users to map critical supply points and estimate exposures. The solution is currently used by three of the top twelve global biopharmaceutical companies, addressing the specific requirements of that industry including accurate modelling of specific supply chain characteristics (diverse geography, multiple production stages, major stock holdings at various points in supply chains). New modules include natural catastrophe event alerts and medical regulatory reporting.

supplychain-risk.com

STREAM INTEGRATED RISK MANAGER
ACUITY RISK MANAGEMENT

This solution brings together all of the data required to understand cyber risk status in the context of threats to business outcomes. Aggregation and correlation features allow users to make informed decisions on the need for action, complying with regulations and standards such as GDPR, ISO 27001 and PCI-DSS while reducing the risk of breaches. In the event of a breach STREAM provides evidence of a diligent risk-based approach to minimise the impact of fines, reputational damage and legal costs. Additional regulations and frameworks, such as those for specific industry sectors can be quickly and easily added either by Acuity or by the user. Key features of STREAM include risk-based compliance, risk acceptance, risk reporting, alerting and workflow, threat and vulnerability management as well as incident management and auditing. Remediation workflow and reporting allows progress to be monitored and the product's Risk Delta functionality provides business risk-based prioritisation for improvement programmes.

Vulnerability scans, penetration test results and control metrics can be imported from external data sources, such as scanning and monitoring systems, and used to update the business risk and compliance status in real-time as well as monitoring and reporting on key indicator performance and trends.

Through the use of real-time dashboards and workflow functionality, this solution aims to ensure that vulnerabilities are alerted to appropriate technical staff quickly, so as to allow for efficient remediation.

acuityrm.com

SYNERGI LIFE
DNV GL

Synergi Life is a comprehensive risk, quality, EHS and operational integrity management solution. It is used by more than 400 companies worldwide, with 800,000 users globally across a number of industries, including energy, healthcare, transport, local government and construction.

The application is translated into more than 25 languages and aims to provide users with all the information they need to prevent unacceptable risks, share lessons they have learned, and manage corrective measures and actions.

The application provides companies with the ability to share and roll-up data across complex, multi-layered organisations, allowing them to recognise trends and ensure compliance with requirements. This is a module-based solution designed to meet the demands from both reactive indicators and proactive initiatives.

These modules can be used as standalone solutions or in combination of several modules that contribute to a total risk and QHSE management solution.

dnvgl.com/synergilife

THESIS BOWTIE
ABS GROUP

THESIS was designed as a cost-effective and reliable way of assessing the diverse risks facing an organisation. This software integrates with risk management to promote safety, reliability and business continuity across the enterprise. Developed to assist risk managers and stakeholders in their decision making process, THESIS delivers a simplified and comprehensive risk management solution for mapping threats, risk events and consequences at all levels of an organisation – from the front-end engineering design stage through to operations and decommissioning.

abs-group.com

WEBRISK
VENTIV TECHNOLOGY

Acquired by Ventiv Technology from Effisoft in October 2017, Webrisk was designed to help risk and insurance managers manage their daily operations more effectively. The solution allows users to perform the necessary analysis and simulations to optimise insurance and risk management programmes.

Webrisk clients use the product to gather, consolidate and analyse insurance renewal information; control and manage policy portfolio; automate the implementation of survey recommendations and handle incidents and claims, create dynamic risk registers and manage risk programmes.

A full hosted solution, this product is updated regularly to provide reporting and analysis tools and mobile integration. It is also offered on an unlimited user basis, encouraging as broad a use of the system as possible.

ventivtech.com

XACTIUM
XACTIUM

Xactium is a cloud-based GRC software provider that aims to help risk managers transform the way that organisations evaluate and manage their enterprise and project risk. As the central risk platform used by the FCA to supervise the market, it has also been adopted by a wide range of financial services organisations from across the industry.

xactium.com

Risk Software Report 2018 – Product features

	Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Magique Galileo	Marsh ClearSight	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium
General/admin/tech																												
Full process analysis hierarchy	•	•		•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•
Full process escalation hierarchy	•	•		•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Objectives hierarchy	•	•	•	•	•	•		•		•	•	•		•	•	•	•	•	•	•		•		•	•	•	•	•
Organisational hierarchy	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Asset hierarchy	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
Financial accounts hierarchy	•			•		•					•			•	•		•	•		•					•	•	•	
Expand and collapse hierarchy	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•		•		•	•	•	•	•
Audit findings	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Scalable and tested to 100 users	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•
Scalable and tested to 1,000 users	•		•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•
Scalable and tested to 10,000 users	•	•			•						•	•	•	•	•	•	•	•	•	•	•	•			•	•	•	•
Context sensitive help	•	•		•	•	•		•	•	•	•	•	•	•	•	•	•	•		•	•	•	•		•	•	•	•
Screen customisation	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Search and filter	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Roll-forward capability	•	•	•		•	•			•	•	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•
Multi currency	•	•	•	•	•		•					•	•	•	•	•	•	•	•	•			•	•	•		•	•
Multi language	•		•	•	•							•	•	•	•	•	•	•	•	•	•			•	•		•	•
Web application	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•
Web service API	•		•	•	•		•			•	•		•	•	•	•		•		•	•	•			•		•	•
Synchronisation with active directory	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Integration with MS Office	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Integration with enterprise reporting systems	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Integration with collaboration tools	•		•	•	•		•	•	•	•	•	•	•	•	•	•	•			•	•	•		•	•	•	•	•
Ability to install software on users own IT infrastructure	•	•	•	•		•	•	•	•	•	•	•	•	•		•	•		•			•	•	•	•	•		
Support for offline working and synchronisation	•	•	•		•					•			•	•	•	•	•	•	•	•	•	•			•	•		
Hosted option / SaaS	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	
Mobile capability: Add / update claims	•			•	•				•		•		•		•			•		•					•		•	•
Mobile capability: Manage tasks / activities	•		•	•	•	•		•	•		•		•	•	•	•	•	•		•	•	•		•	•		•	•
Mobile capability: View reports / dashboards	•		•	•	•			•	•		•	•	•	•	•	•	•	•		•	•	•		•	•		•	•
User security clearance	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Technical support / service desk 24/7	•	•	•	•	•	•	•				•	•	•	•		•	•	•	•	•			•		•	•	•	•
Data management	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Load historic data	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Consolidating data from external sources	•			•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•
COPE data management	•			•	•						•		•		•			•		•				•	•		•	
Deliver secure content	•		•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Integrated document scanning	•													•	•			•		•							•	
Integrated electronic signature	•													•	•			•		•					•		•	
Social Collaboration & Networking	•		•	•	•		•						•	•	•		•	•		•		•			•		•	•
Compatable with All Web Browsers without plug ins	•	•		•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•
Fully accessible via smartphone / tablet	•			•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•
Major functional areas																												
Incident reporting	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
Claims	•			•					•				•	•	•			•		•		•			•		•	

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

Risk Software Report 2018 – Product features

Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Magique Galileo	Marsh ClearSight	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium	
																												Major functional areas
•			•	•	•					•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•		Occurrence
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Standard reports
•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	Business Intelligence reports
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Dashboard
•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	Location / Assets
•			•	•				•				•		•			•		•	•				•	•	•		Fleet
•	•	•	•	•	•	•			•	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	Internal audit
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Assessment
•	•	•	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	Recommendations
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Documents
•	•	•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•		•	•	•	•	•	Project
			•					•				•		•			•		•					•	•	•		Premium calculation and allocations
•		•	•					•	•	•	•	•		•			•	•	•	•	•			•	•	•	•	Policy
			•			•		•				•		•			•		•	•		•		•	•	•		Renewal data collection
•			•					•	•			•		•			•	•	•	•		•		•	•	•		Insurer
•			•	•		•			•			•		•	•		•		•	•	•	•	•	•	•	•	•	Contacts
•			•	•										•	•		•		•	•				•				Track and service recommendations -property and real estate
•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•		•	•	•		•	•	•	•	•	Health and safety hazards
•	•	•	•	•	•		•		•	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	Governance, risk and compliance
		•		•						•			•	•		•	•		•		•	•	•	•				BIA
				•						•			•				•		•			•	•	•				SCM
•				•						•		•	•	•	•		•		•			•	•	•	•			Vendor management
																												Risk Identification
•	•	•	•	•					•	•			•			•			•	•	•	•	•	•	•	•	•	BCM Knowledge base
•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Issues, losses and risks
•		•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	Custom IDs
•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Risk quantification
•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Risk comments
•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Linked documents
•	•		•	•	•		•			•	•	•	•	•		•	•		•	•	•		•	•	•	•	•	Loss and accident identification
•	•		•	•	•		•		•	•	•		•		•	•	•		•	•	•	•	•	•	•	•	•	Linking losses to risk
•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Multiple risk types
•	•		•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Risk linkage
•	•	•	•	•	•	•	•		•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Risk review process
•	•	•	•	•			•		•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	Risk approval
•	•		•	•		•			•	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•		Risk surveys
•	•	•	•	•		•			•	•	•	•	•	•		•	•	•	•	•	•		•	•		•		Control surveys
																												Risk Assessment
•	•	•	•	•	•	•	•		•	•	•		•	•	•	•	•	•	•		•		•	•	•	•	•	Risk matrix
•	•	•	•	•	•	•	•		•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	Qualitative assessment
•	•	•	•	•	•	•	•		•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Quantitative assessment
•	•	•	•	•	•	•	•		•	•	•		•		•	•	•	•	•	•	•		•	•	•	•	•	Gross, Residual, Target
•	•	•	•	•			•			•	•		•		•	•	•	•	•	•	•		•	•	•	•	•	Opportunity

Risk Software Report 2018 – Product features

	Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Marsh ClearSight	Magique Galileo	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium
Risk Assessment																												
Frequency	•	•	•	•	•			•		•	•		•	•			•	•	•	•	•	•		•	•	•	•	•
Financial years modelling	•			•		•							•	•			•	•	•	•	•		•		•	•	•	
Multiple risk impacts for single risks	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•
ROI	•			•				•	•	•	•					•	•	•	•		•	•		•	•	•	•	
Escalation	•	•		•	•	•		•		•	•	•	•	•		•	•	•	•	•	•	•		•	•	•	•	•
Risk aggregation	•	•	•	•	•	•		•		•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•
Relationship matrices	•	•		•	•			•			•	•	•	•		•	•	•	•	•	•	•	•	•	•		•	

	Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Marsh ClearSight	Magique Galileo	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium
Risk mitigation																												
Control assessment - qualitative and quantitative	•	•	•	•	•	•	•	•		•	•		•		•	•	•	•		•	•	•	•	•	•	•	•	•
Testing	•	•	•	•	•	•				•	•		•	•	•		•	•		•	•	•		•	•	•	•	•
Actions	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Fallback	•			•	•	•				•			•	•		•	•	•	•	•		•	•	•		•	•	•
Plan	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
Provision management	•				•						•					•		•	•						•	•	•	
Plans linked to multiple risks	•	•		•	•	•		•		•	•		•	•	•	•	•	•		•	•	•	•	•	•	•	•	
Linked actions to multiple plans	•	•		•	•	•		•		•	•		•	•	•	•	•	•		•	•	•	•	•	•	•	•	
Compliance auditing	•	•		•	•	•	•	•		•	•	•	•	•	•		•	•		•	•			•	•	•	•	•
Certificate management - medical trials				•							•	•			•			•		•					•		•	
Certification for projects											•	•	•				•	•		•					•		•	

	Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Marsh ClearSight	Magique Galileo	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium
Analysis & Reporting																												
Multiple application reporting	•	•	•	•	•	•				•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Probability vs. impact impact diagram	•	•		•	•		•	•		•	•		•	•	•	•	•	•	•	•		•			•	•	•	•
Monte Carlo simulation	•	•												•		•	•		•			•						•
Sensitivity analysis	•				•									•		•	•		•			•				•	•	
Provision management	•				•						•					•		•	•						•	•	•	
Schedules reporting	•			•	•						•	•	•		•	•	•	•	•	•	•	•		•	•	•	•	
Data driven reporting	•	•		•	•		•		•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Ad hoc reporting	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Automated email report distribution	•	•		•	•	•				•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•
Risk adjusted balanced score cards	•				•							•	•	•	•	•				•	•	•		•	•	•	•	•
Risk adjusted GANT chart	•										•	•	•	•		•		•	•								•	
Bayesian analysis														•		•											•	
User-defined dashboards	•	•	•		•	•		•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Integration with business intelligence reporting tools	•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Automatic alerts	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•
Ability to combine data from all modules within a single report	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	• •
Ability to combine data from all modules within a single dashboard	•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•		•	•	•		•	•	•	•	•
Ability to meet user reporting needs without the need from custom reports	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•
Integration with geospatial analytics	•		•	•	•		•		•		•	•	•		•			•		•	•	•	•				•	•

	Active Risk Manager	BarnOwl	Exonaut	Figtree Systems	Fusion Framework Continuity Risk Management System	GuardianERM	HawkSight Software	JCAD CORE	JCAD LACHS	KnowRisk	Maclear eGRC Sute	Magique Galileo	Marsh ClearSight	Metric Stream	Origami Risk	Predict!	Quantate	RiskConsole Advanced	riskHive Enterprise Risk Manager	Riskonnect	Risk Solved	RiskWare	SCAIR	STREAM Integrated Risk Manager	Synergi Life	THESIS BowTie	Webrisk	Xactium
Analysis & Reporting																												
Automatic alerts based on the proximity and severity of external events to locations			•	•	•		•					•	•		•			•		•		•	•		•		•	•
Mapping capabilities			•	•	•		•		•		•	•	•	•	•			•	•	•		•	•	•	•	•	•	•
Drill up / down / through reporting	•	•	•		•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Download to Word	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•			•	•	•	
Download to Powerpoint	•				•					•	•	•	•	•	•	•		•		•					•	•	•	
Export to Excel	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Incident management																												
Web-based incident reporting	•	•	•	•	•	•	•	•	•		•	•	•	•	•		•	•		•		•	•		•		•	•
Convert incidents to claims	•		•	•					•			•	•	•	•			•		•		•			•		•	
Forward and automatically attach emails to the system				•					•				•		•			•		•					•		•	•
Automated incident investigation and escalation	•		•	•	•					•	•	•	•	•	•		•	•		•		•		•	•		•	
Data conversion and consolidation services				•					•				•		•			•		•					•		•	
Anonymous / third party incident reporting	•		•	•			•			•	•	•	•	•	•			•		•					•		•	
Claims management																												
Full claims administration				•									•		•			•		•		•			•		•	
Dashboards for tracking claims metrics and KPIs	•			•					•				•		•			•		•		•			•		•	
RIDDOR / CRU1 Reporting	•			•									•		•			•		•					•		•	
External claims benchmarking													•		•					•					•		•	
Forward and automatically attach emails to the system				•					•				•		•			•		•					•		•	
Data conversion and consolidation services				•					•				•		•			•		•					•		•	
Managing financials through programme structure				•					•				•		•			•		•							•	
Claim audits				•					•				•		•			•		•					•		•	
Policy and premium management & Premium allocation																												
Insurance knowledge base				•									•							•					•		•	
Policy programme functionality				•									•		•			•		•	•						•	
Policy erosion				•					•				•		•			•		•							•	
Allocation of premiums based on exposure values and loss experience				•					•						•	•				•	•							
Tracking of covered locations and perils				•	•				•				•		•			•		•			•		•		•	
Ability to report on premiums by insurer, broker or business unit															•													
Captives support				•					•				•		•			•		•	•				•		•	
Ability to report on exposure by insurer and insurer ratings				•	•				•				•		•			•		•					•		•	
Ability to map insurance programme				•					•				•		•			•		•					•		•	
Ability to diagram policy erosion									•				•		•			•		•							•	
Renewal data				•					•				•		•			•		•	•		•		•		•	
Ability to customise renewal questionnaires													•		•			•		•	•				•		•	
Automated data validation against previously submitted values				•	•				•				•		•			•		•	•		•		•		•	
Automatic reminders for unsubmitted values				•	•								•		•			•		•	•				•		•	
Predefined report templates for renewal data consolidation				•			•						•		•			•		•					•		•	

ABS Group

ABS Group
EQE House, The Beacons,
Warrington Road, Birchwood
Cheshire. WA3 6WJ. UK

Tel: +44 (0)1925 287300
www.abs-group.com/thesis
LinkedIn: https://www.linkedin.com/company/absgroup

ABS Group provides holistic enterprise risk management tools to help you identify, analyse and manage hazards. Our THESIS BowTie™ 6.3 standalone and THESIS Enterprise™ risk management software solutions help document risk analyses in a systematic manner, making the control of hazards easier to understand.

Developed to assist risk managers and stakeholders in their decision making process, THESIS delivers a simplified and comprehensive risk management solution for mapping threats, risk events and consequences at all levels of an organisation – from the front-end engineering design stage through to operations and decommissioning.

THESIS BowTie™ is a cost-effective and reliable way to assess the diverse risks facing an organisation. Our software integrates with risk management to promote safety, reliability and business continuity across the enterprise.

Using the qualitative Bowtie Method, THESIS displays the relationship among hazards, controls, risk reduction measures and business activities, helping managers communicate critical procedures and demonstrate compliance.

DNV·GL

DNV GL
Veritasveien 1, Hovik 1363, Norway

Tel: +47 67 57 99 00 - Norway
Tel: +44 (0)20 3816 4000 - UK
software@dnvgl.com
www.dnvgl.com/synergilife
linkedIn: www.linkedin.com/company/5005106

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organisations to advance the safety and sustainability of their business. With Synergi Life, DNV GL is one of the world's most recognised EH&S/QHSE and risk software providers, offering on-premise, cloud-based and mobile app solutions. Synergi Life is used by more than 350 companies worldwide, with 750,000 users globally across a number of industries, such as energy, healthcare, transport, local government, construction and more.

With Synergi Life you have the tools you need to manage QHSE (or HSE) non-conformances, incidents, risk, risk analyses, audits, assessments and improvement suggestions.

FUSION RISK MANAGEMENT

Fusion Risk Management
3 London Bridge Street – 3rd Floor
London, England SE1 9SG

Tel: +44 (0)20 3884 3538
info@fusionrm.com
fusionrm.com
Linkedin: linkedin.com/company/90668
Twitter: @FusionRiskMgmt

Fusion provides the Fusion Framework® Continuity Risk Management software and Fusion Fuel℠ Advisory Consulting services. Fusion's achievements include BCI's 2016 & 2017 Global Continuity and Resilience Provider of the Year and is a Gartner Magic Quadrant Leader four years in a row. The Fusion Framework System™ delivers integrated BIA & risk assessment, plan development & activation, crisis/incident management, exercises & simulations, integrated risk management, and mobile & enterprise communities to engage all employees for incident response, safety, and security. Fusion Framework delivers vendor risk, facility risk, IT and cyber risk, and related risk agendas. Fusion Framework integrates with leading ENS and ITSM providers, enterprise systems, and more. Learn why 4 out of 5 organizations who evaluate Fusion choose the Fusion Framework System!

JCAD

JC Applications Development Ltd
Manor Barn, Hawkley Rd, Liss,
Hampshire, GU33 6JS

Contact: Phil Walden

Tel: +44 (0)1730 172020
sales@jcad.co.uk
www.jcad.co.uk
Twitter: @jcad2

In business since 1992, JC Applications Development Ltd take great pride in our ability to develop world class software solutions and associated services that enable our clients to manage risk, compliance and claims more effectively. As a result they are better placed to achieve their corporate ambitions, save time, money and offer a superior service to their stakeholders. This is proven by our last customer satisfaction survey where 98% of respondents said that they would recommend us.

With over 200 successful implementations JCAD is a market leader in the provision of claims handling and risk management software to both the public and private sectors. Client representation covers many diverse industries including but not limited to;

- Housing associations
- Local government
- Emergency services
- Charities & NGO's
- Academia
- Finance
- Retail
- Construction
- Facilities Management
- Utilities

JCAD's software is wholly "off the shelf" which enables time efficient implementations, low cost systems and simpler training. Additionally, by offering a best practice approach to risk and compliance management we can focus on the development of new functionality that is then shared across our entire client base. JCAD are an ISO9001 accredited supplier and our hosting partners are accredited to ISO27001.

MAGIQUE GALILEO

Magique Galileo Software Ltd
Ground Floor, Birchin Court
London EC3V 9DU

Tel: +44 (0) 20 3713 4590
info@magiquegalileo.com
www.magiquegalileo.com

Easy to use fully integrated web-based system covering Risk Management, Control Testing and Attestation, Incident/Loss Event Management, Appetite Statements and Indicators / Measures, Emerging Risks, Scenario Analysis, Policy Management and Compliance, Questionnaires and Actions.

Includes extensive email alerting, reporting and analysis though Visualisation tools.

- Configured to meet your exact methodology, terminology, workflow, security and reporting
- Over 250 active clients from 5 users to over 1,000 users
- Mature product developed and enhanced over 20 years
- Every implementation led by experienced Risk Management professionals
- Highly Secure – Cyber Essentials **Plus** Certified

NTT DATA
NTT DATA Figtree Systems

NTT DATA Figtree Systems
Level 3, 2 Royal Exchange
London EC3V 3DG
United Kingdom

Tel: +44 (0)20 722 09210
Fax: +44 (0)20 728 38944
Ayaz.Merchant@nttdata.com
www.figtreesystems.com

NTT DATA Figtree Systems is a specialist software provider for Risk Management Information Systems. Catering to all claims types, our cloud platform streamlines claims administration, while enhancing risk awareness and cost control. Providing configurable workflow, flexible business rules and a full suite of Claims, Risk and Safety Management modules, our software is adaptable to variations in business processes and complexity. Used by clients globally, this award winning system features document creation and management, custom dashboards and reports, smartphone and web-based data-capture, email notifications, and enterprise system integration. Hosted in a secure datacentre, certified ISO 27001, the system delivers centralised data management, while providing remote, real-time access.

Origami Risk
Suite 406, 32 Threadneedle Street
London EC2R 8AY

Contact: Neil Scotcher

Tel: +44 (0) 7775758655
nscotcher@origamirisk.com
www.OrigamiRisk.com
Twitter: @origamirisk
Linkedin: https://www.linkedin.com/company/origami-risk

Origami Risk, the award-winning risk management Software as a Service (SaaS), provides intuitive web-based software that streamlines how risk, insurance and claims data are collected, analyzed and shared—helping users or their clients be more productive and manage the total cost of risk.

Origami's Risk Management Information System (RMIS), Enterprise Risk Management (ERM), Claims Management and Policy Management systems work together, offering speed, flexibility, automation, and robust data import/export, analysis and reporting tools. ERM solutions feature intuitive reporting and audit functions, the ability to streamline processes and drive accountability, and conformance with COSO ERM 2017 and the 2018 update of ISO 31000.

Throughout the UK, Europe and globally, Origami's clients tailor solutions to address:

- Property values collection
- Claims administration and incident intake
- Policy/program management
- Claims and safety audits
- ERM
- Captive management
- Reporting and analytics
- Asset and fleet management

Visit www.origamirisk.com or contact Origami at info@origamirisk.com.

Ventiv Technology
30 – 40 Eastcheap, London, EC3M 1HD

Contact: John Irving

Tel: +44 (0) 20 3817 7407
john.irving@ventivtech.com
www.ventivtech.com
Linkedin: www.ventivtech.com/linkedin
Twitter: @ventivtech

RiskConsole Advance
Whether you're managing risk, safety or insurance programs, your job is more challenging than ever. More data. Increased business complexity. Greater security risks. Heightened expectations. Less time to respond, and with fewer resources.

RiskConsole Advance empowers you to take control of your organisation's data and achieve the clarity you need to make fully informed decisions. Improve your efficiency and maximize scarce resources—while getting back the time you need to think and act strategically.

Fully embedded and integrated into RiskConsole Advance, Ventiv's analytics, reporting, and data-discovery platform is the market's newest, most technologically current offering. Ventiv is the only RMIS provider offering cutting-edge **IBM Watson Analytics** as an embedded, integrated component of our solution. When you add it up, RiskConsole Advance's comprehensive analytics, reporting, and data-discovery empowers you to make data-driven decisions that generate optimal outcomes like reducing claim frequency and severity.

With your processes optimized, best practices embedded and knowledge converted, you have raised your risk technology maturity level to drive better results and make your risk management department more resilient.

Ventiv Technology
30 – 40 Eastcheap, London, EC3M 1HD

Contact: David Thomas

Tel: +44 (0) 20 3817 7387
david.thomas@ventivtech.com
www.ventivtech.com
Linkedin: www.ventivtech.com/linkedin
Twitter: @ventivtech

Webrisk
Acquired by Ventiv Technology from Effisoft SAS in October 2017, Webrisk is a full-featured risk management information system that helps risk and insurance managers manage their daily operations more effectively.
With Webrisk, your daily activity is easier, more reliable and more efficient. Your communication with partners (brokers, insurers, and consultants) and subsidiaries is fluid and timely. Webrisk also allows you to perform the necessary analysis and simulations to optimise your insurance and risk management programs.

Webrisk is known for its ease of use, **as clients like Petrofac, a FTSE 250 international service provider to the oil and gas production and processing industry, attest:** "One of the many things we really like about the Webrisk system is its flexibility and ease of use. This has meant a system which meets our requirements rather than vice versa, and the result is a highly intuitive system for the end user, combined with the ability to immediately consolidate the data for reporting and analyse centrally.

What's your view? Email the editor at deborah.ritchie@cirmagazine.com

Last year was a stark reminder of some fundamental truths for risk professionals. The devastating storms in the Americas were a brutal reality check of the impact of climate change; a spate of global cyber attacks brought home the fact that cyber risk is a reality today, not a problem for the future; and the tragic fire at Grenfell Tower showed that 'traditional' threats are still as dangerous as ever. These are not new lessons; they are wake up calls. They serve as a reminder that we as risk professionals must be prepared for all risks – whether they are dominating the headlines or not; just because artificial intelligence and data analytics are current hot topics does not mean we can forget about other areas of risk.

The good news is that businesses increasingly recognise the value of risk management in addressing these challenges; its profile is higher than it has ever been – a trend that 80% of our members believe will continue throughout 2018. Insurers are also demonstrating an ability to innovate, particularly where cyber risk is concerned. Last year saw a marked improvement in products and services designed to address this progressively worrisome issue, making cyber insurance the fastest growing area of the market in terms of capacity and demand.

What we need now is greater and more effective collaboration amongst insurers, risk managers and brokers. And we think we are beginning to see signs of this. Addressing Airmic members in Autumn last year, Lloyd's chairman Bruce Carnegie-Brown said the insurance industry needed to move away from the transaction model towards a partnership model, adding that risk transfer alone is too simplistic for such threats as cyber, where the complexity of the risk requires an enterprise-wide response.

Airmic shares this view. Today's risks require a joined up approach between insurers, brokers and businesses. Insurance and risk management must be more closely aligned and integrated, and we will be working with our members and partners in 2018 to ensure the trend that began in 2017 gathers momentum in the year ahead.

John Ludlow is CEO of Airmic

In association with airmic

As 2017 drew to a close, we took some time to reflect on some of the issues we faced, and the successes we enjoyed. There were many sizeable challenges placed on the public sector throughout the course of the year, many of which have greatly affected our members.

Amongst these, the fire at Grenfell Tower and the terrorist attacks in Manchester and London are foremost in our minds. There has certainly been a lot going on – what with the Trump inauguration, a General Election, the triggering of Article 50 and some of the most powerful hurricanes ever to hit the Atlantic Basin.

Closer to home we have seen changes to the discount rate, vicarious liability extended to include local authority foster carers, changes to limitation in Scotland and the commencement of reforms to whiplash claims.

Alarm has also had a busy year, with a successful conference in Manchester in June; the delivery of a variety of events across all regions and sectors; and numerous issues of our journal, Public RM, which continues to represent members' views and features submissions to government consultations. This year also saw the relaunch of our Risk Management Toolkit (now included in membership); delivery of our Back to Basics risk management course and success in the form of a national award for our publication *Children's Services: Alarm Guide to Managing Risks*.

2018 will no doubt bring further challenges, so as we brace ourselves for GDPR and Brexit developments, we also look to the positive. The Alarm Conference is returning to Manchester on 24 to 26 June. Our speakers will be delivering presentations under the theme 'Stronger and Louder', which we hope will help empower risk professionals as they strive to tackle the many challenges that await them. The conference offers fantastic opportunities to engage and network with fellow risk professionals, and will also feature our annual gala dinner and awards. For more information on all things Alarm, please visit our website at alarm-uk.org.

Jane O'Leary is vice-chairman of Alarm

In association with alarm

Industry views

The BCI's recent study of emergency communication capabilities and preparedness shows that 40% of organisations have more than one hundred staff regularly travelling internationally; making communication in an incident extremely challenging. It also shows that 34% of those firms considered that their staff were being sent to 'high risk' countries. This made me consider what are the responsibilities of these organisations when sending employees to 'high risk' locations. Good practice suggests that the best place to start is by having an international policy that identifies what level of protection staff will be granted. The norm is to adopt the highest standard of any country in which the organisation operates; for example, if your company is global and has locations in the UK and Cambodia, the company should adopt the UK's approach to staff safety and security.

Specific country and location risks should then be identified and regularly updated as some area risk profiles change on a daily basis. If it is safe to send staff abroad, then consideration should be given to how they will travel. Local travel arrangements can be one of the most daunting risks as statistically more people die abroad from road accidents than from any other cause.

One of the often most neglected areas is the people themselves. What is their general health condition? Have they been medically screened and properly vaccinated? Have they received any pre-deployment training or been briefed on what to expect in their new working environment? Are they aware of the countries cultural sensitivities including religious differences, customs, laws, mannerisms, personal presentation so that they can avoid causing any offence?

As organisations grow and expand throughout the world they must remember the common law 'duty of care' provision that states 'an employer must take reasonable care of your safety, avoid exposing you to any unnecessary risks and ensure a safe system of work.' Two high court cases support this obligation – Palfrey v Ark Offshore Ltd and Duske & Ors v Stormharbour Securites LLP and serve to highlight the risks in this arena.

James McAlister is chairman of the Business Continuity Institute

In association with

Business Continuity Institute

Workers at British Steel have recently faced a complex choice around their pensions – whether to switch to a new scheme, stay with their old one or transfer out of the scheme and take a cash lump sum. The theory was that pension scheme members would read and digest the exhaustive amount of information provided by the scheme trustees and make a rational decision. In most cases this would be to stick with the guaranteed benefits rather than going for the lump sum, which is what far more chose – an outcome that attracted widespread criticism.

So what can risk managers learn from this? One clue comes from thoughtful analysis from the Financial Conduct Authority. It has said: "We expect firms to frame decisions for customers (their 'choice architecture') based on real world consumer behaviours and not to exploit biases. Best practice should take on board positive uses of behavioural research to help customers towards better outcomes."

Employers and pension schemes are not regulated by the FCA, but they can take on these ideas about best practice. For many British Steel workers, informal conversations with colleagues were more important than company-sponsored seminars, and a big cash payment now was more tempting than a guaranteed income paid later. These insights were already available from the science of behavioural economics, but pension trustees have been unwilling to act on them because of perceived legal risks around promoting one choice above others. But ignoring vital lessons around communication has created different, reputational risks. Eventually, firms controlling pension liabilities will be judged by the same standards that financial services firms are judged – on whether they use the most effective forms of communication to get the best outcomes. Adapting to these new expectations will mean taking more regulatory risks. Firms will have to create a 'decision architecture' that promotes a sensible outcome. In doing so, they will face the accusation of being biased, but this will be preferable to being accused of leaving members without the care and support they deserve.

Dr Matthew Connell is Director of Policy and Public Relations at the Chartered Insurance Institute

In association with

Chartered Insurance Institute

Standards. Professionalism. Trust.

What's your view? Email the editor at deborah.ritchie@cirmagazine.com

This year, global political risk continues to be one to watch, its effect on markets ongoing. Closer to home, the City of London and the wider stage is braced for Brexit along, with uncertainty and political unrest globally. Meanwhile, artificial intelligence and virtual reality are hot topics for the sector at the present and companies are investing heavily in research and software to help predict how these technological changes present both positive opportunities and risks to the business. Data breaches also feature in the top five risks for the sector along with how companies will manage the incoming General Data Protection regulations.

These, along with oil price and financial market fluctuations are among chief concerns for businesses voiced by some of the UK's leading risk experts as they look ahead to 2018.

This year, the banking and financial services sectors will be facing changes in not only the way that their products and services are regulated, but in the ways that these are delivered to customers and how the value of a customer over their lifetime is managed.

The implementation of PSD2 lays the foundation for the advancement of open banking, the potential benefits of which include improved customer experience, new revenue streams, and a sustainable service model for underserved markets. While open banking stands to have a plethora of opportunities for end-users and service providers alike, it is also likely to introduce an entirely new financial services ecosystem, in which banks' roles may shift significantly. It also requires a closer look at risks related to regulation and data privacy, which helps to explain why global markets have taken varying approaches to governance which is likely to continue into 2018 and beyond.

Organisations need to ensure that risk in the boardroom is taken seriously to ensure organisational success and longevity. It is easy to see, therefore, why enterprise risk management has never been higher on the agenda.

Nicola Crawford, CFIRM is chair of the Institute of Risk Management

In association with irm

Legal considerations of parametrics in insurance

A new study explores the benefits of parametrics in insurance, how they have been used so far and, crucially, the potential regulatory pitfalls related to their use. Deborah Ritchie takes a look at the report

Parametric triggers have been in use in the capital markets for some 20 years now; their application in insurance more recent. The legal and regulatory considerations for their use are therefore partially uncharted territory.

This was the basis for a recent study carried out by law firm Clyde & Co into the legal and regulatory considerations that arise with the growing use of parametrics across the industry. The report also explores the benefits of parametric insurance – which centre on speed, certainty and the ability to plan ahead.

Drawing on insights from the firm's global network of insurance lawyers, the study explores the growth of parametric insurance and considers the important role it has to play in building resilience to natural catastrophes. The protection gap means that in middle or low-income countries, the uninsured proportion of catastrophic losses often exceeds 90 per cent. Meanwhile, the Bank of International Settlements calculates that, particularly in developing markets, the worst natural catastrophes can – in some cases permanently – reduce a country's GDP by almost 2 per cent. In 2017, economic losses caused by natural catastrophes looked set to top US$300bn (according to data compiled by Swiss Re) compared with an average of US$178bn for the previous 10 years.

Considering some of the legal and regulatory challenges that have already arisen, or may be faced in the future, Clyde & Co's report contends that the way parametric products are treated in the law and by regulators will evolve and become clearer as case law and precedent develops. But, it suggests that with the level of support currently being given by governments around the world, together with demand from buyers and proven success of parametric insurance products to date, regulators and law makers are expected to support and encourage the responsible roll-out of parametric insurance rather than attempt to hold it back.

The paper also explores the question of basis risk; the concept of insurable interest; and the indemnity principle, which means that in theory, in certain jurisdictions, losses must be valued or assessed before claims can be paid. Many of these issues can and have been successfully addressed. Different jurisdictions' regulators and lawmakers are finding novel ways to approach parametric insurance and foster these products' development and deployment in local markets. The study goes on to consider schemes where improved modelling has been deployed to reduce basis risk, where mobile networks and satellite data are deployed to reach previously underinsured populations, or where mixed models are combining parametric and traditional indemnity solutions.

Clyde & Co partner, Nigel Brook, says these types of insurance products are developing rapidly at local, regional and national level as they provide an elegant solution for risk transfer concerns, often for populations that were previously uninsured and for whom the protection gap has traditionally been widest.

"That is why they are gaining so much attention, particularly following a year where the threat from natural disasters has been writ so large," he says. "With continued support and increased understanding, parametric insurance can fulfil its vast potential and, alongside traditional insurance and other novel forms of risk transfer, play a key part in closing the protection gap. This paper sets out to provide additional background and ballast to support the industry and other stakeholders as the development of parametric insurance continues apace."

Written by Deborah Ritchie

PROFESSIONAL SERVICES GUIDE

BUSINESS CONTINUITY SOFTWARE

ClearView BCM Software
Developed through a combination of practical experience of BCM consultants, live client feedback and technology experts, ClearView has quickly become a leader in the global BCM software market.

ClearView has removed many of the barriers that organisations experience when implementing BCM software, ensuring that ClearView delivers improvement to their BCM processes.

- Delivers ease of use for straight-forward, effective deployment and maintenance of BIA's, plans, exercises, risk and incident management. Users do not need extensive training and can pick up and use ClearView quickly and easily, even if only accessed infrequently
- Achieves a high level of modularity which means that configuration allows the solution to meet the needs of organisations precisely, but in a very cost effective manner
- Accessible from any web browser and mobile device, with mobile applications for all major platforms.
- Provides alignment to ISO22031 and Regional BCM standards
- Fully integrated Emergency Notifications and dynamic Incident Management module
- Winners of BCM Software of the Year for an unprecedented 5 years between 2012 and 2017.
- Fully ISO 27001 (information security management) and ISO 9001 accredited to provide the highest levels of security and robustness. Trusted by international private and public sector organisations
- Implemented by consultants with many years BC experience so we understand exactly what you want and can offer professional help. Much more than a software service
- Backed up with global support for clients in all sectors and all sizes
- Comprehensive reporting and dashboard analysis plus a custom report builder and integrated What If?/GIS capability for scenario mapping

ClearView – we make the complicated simple.

clearview
Making the Complicated Simple
CIR BUSINESS CONTINUITY AWARDS
WINNER 2012/2013/2014/2015/2017
BUSINESS CONTINUITY MANAGEMENT PLANNING SOFTWARE OF THE YEAR

ClearView Continuity
Astral House
Granville Way
Bicester
Oxfordshire
OX26 4JT

Tel: +44 (0)1869 354230
www.clearview-continuity.com

Daisy Shadow-Planner enables you to plan, develop, test and execute more streamlined and structured Business Continuity. Taking the pain out of the entire process, Shadow-Planner helps your people work smarter and faster and enables your business to deliver against its BC commitments more quickly, efficiently and cost effectively.

Designed by BC specialists, this suite of integrated software supports the entire Business Continuity Management (BCM) lifecycle: from impact analysis through developing plans to testing and reporting. Daisy supports you every step of the way, helping you create the strongest and most effective plans to minimise downtime and ensure you can work 'business as usual'.

Shadow-Planner is based on four core modules:
• Business Impact Analysis (BIA)
• Business Continuity Planning
• Notification
• Mobile Plans
Organisations in the financial services sector, public sector and others in regulated industries have used Shadow-Planner to help comply with business continuity standards such as ISO 22301 and other specific codes of practice.

How you benefit
A low-cost solution, requiring no local cap ex or hardware investments, you can:
• Get rid of inefficient, inaccurate and risky manual approaches - Word documents and spreadsheets
• Ensure all essential data (plans, contacts, documentation and more) are in a single secure location, at your fingertips
• Be assured that all data is regularly reviewed, updated and consistent
• Achieve faster ISO 22301 BC certification

Shadow Planner
BCM Software

Contact Daisy to find out more about the unique benefits of Shadow-Planner:
Call +44 (0)344 863 3000
Email enquiry.dcs@daisygroup.com
https://daisygroup.com/campaign-shadow-planner

daisy.

BUSINESS CONTINUITY SOFTWARE

Premier Continuum
1010, Sherbrooke West, #800, Montreal
(Quebec), H3A 2R7, Canada

Tel: +1.514.761.6222
Toll-Free: +1.877.761.6222
info@premiercontinuum.com
www.premiercontinuum.com
Twitter: @1continuum

ParaSolution is a web solution simplifying and managing Business Continuity, Disaster Recovery, Risk Management and Emergency Management over the last 15 years. ParaSolution is proven in large and small organizations including the financial sector, manufacturing and governmental agencies. With always the client at the heart of our considerations, here are key features:

- EASY TO USE, thanks to its re-engineered user interface and automated workflows sending reminders.
- EFFICIENT, since information captured in the BIA is automatically available in other steps of the lifecycle and connected to a centralized and integrated database including stakeholders contact information.
- MULTILINGUAL, the solution communicates with users in their preferred language (interface and notifications).
- ParaSolution comes with standardized templates, based on industry best practices such as ISO 22301 and BCI Good Practices, while allowing EXTENSIVE CUSTOMIZATION to suit your organization's needs.
- MEASURE compliance to ISO 22301 using integrated ICOR self-assessment tool and obtain guidance in progression.
- ParaSolution SaaS is highly available, hosted on secured and audited servers and can also be hosted by your organization.

Premier Continuum Inc., proud developer of ParaSolution, is a training partner of the BCI and of ICOR and a consulting firm with hands-on experience, celebrating its 20th anniversary.

UK & European Head Office
Unit B Heathrow Corporate Park,
Green Lane, Hounslow,
Middlesex
TW4 6ER

Tel: + 44 (0) 800 143 413
infoavail@sungardas.com
www.sungardas.co.uk

US & RoW
680 East Swedesford Road
Wayne, PA 19087 USA

Toll-Free: 1 800-478-7645
Local (US): 1 610-878-2644
Email: AS.SoftwareSupport@sungard.com
www.sungardas.com

Sungard AS Business Continuity Management Planning Software

Assurance^{CM}

Brand new to this edition of the report is **Assurance^{CM}** which was designed by users, for users. This next-generation business continuity software and risk management solution removes the barriers to organisation-wide engagement and builds greater confidence in contingency plans. It's about extending beyond simply addressing compliance requirements. It's also about knowing teams are prepared to recognise threats to the business and empowering them to engage locally before incidents lead to major disruptions.

So far our users rate the **Assurance^{CM}** experience as:

Intuitive – Simple and easy, get your program up and running with minimal training
Aware – Merge external happenings with enterprise plans and gain real-time contextual insight to act decisively
Alive – Eliminate manual data management and trust that your data is accurate and up-to-date
Efficient – Yet secure to help you work smart, engage users and delight stakeholders on program effectiveness
Independent – SaaS and mobile, connect quickly to people and information that matters the most

And a 100% SLA availability guarantee.

Plans and testing do not deliver outcomes, people do. **Sungard AS Assurance^{CM}** is about enabling you to take what we learn back into the business continuity/disaster recovery planning cycle and share it across the company for better outcomes.

ASSURANCE^{NM} (NOTIFICATION MANAGER)

Introducing our new powerful emergency notification tool, designed for when you need it most to ensure the effect send of critical alerts to your key recipients at any time, using any device, and get the response you need.

Assurance^{NM} Alerting and Mobile Services from Sungard Availability Services (powered by Send Word Now®) leverages a variety of communication methods to transmit tens of thousands of voice and text messages in minutes. The Assurance^{NM} communication solution is built on an award winning platform that is used by both public and private sector organisations worldwide, offering them market leading capabilities and superior performance which Sungard AS customers can rely on. For more information please contact Sungard AS:

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

For more information:
Call +44 (0) 344 863 3000
Enquiry.dcs@daisygroup.com
www.businesscontinuitytransport.com

Daisy has become the UK's go to partner for resilient, secure and always available communications and IT infrastructure managed services.

As the UK's business continuity industry leader with over 25 years' experience, Daisy is embedding resilience into its entire service portfolio, focussed on enabling today's digital business in the key areas of always-on infrastructure, connect & protect and agile workforce.

Business Continuity Management:
Daisy's BCM consultants and Shadow-Planner software work with you to deliver digital business resilience and address the new risks of the digital economy. We advise, deliver, support and manage all or part of your business continuity management, including emergency response planning; crisis and reputational risk management; operational and business recovery planning; infrastructure process and IT risk analysis; supply chain risk management; authentic exercising, maintenance and awareness.

Workplace and FlexPlace Recovery:
Daisy has got your offices and your people covered from 18 specialist business continuity centres available UK-wide, mobile and virtual office solutions delivered to the home and complex call centre and financial trading positions. We usually have customers up and running within an hour and not just for business interruptions, but to cope with peak or seasonal trading and the flexibility digital businesses now demand.

ITDR, FlexTech and Data Availability:
Daisy's flexible IT and data recovery services will protect your technology, data and communications, available when the need arises and for test and development scenarios. We have nine resilient UK data centres and an award-winning portfolio of data availability services, applauded by industry analysts. For replacement IT onsite fast, we have over 1,000 servers and seven ship-to-site, mobile data centre units, all ready to dispatch if disaster strikes. This can be a safe roll-back recovery option in the event of cyberattack.

BUSINESS CONTINUITY, LOGISTICS

CMAC Business Continuity Transport
The Globe Centre, St James Square,
Accrington, Lancashire BB4 0RE

Contact: Ashley Seed

Tel: +44 (0) 1254 355 126
bctenquiries@cmacgroup.co.uk
www.businesscontinuitytransport.com
Twitter: https://twitter.com/CMACgroupUK
Linkedin: https://www.linkedin.com/company/10540515/

CMAC Business Continuity Transport makes moving your people safely, simple. We believe that everyone should be moved safely, whether it is in an emergency or as a planned exercise. We want everyone to feel secure in the knowledge that if they can no longer work at their usual location, they will be safely moved, just by making one phone call to our 24/7/365 call centre. We were established in 2007 and have become the UK's leading dedicated provider of business continuity transport.

CLAIMS HANDLING & RISK MANAGEMENT SOFTWARE SOLUTIONS

JC Applications Development Ltd
Manor Barn, Hawkley Rd, Liss,
Hampshire, GU33 6JS

Contact: Phil Walden

Tel: +44 (0)1730 172020
sales@jcad.co.uk
www.jcad.co.uk
Twitter: @jcad2

In business since 1992, JC Applications Development Ltd take great pride in our ability to develop world class software solutions and associated services that enable our clients to manage risk, compliance and claims more effectively. As a result they are better placed to achieve their corporate ambitions, save time, money and offer a superior service to their stakeholders. This is proven by our last customer satisfaction survey where 98% of respondents said that they would recommend us.

With over 200 successful implementations JCAD is a market leader in the provision of claims handling and risk management software to both the public and private sectors. Client representation covers many diverse industries including but not limited to;

- Housing associations
- Local government
- Emergency services
- Charities & NGO's
- Academia
- Finance
- Retail
- Construction
- Facilities Management
- Utilities

JCAD's software is wholly "off the shelf " which enables time efficient implementations, low cost systems and simpler training. Additionally, by offering a best practice approach to risk and compliance management we can focus on the development of new functionality that is then shared across our entire client base. JCAD are an ISO9001 accredited supplier and our hosting partners are accredited to ISO27001.

CLAIMS HANDLING & RISK MANAGEMENT SOFTWARE SOLUTIONS

Ventiv Technology
30 – 40 Eastcheap, London, EC3M 1HD

Contact: John Irving

Tel: +44 (0) 20 3817 7407
john.irving@ventivtech.com
www.ventivtech.com
Linkedin: www.ventivtech.com/linkedin
Twitter: @ventivtech

RiskConsole Advance
Whether you're managing risk, safety or insurance programs, your job is more challenging than ever. More data. Increased business complexity. Greater security risks. Heightened expectations. Less time to respond, and with fewer resources.

RiskConsole Advance empowers you to take control of your organisation's data and achieve the clarity you need to make fully informed decisions. Improve your efficiency and maximize scarce resources—while getting back the time you need to think and act strategically.

Fully embedded and integrated into RiskConsole Advance, Ventiv's analytics, reporting, and data-discovery platform is the market's newest, most technologically current offering. Ventiv is the only RMIS provider offering cutting-edge **IBM Watson Analytics** as an embedded, integrated component of our solution. When you add it up, RiskConsole Advance's comprehensive analytics, reporting, and data-discovery empowers you to make data-driven decisions that generate optimal outcomes like reducing claim frequency and severity.

With your processes optimized, best practices embedded and knowledge converted, you have raised your risk technology maturity level to drive better results and make your risk management department more resilient.

WORK AREA RECOVERY

Fortress

Fortress Availability Services Limited
City Reach, 5 Greenwich View,
London, E14 9NN

Tel: +44 (0)20 3858 0099
info@fortressas.com
www.fortressas.com
Twitter: @fortressas
LinkedIn: https://www.linkedin.com/company/fortress-availability-services-limited

Fortress is London's first independent work area recovery centre provider in over a decade.

We provide modern, flexible and more relevant work area recovery services to London and around the world.

Our modern facilities provide a bright and current environment designed for agile and collaborative working. The aim is to provide a replica of a modern office, somewhere comfortable and familiar where your staff feel happy to carry on business as usual.

We always support your recovery, in test and in invocation, in person and onsite with our highly experienced recovery technicians. We also give you control over your recovery environment and that gives you faster recovery.

Fortress values our customers and we will always deliver local, high touch, service led interactions from both a commercial and technical perspective.

So please get in touch and we will be pleased to explain how we are different and how we can help you provide your organisation a more modern and relevant solution to their work area recovery needs.