Book review
Inspiration for risk professionals

News & analysis
A round-up of the latest industry news and views

The interview
Nigel Brook on the COP 28 agenda

cirmagazine.com

Q4/2023

CIR
CONTINUITY INSURANCE & RISK

Focus Feature with QBE Europe *Mitigating the risks around the use and storage of lithium-ion batteries*

Building safety *We take a look at the ongoing issue of building safety of multiple-occupancy residential buildings*

Business Continuity Software Report 2024 *Your guide to the latest developments in the business continuity software market*

Pastures new

Finding synergies in climate and supply chain goals

View: "Many organisations operate under the illusion that their governance works"

Comment

We are living in a multipolar world of economic inter-connection and geopolitical fragmentation – one in which, for the past few years, businesses have faced a high level of crisis complexity, and 2024 looks set to be no different.

From the strained relationship between the US and China, and Russia's invasion of Ukraine, to, more recently, conflict in the Middle East, geopolitical tension threatens international co-operation on many of the most pressing issues of the day, exacerbating an already overwhelming array of risks.

In its annual forecast of business threats, Control Risks cites geopolitical competition and localisation as two of the major trends anticipated to shape global business in 2024, as the former forces capital to take sides; and the latter demands that companies change the way they do business.

The group refers to this dynamic, which is laden with both risk and opportunity, as 'the great realignment'.

Companies that get ahead of this geopolitical realignment will be the most resilient to shocks, wars and unrest, according to the forecast, whilst those that find a way to localise their operations will be more successful, as well as more compliant – a trend that chief executive officer of Control Risks, Nick Allan, notes has been building for some time. "Sweeping global narratives are often less use than granular, local understanding," he explains. "Localisation is the currency of the great realignment."

In addition to this dual trend, climate disruption, threats to digital integrity, and a general 'crisis overload' are anticipated by Allan to test the resilience of risk management functions at a new level as we move through 2024.

The disruption brought about by climate change will be the principal threat multiplier in the coming year, as climate events lead chiefly to supply chain disruptions and migration, exacerbating conflict, political instability and economic protectionism in their wake.

As world leaders convene in Dubai for COP 28, the climate crisis message is louder and clearer than ever before.

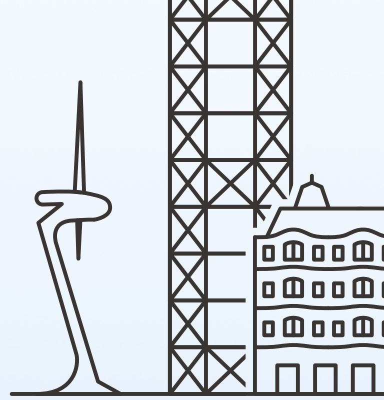
"According to the UN, the past eight years were the warmest ever recorded globally, and evidence suggests that 2024 will be no different," Allan states. "This makes the confluence of simultaneous weather developments around the world increasingly likely, with the potential to dramatically impact the business environment. Operational risk levels will be higher than ever. The need for many businesses to catch up on their climate adaptation needs has never been more pressing."

Rounding out its top risks for the coming year, Control Risks highlights the wide-ranging series of threats associated with artificial intelligence. The group portends cyber attacks enabled by, and targeting, AI systems, a reduction in human intervention in the digital ecosystem, and complexity resulting from regulatory developments across the AI sphere worldwide.

All in all, it's a less than cheery outlook for risk management professionals, as the feedback loop between drivers of disruption and the disruption they cause intensifies, as economic pressure and extreme weather events feed into more disruptive elections, state fragility, conflict, mutating cyber, digital and physical risks, geopolitical realignment and mushrooming regulation.

Risk management functions everywhere will be under extreme pressure to perform in the face of increased expectations from boards, customers and colleagues. This will be harder still for those facing cost-cutting exercises at just the wrong time.

Deborah Ritchie is editor of CIR Magazine



PERSPECTIVE PUBLISHING

PPA Publisher Member

recycle
When you have finished with this magazine please recycle it.

Editorial & features

News, views & regulars

CIR
CONTINUITY INSURANCE & RISK

Group 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

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

Subscriptions
To subscribe please complete the registration form online, by going to www.cirmagazine.com and clicking on a story (form will pop up).

CIR Magazine is published by:

Perspective Publishing Ltd
5 Maidstone Buildings Mews
London
SE1 1GN
England

ISSN 1479-862X
cirmagazine.com


BIGGER PICTURE.
BETTER DECISIONS.
Getting a full and complete picture of risk can transform the decisions your organisation makes. Data siloed in spreadsheets or different systems makes that difficult, if not impossible. Origami Risk delivers innovative risk management, insurance, and safety solutions from a single cloud-based platform that breaks down data silos and helps you see beneath the surface.
ORIGAMI RISK
© 2023 Origami Risk
ORIGAMIRISK.CO.UK

Economic and societal threats top list of worries in G20

Heightened economic risks dominate G20 business leaders' near-term concerns, according to the latest analysis from the World Economic Forum. CIR takes a look at the headline findings

Economic downturn, inflation and an erosion of social cohesion rank amongst the biggest risks for G20 countries over the next two years, according to a World Economic Forum survey of business leaders.

The *Executive Opinion Survey* gathered the views of more than 11,000 leaders from over 110 countries between April and August 2023.

This year's survey highlights how, even prior to the current conflict in the Middle East, increasingly intertwined economic and societal risks were perceived as the most significant concerns for the Group of Twenty (excluding Russia and China) against a backdrop of escalating global political tensions and persistent inflationary environments.

Economic downturn was the most commonly cited risk by business leaders this year – being identified as the top risk by 13 members of the group.

Inflation, labour and/or talent shortages, energy supply shortages and an erosion of social cohesion and well-being were also tagged among the top five risks in the near-term.

Following a year of record-breaking global temperatures and severe weather-related events, environmental risks were, somewhat surprisingly, outweighed by other concerns in this year's results, the WEF said, and, in a continuation of last year's findings, were cited just eight times in this year's top five risks. Extreme weather events were the only environmental risk to make the top 10 this year across all of the high income, upper middle income, lower middle income and low income country groups.

"Businesses may feel they have little control over existential threats such as climate change. However, it is critical for companies to explore ways to mitigate these risks while at the same time responding to the immediate challenges"

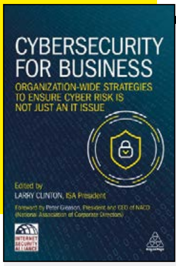
This year, the report's authors highlight a striking prevalence of common concerns amongst advanced economies and emerging markets, as economic downturn was ranked as the top risk across all regions.

Technological risks, meanwhile, including threats relating to artificial intelligence, appear only three times in the top five rankings.

Commenting on the findings, Peter Giger, group chief risk officer, Zurich Insurance Group, said: "Short-term risks such as economic and labour market-related ones dominate the global agenda today. It is important for companies to respond to these challenges keeping a balanced perspective on short and longer-term risks. Businesses may feel they have little control over existential threats such as climate change. However, it is critical for companies to explore ways to mitigate these risks while at the same time responding to the immediate challenges.

Carolina Klint, chief commercial officer, Europe, Marsh McLennan, added: "Acute economic and societal risks continue to worry G20 business leaders in the near term. While rightly addressing these immediate concerns, they should also remain mindful that, by overlooking significant technological risks, they could leave their organisations vulnerable to increasingly sophisticated cyber and AI-related threats which may profoundly affect their prosperity and the communities in which they are based."

Inspiration for resilience professionals



Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue

By Larry Clinton
Kogan Page, 2022
koganpage.com

This is not just another cyber security book. This is a cyber security book that recognises that cyber security is not only a technology issue, but a strategy and leadership issue, too.

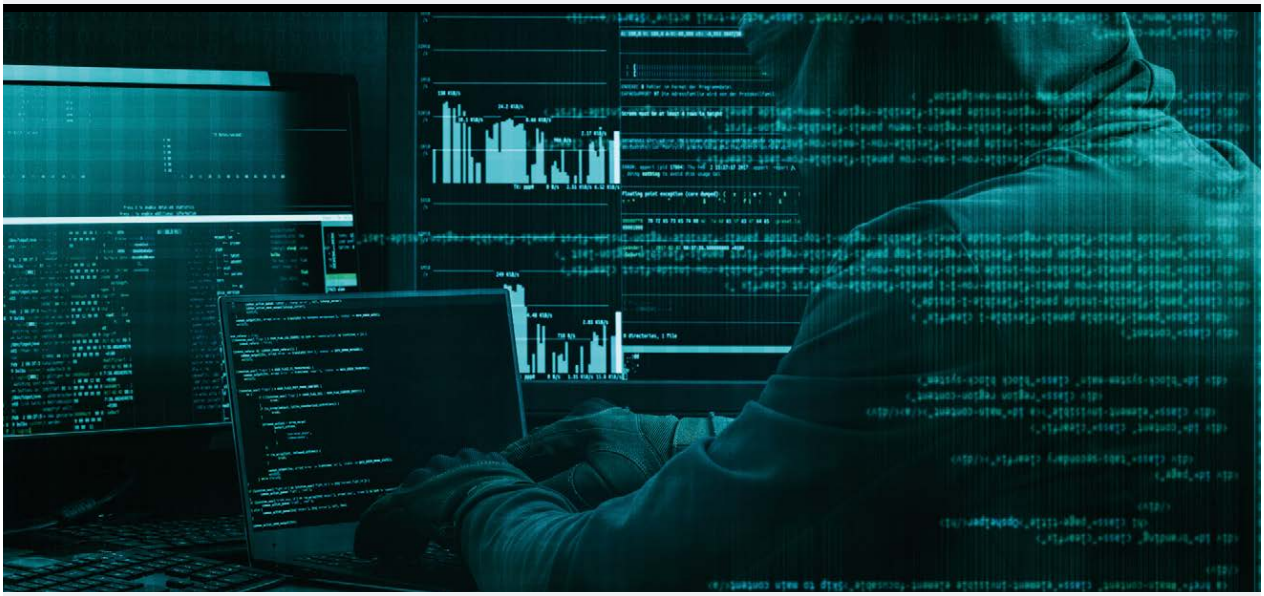
As the management of cyber risks evolves – and regulatory expectations increase – the approach taken in *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue* will be of great value to companies looking to achieve digital transformation goals without creating undue risk, helping readers to contextualise the risk in terms of financial and operational outcomes.

Author Larry Clinton is president of the Internet Security Alliance. He advises industry and government on cyber policy, and has briefed NATO and the US Congress. Twice named in the NACD 'Directorship 100' list of the most influential individuals in corporate governance, Clinton has played a key role in advancing the practice of cyber security, which, as former United States Army general, Keith Brian Alexander notes in his praise for the book, is a matter of national security: "The only way to effectively protect ourselves is through a collective defence model. *Cybersecurity for Business* describes the roles and responsibilities individuals across an organisation must take in this new age to work together to protect their enterprise and, in so doing, contribute to our nation's defence."

In his latest book, Clinton examines the need to take an enterprise-wide approach to cyber risk; looks at the growing threat as an issue that is not confined to IT; considers how boards are addressing cyber risk; and tackles the way organisations may be better structured for the digital age. He then goes on to outline a modern approach to assessing cyber risk, and considers the management of cyber risk from an enterprise-wide perspective.

Subsequent chapters are dedicated to examining in depth the roles and responsibilities of human resources management in cyber security; legal and general counsel; audit and compliance; and technical operations. Consideration of cyber security in mergers and acquisitions has a dedicated chapter, as does the role of cyber operations in developing a "culture of security".

And, as readers of this magazine will be comforted to know, cyber security in the context of supply chains and crisis management are also addressed in a book that is becoming a must-read for business leaders.



News briefing

A round-up of the latest industry news

In its Policy Statement on residential multi-occupancy buildings, the Financial Conduct Authority confirmed a series of measures specifically designed to protect leaseholders. From the beginning of 2024, insurers will be forced to act in leaseholders' best interests, treating them as customers when designing new products.

BIBA welcomed the rule changes announced by the FCA, in particular, the introduction of the new policy stakeholder status for leaseholders, and the increased transparency requirements around insurance arrangements and remuneration. The association had formerly commissioned extensive work to help members better demonstrate fair value for the activities and services they provide.

AXA Commercial deployed artificial intelligence to help establish if any buildings owned or occupied by customers were impacted by RAAC in the UK. The insurer used the AI-powered tool to review more than 70,000 multi-page documents in one week – a job, it said, would otherwise have taken 12 months to complete manually.

Most AI decision makers in the insurance industry are happy with the state of their AI governance, with 90% of respondents to a survey carried out by DLA Piper saying they believed their approach to be effective. The figure was 83% across all sectors.

Flexible working is key to creating a more diverse and inclusive workforce, according to a report published by the University of Nottingham and Browne Jacobson, whose authors also concluded that excessive alcohol consumption at team building and client events fuelled discrimination and harassment.

Origami Risk announced the acquisition of Dais Technology, a provider of no-code insurance technology. The acquisition increases Dais' market reach and client support capabilities, and expands Origami's suite of P/C insurance solutions for MGAs, insurers and reinsurers.

Chubb launched a new Lloyd's of London consortium designed to provide insurance coverage for risks associated with the transit and storage of lithium batteries, in a changing market for lithium battery transit and stock insurance. Meanwhile, Safetytech Accelerator signed up major UK maritime insurers, the UK P&I Club and TT Club to its Cargo Fire and Loss Innovation Initiative.

The world is falling "dangerously short" of the ambition that is needed to secure a safe future climate, according to analysis from PwC, which found that no G20 country achieved a decarbonisation rate of more than 11% in a single year since 2000. A similar warning shot was fired by Zurich Insurance after it said the world was not on track to hit the Paris Agreement targets, and warming could exceed 1.5 degree Celsius as early as 2040 with huge potential implications for business.

Zurich Resilience Solutions and KPMG Switzerland formed a strategic collaboration to offer advisory services to address the physical and transition risks associated with climate change. Sedgwick meanwhile introduced a climate risk and resilience programme designed to address the impact of climate-related losses. And Allianz published its first comprehensive net-zero transition plan, outlining its commitment to achieve net-zero emissions by 2050 in its proprietary investment and P/C underwriting portfolios; and by 2030 within its own operations.

For the full story behind all these headlines, visit **cirmagazine.com**

Legal and compliance department investment in governance, risk and compliance tools will increase by 50% by 2026, according to Gartner. It said assurance leaders are seeking out technology solutions to help them address increasing regulatory attention on executive risk oversight and monitoring.

Over half (54%) of consumers said that they would stop buying from a company if they were found to have been misleading in their sustainability claims, according to research from KPMG. The findings suggest that the concept of 'greenwashing' is widely recognised by consumers today.

Lloyd's and Moody's Analytics announced plans to jointly develop a solution to help to quantify greenhouse gas emissions across managing agents' underwriting and investment portfolios. The solution aims to aid managing agents in meeting expected regulatory reporting requirements.

As the offshore wind sector sees significant growth and opportunities, the industry faces an increased and varied range of risk, according to a new report from Allianz Commercial. It warned insurers and developers of the need to adapt to the challenges posed by bigger turbines and increased natural catastrophe risks.

UK financial services firms reported 640 cyber security breaches to the Information Commissioner's Office in the year to 30th June 2023, representing a threefold increase on the 187 cyber security breaches in the previous period, according to research conducted by law firm RPC.

Businesses found to have breached UK data protection laws when falling victim to cyber attacks could receive lower fines in respect of those infringements if they engage appropriately with the UK's National Cyber Security Centre, under a new agreement between the NCSC and the Information Commissioner's Office.

US-based medical device manufacturer Medtronic is facing a legal battle over allegations that it shared a 'treasure trove' of diabetes patient data with tech giant Google. Data and analytics company GlobalData warned that the case could lead to heightened scrutiny of the sector.

CREST and IASME agreed to partner with the National Cyber Security Centre to support the delivery of its new Cyber Incident Exercising scheme. Organisations wishing to join the CIE scheme will be assessed against the NCSC CIE Standard. CREST and IASME will manage the assessment, onboarding, monitoring and offboarding of providers assured under the scheme on behalf of the NCSC.

The Institute of Risk Management announced the appointment of David Epstein as non-executive director. Mr Epstein, group ALM and treasury director at Aviva, and a director of subsidiary, Aviva Capital Partners, has over 20 years' experience in financial services across investment banking, pensions, insurance and reinsurance.

McGill and Partners joined forces with Renew Risk to develop catastrophe models for offshore wind portfolios, via an initial five models in the Oasis framework, an open-source cat model platform, covering Northeast US hurricane, Taiwan earthquake and typhoon, and Japan earthquake and typhoon.

Stop loss strategies

As COP 28 approaches, Deborah Ritchie speaks to Nigel Brook about what corporates and their insurers should be aware of, and what new legislations and technological innovations may be on the horizon post-COP and as we head into a new year

What should corporates and their insurers be aware of as COP 28 approaches, and discussions focus on what can be achieved by 2030, rather than 2050?

If discussions at COP 28 do lead to an increase in policy ambition – which could take a number of forms – then it could be quite consequential for the fossil fuel industry over the next seven years, with an acceleration of the transition from fossil fuels to renewables. If that were to happen in a concerted way, it could materially affect operations and capital expenditure.

Something we might see as part of any policy shifts coming out of COP 28 is countries starting to move subsidies away from fossil fuels towards renewables. Global deployment of new solar and wind is already growing exponentially, and such a shift would increase this acceleration. And growth in renewables, or indeed in other technologies critical to the transition (such as electric vehicles, green hydrogen, green steel), should create underwriting opportunities for insurers.

Energy insurers are already seeing a shift in who is buying cover and the risks being covered, such that I think most insurers expect the make-up of their energy books to change substantially over the next seven to 10 years as renewables account for more and more electricity generation around the world and electric vehicles erode oil demand.

"An increase in policy ambition could be quite consequential for the fossil fuel industry over the next seven years, with an acceleration of the transition from fossil fuels to renewables"

Even for the existing companies they underwrite, the balance of their business will shift as well, and so too will the risks that come with that. Risks associated with offshore wind, for instance, are quite different from those in oil exploration and production – and that will have implications on their books of business, if not directly necessarily on their loss experience.

Quite a few insurers are setting ambitious policies to move away from insuring fossil fuels but that's not something that will happen overnight, of course.

What new legislation is on the horizon, and which sectors will be the most heavily impacted?

What we're increasingly seeing is climate and nature being spoken about in the same breath.

Since the Taskforce on Climate-Related Financial Disclosures voluntary reporting framework was published in 2017, it has rapidly become the gold standard; new European climate reporting regulations wrap themselves around it, the UK and other countries are making TCFD reporting mandatory, and the International Sustainability Standards Board has also adopted the framework.

We now have reporting recommendations from the TNFD (the Taskforce on Nature-Related Financial Disclosures), which were published on 18 September. I'd expect to see these following a similar playbook to TCFD, in terms of adoption by voluntary standards bodies and ultimately by legislators. The ISSB has already indicated that it will take the TNFD recommendations into account.

I think this topic will rise rapidly up the agenda, not least because the rapid degradation of nature and loss of biodiversity poses real dangers to the world economy. It's been estimated that over 50 per cent of the world's GDP is moderately or highly dependent on nature and its services.

A key problem is that most companies don't have the information needed to understand the ways in which their operations and value chains and financial performance could be impacted by the degradation of ecosystems. New EU reporting obligations will force companies to address this.

In Montreal last December countries around the world agreed to address biodiversity loss, restore ecosystems and establish a sustainable food system, with ambitious goals for 2030. These include conservation of at least 30 per cent of the world's lands, inland waters, coastal areas and

"Quite a few insurers are setting ambitious policies to move away from insuring fossil fuels but that's not something that will happen overnight, of course"

Nigel Brook is a partner at law firm Clyde & Co

oceans, and restoration completed or underway on at least 30 per cent of degraded on- and off-shore ecosystems.

Nature is expected to be high on the agenda at COP 28 too. One of the goals for discussion is making people and nature central to climate action, and we should also see plans to preserve rainforests and to implement nature-based solutions, such as restoring mangroves, which act as carbon "sinks" but also safeguard coastlines and ecosystems.

Tied in with this is the issue of water shortage – again a looming crisis that plays into the other two. Various factors are at play, including changing rainfall patterns due to climate change; natural aquifers being overdrawn by growing populations; and poor water management.

It is increasingly a concern for businesses, too – McKinsey have estimated that two-thirds of businesses face substantial water risks in their direct operations or in their supply chains. CDP have estimated the cost to businesses of water risks is U$301 billion – and that the expense of addressing these risks was less than a fifth of this figure.

"Today nearly all hydrogen is not 'green' because it is produced from coal or natural gas with high CO2 emissions. In the future it could be made in a climate-friendly way by electrolysing water using renewable electricity, and then be used to store surplus green energy or to decarbonise hard-to-electrify sectors"

What technological innovations can we expect to make headlines during COP 28?

Wind and solar are now firmly established, with deployments growing exponentially. To illustrate this, in solar, the world is currently adding the equivalent of a new nuclear reactor every day. We're also seeing exponential growth in batteries, electric vehicles and heat pumps.

At COP 28 we could also hear about new and emerging technologies such as modular floating wind arrays (which can be deployed in deep water), direct air capture (to remove CO2 from the atmosphere), and lab-grown meat (to address the heavy carbon footprint of cattle).

We'll also probably hear quite a lot about hydrogen. Today nearly all hydrogen is not 'green' because it is produced from coal or natural gas with high CO2 emissions. In the future it could be made in a climate-friendly way by electrolysing water using renewable electricity, and then be used to store surplus green energy or to decarbonise hard-to-electrify sectors such as long-distance transport and heavy industry. When burned it doesn't produce any CO2.

Interview by Deborah Ritchie

Pastures new

Disordered by geopolitical risks, macroeconomics and the pandemic, global supply chains are rebuilding in the context of a growing focus on climate risk. Jeremy Hughes looks at how companies are finding synergies between the two to create mutually beneficial outcomes

The Covid-19 pandemic triggered a dramatic and swingeing realignment of global supply chains. Around the world, businesses and industries that relied on extended supply chains experienced disruptions and delays that called into question the very basis of their business models, in some cases driving companies to the brink of bankruptcy.

Even without the unexpected invasion of Ukraine in February 2022 which prolonged the economic downturn and hampered business recovery, supply chains were ripe for a radical shake-up. While this is underway, increasing climate risk disclosure requirements are creating an urgent imperative to uncover and manage supply chains' inherent ecological risks.

Whilst there is work to be done to both reduce supply chain risks and address climate change risks, there are synergies to be found between the two otherwise separate fields that can – and do – lead to mutually beneficial outcomes.

Opening new doors

Manufacturers and retailers looking to reduce supply chain risk have taken steps to increase resilience by cutting distances and dependencies.

One key strategy for US manufacturers has been to regionalise, onshore or nearshore production to reduce reliance on Asia, particularly China. Apple, for instance, has shifted some of its production from China to India, while Foxconn, a major Taiwanese Apple supplier, has opened facilities closer to iPhone's home in Mexico.

Thanks to lower labour costs, proximity to the US market, and trade agreements such as the United States-Mexico-Canada Agreement, Mexico has seen an influx of US brands in

"Suppliers are taking responsibility for monitoring and restocking a customer's inventory, gaining access to real-time data on the customer's stock levels"

recent years, and is now home to new facilities for such major names as Ford, General Motors and Whirlpool, among others.

Collaboration is a key strategy for reducing supply chain risk. Whilst supply chain relationships have historically been jealously guarded, many are now working together to improve efficiency, reduce costs, and enhance overall performance.

In vendor-managed inventory arrangements, for instance, suppliers are taking responsibility for monitoring and restocking a customer's inventory. They gain access to real-time data on the customer's stock levels, and can proactively replenish supplies as needed, ensuring the customer never runs out of essential items.

And with joint product development agreements, manufacturers and suppliers collaborate to develop new products or improve existing ones, reducing time-to-market and enhancing product quality in the process. Cross-docking arrangements enable products to be transferred directly from inbound transportation to outbound transportation without being stored in a warehouse, while more companies are partnering with third-party logistics providers to manage transportation, warehousing and distribution.

Technology and data analytics has a critical part to play. Enhanced capability in internet of things sensors enables data collection for shipments with greater granularity than ever before, while distributed ledger technology or blockchains not only provide secure tracking, but advanced automation as well.

In one innovative implementation of DLT, Singapore's adoption of electronic bills of lading for processing on a blockchain-enabled platform has enabled simultaneous handling of complex customs and trade finance procedures which until recently were paper-based, requiring time-wasting manual treatment. Taking the slack out of shifting cargoes in this way promises reduced downtime for shipments and greater precision in delivery timings.

Technology and big data are also key to better risk prediction, and emerging developments in artificial intelligence and big data hold great promise in this arena. Predictive analytics, for instance, uses statistical modelling, data mining and machine learning to identify vulnerabilities in supply chains. The resulting insights can help to forecast demand, optimise shipping routes, and enhance warehouse efficiency.

Finding synergies

Policymakers seized on the fundamental reset forced on the world by the pandemic to refocus on sustainability. President Biden's Build Back Better framework, the EU's Recovery Plan for Europe, NextGenerationEU, and China's 14th Five-Year Plan all set out new intentions to embed greater sustainability into programmes designed to rebuild the global economy. At the same time, these efforts also drove enhanced ESG disclosure standards for companies.

In the EU, the Corporate Sustainability Reporting Directive was enacted in January 2023, while in the US, the Securities and Exchange Commission directs all public companies to disclose data that is material to investors, including information on ESG-related risks.

"Singapore's adoption of eBols for processing on a blockchain-enabled platform has enabled simultaneous handling of complex customs and trade finance procedures"

The UK's Financial Stability Board created the Task Force on Climate-related Financial Disclosures to advance proposals on what information companies must disclose, and the IFRS Foundation and the International Accounting Standards Board's Sustainability Disclosure Standards for companies, S1 and S2, will take effect in January 2024.

In short, companies already engaged in de-risking their supply chains are also required to look into, quantify and publicise their environmental and social risks. The burden falls heaviest on larger corporations in high-emitting sectors, including power generation, heavy manufacturing and transport.

Most, if not all, have started by addressing the most obvious risks, such as GHG emissions. The GHG Protocol, jointly produced by the World Business Council for Sustainable Development and the World Resources Institute, places this into three categories across a company's operations.

Scope 1 emissions originate from sources owned or controlled by an organisation; Scope 2 are indirect greenhouse gas emissions – such as at power generation plants. Scope 3 includes all other indirect emissions in an organisation's value chain, including both upstream and downstream, often beyond its direct control.

Investors increasingly require companies to declare these risks as they become more active in exercising their voting rights on all aspects of ESG. On top of this, corporate financing is increasingly tied to sustainability criteria. This means quantifying risks as accurately as possible has a direct financial consequence for the company – and done well, could offer a significant competitive advantage.

While none is complete or comprehensive, consultancies have brought a range of measurement, quantification and analysis services to market. Value-adds include advice on managing carbon footprint, reporting and adaptation.

The Big Four auditing firms all offer variations of this service, while newer specialist consultancies now provide sustainability advisory services. And market information providers such as S&P, Moody's and Fitch leverage their position in analysing corporations' risks to include environmental, social and governance factors.

Responsible response

Faced with growing pressure to mitigate their carbon footprint and consider their impacts on communities, businesses are adapting their operations – if not their business models – to comply. And it stands to reason that the companies that adapt best will be the winners of the future.

Adaptation was a major focus at COP27 held in Egypt last year. UN Climate Change Executive Secretary Simon Stiell said, "[While] adaptation alone cannot keep up with the impacts of climate change, which are already worse than predicted, adaptation actions are still crucial and are critical to upgrade small-scale, fragmented and reactive efforts."

According to the World Economic Forum's *Global Risks Report* for 2023, failure to adapt to climate change is the second-greatest risk for companies over the next ten years. Such adaptation includes more than limiting supply chain risks. From enhancing infrastructure resilience and disaster preparedness to education and community engagement, adaptation requires the involvement of every area of the business.

Business leaders are aware of the implications; according to PwC's 2023 *Global CEO Survey*, almost 40 per cent of CEOs believe their companies will no longer be economically viable in ten years' time if they do not adapt. In addition, although climate change was less prominent as a risk within the next year compared with other global risks, CEOs still anticipate climate change significantly affecting their cost structures (50 per cent), supply chains (42 per cent) and physical

"Some 40 per cent of CEOs believe their companies will no longer be economically viable in ten years' time if they do not adapt, and more anticipate climate change to significantly affect their cost structures"

assets (24 per cent) to a moderate to substantial degree. As a result, 48 per cent of CEOs are modifying their supply chains: 46 per cent are adjusting their presence in current markets and/or expanding into new markets, while 41 per cent are diversifying their product or service offerings.

Fresh fields

Adaptation can also be a spur to innovation. Apart from new technologies under development to generate, store and distribute clean energy, or to capture and sequester CO2, fresh ways of producing and consuming goods are rapidly emerging in a drive to reduce waste and prolong utility. While many new business models will take time to gain scale, others may evolve from incumbents not content to sit still while the landscape changes around them.

As Boston Consulting Group points out: "Once companies move beyond what can be achieved though technical and operating efficiencies, most will need new operating models and ways of working."

And PwC states that, in the context of digital transformation, "the starting point for enterprise transformation of this sort often is a reimagination of a company's place in the world – looking beyond the current portfolio of businesses and products to determine what value an organisation will create, and for whom."

For example, Danish multinational energy provider Ørsted, founded as a natural gas supplier in the '70s, in 2009 adopted its '85/15 vision' strategy to switch its activities from 85 per cent based on fossil fuel to 85 per cent based on green energy. Today it provides offshore and onshore wind, solar and storage solutions, which together provide 92 per cent of its energy output.

In the consumer goods sector, Global big-hitters Unilever and Nestlé have both invested time and capital in alternative proteins which, compared with traditional meat production, require less land, water and energy, resulting in lower emissions and reduced ecosystem disruption.

Growth has been significant, perhaps driven by consumers' need to economise during the recent cost-of-living squeeze. Boston Consulting Group calculates that the US retail alternative protein market grew by nine per cent in 2022. Overall, the alternative protein industry attracted US$5 billion in disclosed investments in 2021 – a fivefold increase over three years.

Furthermore, the consulting firm estimates that the combination of technology and business model innovation has the potential to reduce greenhouse gas emissions by up to 80 per cent over current levels.

Perhaps the most compelling outcome from the current wholesale redrawing of global supply chains is that, thanks to reduced emissions and technical innovation, the benefits of investments in adaptation accrue to stakeholders beyond those the investing corporations service. Getting to grips with supply chain risks, be they financial or environmental, has a network effect that will help to address the most pressing threats to communities and ecosystems.

Gaining momentum

The winds of change in the energy sector have been blowing strongly in favour of renewables for some time. Despite the huge opportunities, projects come with substantial risks, putting insurers at the very centre of future development, writes Martin Allen-Smith

As the effects of climate change become increasingly clear through significant weather events and rising average temperatures, minds – from political leaders to consumers – have become focused on the existential priority of moving towards a net zero future.

At the heart of achieving this is how we source the energy that powers pretty much everything in our day-to-day lives, and inevitably it means undertaking huge changes in systems and infrastructure if society is to move away from the fossil fuel-burning status quo.

This year, a record number of clean energy projects have been awarded funding from the government's renewables scheme, which it says has the multiple aims of helping the UK grow the economy, achieve net zero, protect families and businesses from volatile global gas prices, and strengthen energy security.

From the first annual 'contracts for difference' round, a total of 95 clean energy projects have been successful with their bids, with a total budget funding of £227 million – which the government says secures sufficient energy to power the equivalent of two million homes. Significant numbers of solar power and onshore wind, and a record number of tidal energy schemes, have been awarded funding under the scheme. For the first time, geothermal projects – which use a natural heat source underground for generating power – have also been successful.

Elsewhere, the European Parliament recently voted to expand its ambitions for renewable energy, declaring that renewables will have to make up 42.5 per cent of the EU's energy consumption by 2030, with

Mangroves capture CO2 from the atmosphere

"With energy transition and climate resilience at the top of the industry's agenda, responses suggest a bullish appetite for sustainable energy, with the majority of insurers planning for double-digit growth, mainly driven by new business, rather than rate"

the aim of achieving 45 per cent.

The update of the renewable energy directive builds on the deal already established in March, but that 'final' deal was held up by countries seeking more latitude on nuclear energy and gas. The legislation will also speed up procedures to grant permits for new renewable energy power plants, such as solar panels or wind turbines, or to adapt existing ones.

New energy projects present huge opportunities in a sector that is only likely to grow, but it also comes with sizable risks. For renewable energy asset owners and investors, material damage and business interruption insurance should provide a crucial safety net, protecting property assets and the business for loss of income against unforeseen events. In the current climate of increasing asset reinstatement values and wholesale energy prices soaring, underinsurance is one of the major risks that is facing the industry.

Carl Gurney, renewable energy director at Marsh says: "Insurance is often seen as a necessary evil driven by legal or contractual requirements. However, engaging with insurers early on can actually become a cost benefit as it enables them to review designs to ensure the right loss controls are factored in and the correct construction and operational controls are implemented. This will help improve...return on investment, and allow insurers to keep underwriting risks to ensure climate change targets are met."

A report from broker Howden assessing underwriting appetite by line of business for the London Market found the stand-out class of business to be sustainable energy. With energy transition and climate resilience at the top of the industry's agenda, responses suggest a bullish appetite for this class, with the majority of insurers planning for double-digit growth, mainly driven by new business, rather than rate, and additional carriers considering entering the space.

Further to last year's survey, which revealed that the market was keen to embrace new opportunities such as sustainable energy, this year's findings reveal that 80 per cent of insurers plan for growth in the sector, with an average planned GWP growth of 13 per cent across respondents. This year, 35 insurers responded with planned growth of between 15 and 25 per cent, with two further markets considering entry into this line of business.

Anne Rohbeck, CUO of specialty at Swiss Re, says renewables projects present a number of challenges for investors, not least a need for high up-front investment and uncertain returns which can take a long time to realise. Novel technologies can also add to the risks and unknowns. "While there are undoubtedly some elements in common, each project comes with a different set of risks uniquely influenced by factors such as location and technology.

"On top of all of this looms the growing risks associated with climate change. More severe weather conditions like floods, convective storms and hail events add to the potential hazards associated with renewables projects. All of this combined can deter investors and has contributed to the financing gap."

Swiss Re has highlighted a number of key actions for insurers to prioritise in order to best support sustainable energy developments. Crucially, it requires an innovative approach to risk management and product development from the sector which it says can unlock the necessary capital and give further momentum to the green transition. This includes underwriting risks during the construction phase, leaning on insights and data gathered from previous experience to help balance out uncertainties.

"Renewables projects present a number of challenges for investors, not least a need for high up-front investment and uncertain returns which can take a long time to realise. Novel technologies can also add to the risks and unknowns"

The insurance industry also has a role to play in encouraging innovation and supporting the adoption of new technologies, using its perspectives on the risks involved to share insights to inform new projects, and help address risks and volatility without sharing proprietary information. This is particularly relevant given the talent gap in the renewables sector in some markets.

This year, Swiss Re set up the 'centre of competence' for renewable energy, which aims to help address the data and knowledge gaps in frontier markets, as well as draw on existing relationships and partnerships to support projects. By using insights unique to each region, incorporating data such as local weather conditions, the aim is to help insurers obtain a big picture view of their projects.

Process components, fermenters and biogas storage tanks

Alongside this, insurers can also use their own assets to invest in renewable projects. Specialists such as Climeworks allow insurers to enter long-term purchase agreements for direct air capture and storage of carbon dioxide.

Rohbeck says: "As we work towards meeting the carbon-curbing targets set out in the Paris Agreement, the renewable energy transition is fundamental. And insurers play a role in managing the far-reaching systemic change that's needed to make this a reality. By boosting access to finance, helping manage risks and supporting innovation, the sector can help drive further momentum in adding renewable capacity."

Carbon capture ambitions

With the urgent need to limit climate warming and reduce greenhouse gas emissions, interest is growing in carbon capture storage, which involves capturing CO2 from industrial processes and storing it underground. The technology is attracting significant investment globally, with global market size expected to grow to US$180 billion by 2030.

According to the International Energy Agency, there are around 300 projects in various stages of development across the value chain, with ambitions for over 200 new capture facilities in operation by 2030. CCS facilities will capture around 125 Mt CO2 per year by 2030, up from 45 Mt CO2 captured in 2022.

Wouter Bosschaart, a director in Aon's Strategy and Technology Group and author of a recent report on transformative trends for the re/insurance market, says: "The CCS market represents a significant opportunity for insurers. With potential premiums of US$1 billion-5 billion by 2030, CCS is ranked in Aon's top ten megatrend re/insurance opportunities. High levels of

"High levels of investment, coupled with a more open regulatory environment, are driving growth in the number of planned projects and therefore a growing need for re/insurance protection"

investment, coupled with a more open regulatory environment, are driving growth in the number of planned projects and therefore a growing need for re/insurance protection."

In the US, recent legislation has pledged around US$12 billion for CCS-related initiatives over the next five years, targeting 80 additional projects to be operational by 2030, with CCS capacity increasing fivefold. In Europe, around 50 projects are scheduled for completion by 2030, with significant activity in the UK, the Netherlands and the Nordics.

While more than 50 per cent of existing CCS facilities are based in the US, a surge in projects is expected across Europe and Asia by 2030, with Europe forming 30 per cent of the global market size. It brings several opportunities for insurers, including demand for property and business interruption insurance, as well as construction cover for new projects.

"Despite significant investment, many re/insurers are reluctant to cover CCS-related risks," Bosschaart adds. "CCS is still in its early stages and the technology has yet to demonstrate sustained success, so a lack of technical knowledge of carbon storage solutions within the industry remains. With few re/insurers currently active in the market for CCS risks, those that are first to develop the expertise and knowledge will hold the advantage."

Ahead for heights?

After years of adjournments and stalling in government, and a series of other setbacks, could progress soon finally be seen in the UK's ongoing building safety scandal? David Adams investigates

Six and a half years after the Grenfell Tower disaster, the market for insuring high-rise, higher risk multi-occupancy residential buildings in the UK is now as much in need of repair as the least fire-resilient of those buildings. The costs and difficulty of finding insurance for these buildings have increased enormously, and attempts to complete remediation work have also been delayed by problems sourcing insurance for companies and contractors undertaking this work.

Between 2016 and 2021 premium rates for multi-occupancy residential buildings increased by 125 per cent, according to the FCA's September 2022 report on insurance for multi-occupancy buildings.

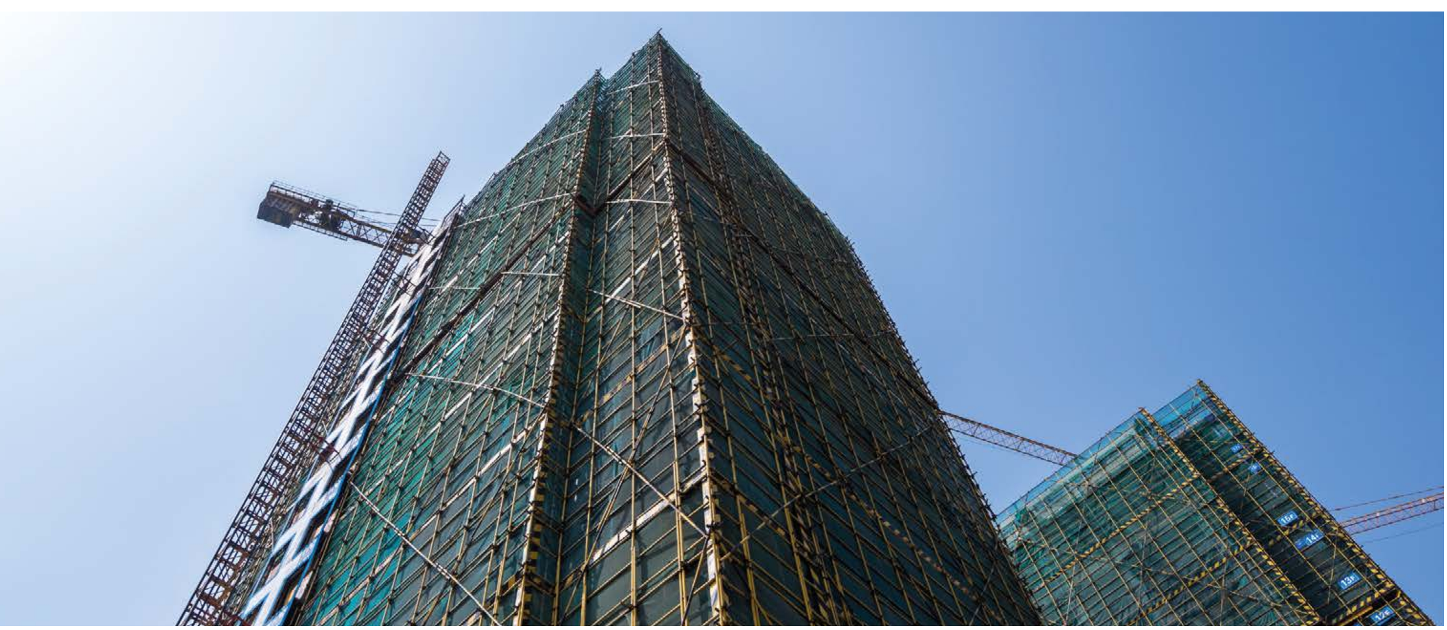
"Insurers started asking a lot more questions … [and] in cases where combustibility issues were found, premiums increased," says Alastair Blundell, head of general insurance at the British Insurance Brokers' Association. "But capacity decreased at the same time. That caused immense pressure and concern for leaseholders and property owners."

David Ovenden, chief underwriting officer at Axa, points out that price tends to be a function of market capacity. Where an insurer might previously have written 100 per cent of the risk attached to a building, the discovery of combustible materials, or a lack of fire resilience (protection systems, fire breaks and so on) in the building might reduce the insurer's ability to underwrite that risk to 10 per cent.

"That means a broker would have to go out and get more capacity … and it can get expensive," says Ovenden. "It's unfortunate, but it's logical, rational and defensible. It's a balanced view of the risk we face."

Other issues are also influencing the market, Ovenden continues. One is the difference between "fire safety" and "fire resilience". The former may be applied to a combustible building that the fire service are confident they will be able to remove people from, simply because it is not a tall building. Insurers, the ABI and other experts are currently consulting with government on including a requirement for fire resilience in fire safety standards.

"We need resilience in there, otherwise the insurance industry is



going to struggle to get premiums down to a level that people are going to want to pay," Ovenden warns.

Meanwhile, the ABI, BIBA and McGill & Partners have been working together to create a Fire Safety Reinsurance Facility (which is due to be launched before the end of this year) in the hope that it would allow insurers to increase risk capacity for medium height and tall residential buildings with material fire safety issues. It could also mean insurers may be able to provide cover for whole buildings.

"That will allow mainstream insurers to look at these more difficult risks and offer more capacity, hopefully at a more affordable price," Blundell insists. "So that is a glimmer of hope."

The other key challenge lies in providing affordable insurance, particularly professional indemnity cover for companies and contractors working on remediation of existing buildings with fire safety issues.

One reason this problem persists is the nature of the two main routes to remediation work. The first is remediation by the developer that constructed the building. The second is via an application to the government's Building Safety Fund, which was designed to enable remediation in buildings over 18m high. There is also a Cladding Safety Scheme, known previously as the Medium Rise Scheme, for buildings between 11m and 18m high.

There is some concern within the insurance industry about a lack of independent oversight in cases where the developer takes responsibility for remediation. Ovenden says Axa is among insurers that offer landlords support to ensure developers remediate the building to an A1 standard of fire resilience, with all combustible material removed from the structure "by helping the landlords ask the right questions".

In cases where the Building Safety Fund is used, the other major problem is the obligation for companies and contractors carrying out the work to find PI cover of up to £10 million.

"The reality is that very few firms can purchase that level of PI," says Blundell. BIBA fears this will leave remediation work as the preserve only of a few of the largest firms, reducing competition, slowing progress and keeping costs high.

It has suggested a range of measures to resolve these issues. They include reviewing PI requirements for both the Building Safety Fund and the CCS. BIBA supported the EWS1 approach (which, leaseholders tell us, has created its own, separate issues) for confirming that safety assessments had been conducted on buildings and suggests a similar type of modelling might be used to help insure professionals undertaking remediation work against safety liabilities. More radically, BIBA suggests that the government could consider removing the burden of professional liability from contractors responsible for fire safety or fire remediation work within these projects.

It also suggests reviewing the joint and several liability regime that governs UK construction contracts, replacing it with a more proportionate approach to allocating liability as is the case in the equivalent regime in Australia.

What the government has done so far in relation to the various issues around high-rise buildings and fire safety is to begin creating a new regulatory regime, in line with the recommendations of Dame Judith Hackitt's Independent Review of Building Regulations and Fire Safety, published in 2018. Parliament passed new building and fire safety legislation in 2021, introducing new fire safety regulations, and created the Building Safety Regulator.

The new regime also mandates creation of a 'Golden Thread' of information about each building, stored in an accessible digital

format, including details of Building Regulations compliance and the identification and mitigation of safety risks. Every building in scope will also need a Principal Accountable Person, responsible for managing the building's safety, by preventing and reducing fire spread and structural failures. They will need to produce a safety case report summarising safety risks affecting the building and how these are managed.

"The undertaking of building safety case reports is a really positive step forward," says Julian Strutt, director, property and real estate, at Charles Taylor. He points out that in the past, information about the construction of buildings was often lost as those buildings changed hands, or when further renovation works took place.

"The opportunity to gather that information and to identify risk helps not only the insurer, but also gives the leaseholder more confidence about the building they are living in," he says.

Leaseholders will also benefit from the FCA's ruling in September 2023 that insurers must act in leaseholders' best interests, treating them as customers when designing insurance products. Insurers will be banned from recommending policies based on commission or remuneration and must provide much more transparency around policy details and pricing.

The ruling follows the FCA's 2022 review of this market, which concluded (unsurprisingly) that leaseholders had experienced higher costs but received poor value in recent years. One reason for this was the practice of insurance brokers sharing commission with whoever was arranging buildings insurance policies, including property managing agents, landlords and freeholders.

In a statement responding to the ruling, ABI director of general insurance Mervyn Skeet agreed leaseholders "deserve greater transparency" around policies, but also asserted that "the ultimate solution to the problem is to remediate buildings to a standard that saves both lives and property and we urge government to progress this urgently".

In late October the government announced it had agreed a pledge with five leading brokers that they would end the practice of sharing commissions with those placing or arranging buildings policies. The insurers also promised to put a 15 per cent cap on the proportion of a premium brokers take for arranging cover.

The ABI has also advocated other changes to help increase capacity and reduce insurance costs. They include the government providing cover for catastrophic losses to affected buildings above a certain amount; removing Insurance Premium Tax from policies for affected buildings; and more clarity on how information recorded on the Golden Thread for each building will be recorded and stored.

At BIBA, Blundell points out that net zero and sustainability issues are likely to become ever more prominent in future, forcing further adaptations of both regulation and of insurers' practices and policies. For example, he notes the development of new, timber-based construction methods for tall buildings. "We need to anticipate what new risks could come down the pipe and be prepared to look at those," he says.

"I think the industry wants to do the right thing," Blundell continues. "The McGill risk sharing scheme should help in terms of bringing more capacity in at a more affordable price. This has historically been a competitive market for insurers and brokers and we should get back to that situation once buildings are being built to the right standards. We have good historical evidence that when a building is remediated and the fire safety issues are resolved, the cost of buildings insurance can be negotiated downwards by our members." There is some light at the end of the tunnel, it seems – but we still don't know how long the tunnel is.

Creating an enterprise-wide GenAI policy

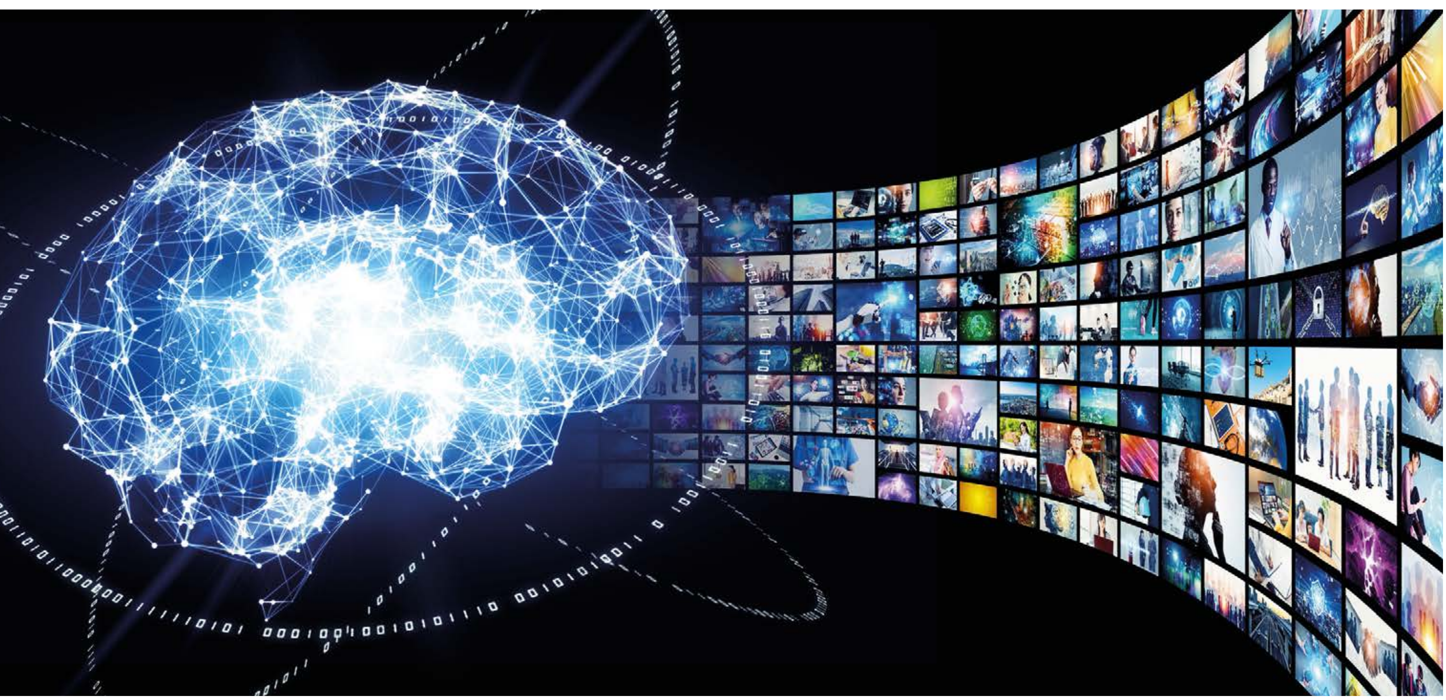
As companies look for ways to make generative AI valuable to the enterprise and to employees, guidance has been issued to help general counsel establish policies that will prepare them for possible future legal requirements. CIR looks at the report

Generative AI has seen a huge growth in popularity in the past year. And, as employees experiment with the numerous tools increasingly available to them, general counsel is being called upon for support in issuing guidance on its safe use.

The first goal, according to guidance issued by Gartner this quarter, is to align on risk tolerance. In determining the company's risk tolerance, legal leaders should borrow a practice from enterprise risk managers and guide a discussion with senior management on 'must-avoid' outcomes, it says, suggesting that they discuss the potential applications of generative AI models within the business, and, once these are identified, consider the outcomes that may result from them, and which entail acceptable risk given the potential benefit of AI.

"To craft an effective policy, general counsel must consider risk tolerance, use cases and restrictions, decision rights, and disclosure obligations," says Laura Cohn, senior principal, research at Gartner. "Having GenAI guardrails and policies in place will better prepare enterprises for possible future legal requirements. Guidance on using generative AI requires core components to minimise risks while also providing opportunities for employees to experiment with and use applications as they evolve."

Based on practices in AI policies instituted by companies and city governments, analysts at Gartner propose that general counsel direct organisations to consider three further actions when establishing a policy:



Determine use cases and restrictions
Legal leaders are advised to gain an understanding of how generative AI could be used throughout the business by collaborating with other functional leaders. The report's authors suggest that they compile a list of use cases and organise them according to perceived risk — both the likelihood and severity of the risk.

For higher risk situations they might consider applying more comprehensive controls, such as requiring approval from a manager or AI committee. In the highest-risk cases, outright prohibition may be the only option. In lower risk use cases, which they define as staff coming up with ideas for a fun activity during a staff off-site, basic safeguards, such as requiring human review, may be all that is needed.

"General counsel should not be overly restrictive when crafting policy," Cohn says. "Banning use of these applications outright, or applying hard controls, such as restricting access to websites, may result in employees simply using them on their personal devices. Leaders can consider defining low risk, acceptable use cases directly into policy, as well as employee obligations and restrictions on certain uses, to provide more clarity and reduce the risk of misuse."

Agree on decision rights and risk ownership
At this point in the development of the technology, Gartner advises that leadership teams agree on who has the authority to make decisions on generative AI use cases. It proposes that legal teams work with functional, business and senior leadership stakeholders to align on risk ownership and review duties.

"Document the enterprise unit that governs the use of AI so that employees know to whom they should reach out with questions," Cohn advises. "General counsel must be clear if there are uses that do not need approval, specify what they are directly in the policy, and provide examples. For use cases that need approval, inform employees what they are, clearly document the role that can provide approval, and list that role's contact information."

Decide on disclosures
Organisations should have a policy of disclosing the use and monitoring of generative AI technologies to both internal and external stakeholders, according to the report's authors. In this respect, general counsel should help companies consider what information needs to be disclosed and with whom it should be shared.

"A critical tenet common across global jurisdictions (including the standard-setting EU) is that companies should be transparent about their use of AI, Cohn explains. "Consumers want to know if companies are using generative AI applications to craft corporate messages, whether the information appears on a public website, social channel, or app.

"A critical tenet common across global jurisdictions is that companies be transparent about their use of AI. Consumers want to know if companies are using generative AI applications to craft corporate messages, whether the information appears on a public website, social channel, or app"

"This means general counsel should require employees to make sure the GenAI-influenced output is recognisable as machine-generated by clearly labelling text. Organisations also may consider including a provision to place watermarks in AI-generated images to the extent technically feasible," Cohn concludes.


QBE.
Prepared.
How can businesses build resilience in a challenging operating environment?
Visit QBEeurope.com/sector-resilience to find out.
QBE
Business insurance

Sponsored by

QBE

CIR
CONTINUITY INSURANCE & RISK

Protecting against health risks around lithium-ion batteries *Lithium-ion batteries are found in almost every home, business and workplace in the modern world. While lithium-ion cells power the lives of millions of people every day, Nick Fox, senior risk manager, QBE Europe, examines some of the associated health and safety risks*

10 ways to mitigate risk in use and storage of lithium-ion batteries *As a leading business insurer, QBE is aware of the risks that lithium-ion batteries can pose in commercial and industrial environments. Adrian Simmonds, interim practice leader at QBE Europe, outlines the steps employers can take to mitigate the risks*

Lithium-ion batteries: Mitigating the risks

QBE

Sponsored by

Protecting against health risks around lithium-ion batteries

Lithium-ion batteries are found in almost every home, business and workplace in the modern world. While lithium-ion cells power the lives of millions of people every day, Nick Fox, senior risk manager, QBE Europe, examines some of the associated health and safety risks

The risk of fire posed by lithium-ion batteries is well documented, regularly featuring in headlines and dominating conversations around electric vehicles, battery energy storage systems and battery waste handling.

Frequency is growing too; the London Fire Brigade reported callouts to battery fires once every two days in 2023, and the running total of 'e-fires' in the capital had already outstripped the 116 recorded in 2022 by September.

The unique risks of lithium-ion fires

Thanks to a phenomenon called thermal runaway, within a lithium-ion battery any internal fault or external conditions (such as overcharging or mechanical damage) can begin an irreversible and uncontrollable self-heating state. Once a battery begins heating in a thermal runaway, it can only end one way: with extremely high temperatures, fire, smoke and vapours.

Thanks to the fast-building intensity of thermal runaway, the time between the fault or damage occurring and the release of toxic vapour during a fire can sometimes be just a few minutes, or even seconds.

Additionally, lithium-ion battery fires not only burn for much longer periods than 'normal' fires, but they can reignite hours, days, or even weeks later, and multiple times – making the risk much more complex.

While the risk to property is widely discussed in the context of lithium-ion fires, there is less conversation around what risk managers should be aware of when considering health risks in those same events.

Although contact with toxic materials is unlikely when handling lithium-ion batteries in a controlled manner, if the integrity of the battery housing is damaged, or the cell catches fire, the explosion can often be so violent that it shatters the battery. This immediately releases a dangerous shower of fragments, corrosive chemicals and poisonous vapour – highly hazardous health risks for anyone nearby.

Highly hazardous: the risk to life

Highly toxic combustion products from lithium-ion fires can result in damaging and even fatal health outcomes for those exposed to them.

Vapour clouds can form when a lithium-ion battery explodes without the gases igniting or being vented to the atmosphere. Such containment can occur in a closed storage room or a shipping container where there are no immediate ignition sources.

This vapour cloud is not like smoke; it's a mixture of toxic and explosive gases. Often it will not spread like smoke – due to differences in density it pools at ground level, proving more dangerous to those trained to stay low during a fire to avoid inhalation.

In fact, even in instances where the gases can disperse, there is still the possibility that toxic health effects may occur from brief exposure, albeit at a lower impact.

Battery substances posing serious health risks

Hydrogen fluoride: Hydrogen fluoride can exist as a colourless gas which, despite dispersing quickly in air, can still enter the body through inhalation. When hydrogen fluoride is dissolved in water, it may be known as hydrofluoric acid, a highly toxic, reactive chemical which enters the body through direct contact. Health risks include:

- Very serious and extremely painful burns from any skin contact, the extent of which can be missed at initial stages, as it can take up to 24 hours after contact before pain is experienced.
- Continued breakdown of flesh and tissue and damage to organs long after initial efforts have been made to wash it from the skin.
- Irreparable damage to the eye, even with very small quantities of diluted hydrofluoric acid.
- Fatal toxicity by inhalation.

Carbon monoxide and carbon dioxide: Ignition of lithium-ion batteries results in the release of carbon monoxide and carbon dioxide. Both interfere with the absorption and transport of oxygen around the human body, leading to oxygen deprivation of tissues and organs. Reduced oxygen flow to the bloodstream and cells initially causes fatigue, clumsiness, breathlessness, confusion and increased heart rate. With continued or increased exposure, symptoms may worsen to include nausea, vomiting, convulsions, or coma – before progressing to death.

Cobalt: At high temperatures, cobalt is attacked by atmospheric oxygen and by water vapour, producing cobalt(II) oxide. Vomiting and abdominal pain are the results of ingestion, inhalation and/or skin contact with dusts or solutions containing cobalt.

Nickel: The toxicity of nickel metal and inorganic nickel compounds vary depending on their solubility, but short-term effects can include both irritation of the skin (on contact with dust or solutions of soluble nickel salts) and eye irritation (from exposure to nickel dust, fumes, or splashes from nickel-containing solutions). It can also enter the body via inhalation of dust, fumes or mist.

Copper: Owing to its heat and electrical conductivity as well as its resistance to corrosion, ductility and malleability, copper has many industrial applications and is widely used in electrical wiring and switches. Occupational exposure to copper is usually via inhalation (leading to a fever, headache, fatigue, cough, sore throat and tightening of the chest) and ingestion of contaminated food and liquids (causing stomach pain, nausea, vomiting and diarrhoea).

Aluminium: Aluminium powder is flammable and given an ignition source can ignite on contact with air in a dust explosion. Aluminium reacts with alcohols, and water reacts violently with oxidants, strong acids, strong bases and chlorinated hydrocarbons causing a fire and explosion hazard.

Inhalation of aluminium dust can cause irritation of the respiratory tract, whilst ingestion may result in burning in the mouth and throat and mild gastrointestinal upset and in severe cases, ulceration of the lips and mouth.

Advice for risk managers

Risk prevention strategies are essential to mitigate health risks in relation to lithium-ion batteries. In addition to undertaking a fire risk assessment, firms should develop a comprehensive procedure to prepare for emergency events, in consultation with relevant employees.

Emergency procedures should be structured so that all those working with or near lithium-ion batteries have a thorough understanding of the actions they should take, alongside any specialist clean-up of released materials.

Employees should be made aware that manual fire extinguishers do not work effectively on lithium-ion battery thermal runaway fires. Extinguishing the flames changes the threat from a fire hazard to an explosion hazard, so employees should evacuate immediately and call the Fire Brigade rather than attempting to tackle a lithium-ion battery fire themselves.

Whilst specific control measures implemented will be guided by an individual site risk assessment, in response to health and safety risks, they are likely to recommend firms to:

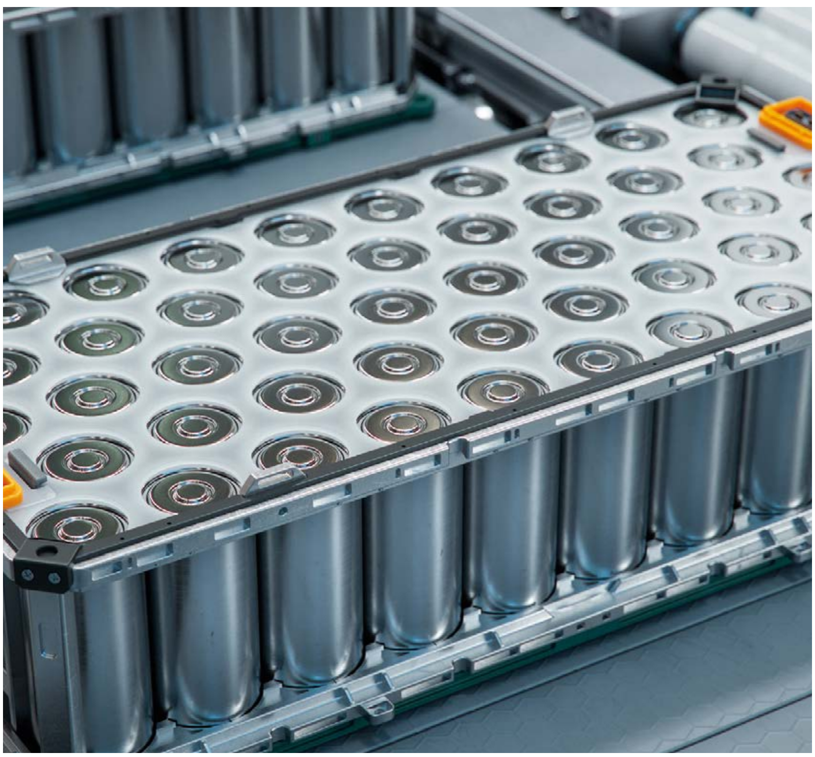
- Identify a suitable local exhaust ventilation of the battery charging area.
- Establish a requirement to wear suitable personal protective equipment including gloves, eye protection, boots and apron.
- Segregate the charging area: access for authorised personnel only.
- Ban metal objects in pockets which could fall onto the battery or bridge across its terminal.
- Keep sources of ignition (such as flames, sparks, electrical equipment, hot objects and mobile phones) away from batteries that are being charged, have recently been charged, or are being moved.
- Use suitable single-ended tools with insulated handles and fit temporary plastic covers over the battery terminals when handling.
- Maintain a readily-accessible and in-date supply of the antidote to exposure to hydrofluoric acid – calcium gluconate gel. Whilst suitably trained first aiders can administer the gel, in view of the severity of the effects of exposure to hydrofluoric acid and the swiftness with which it is desirable to apply the antidote, consider specifically training individuals in its application in any area where exposure may occur.
- Ensure hand washing facilities with warm water are available.

This guidance was produced in partnership with Finch Consulting. For a detailed employer guidance note on health and safety risks around lithium-ion batteries, visit the QBE Document Library: www.qbeeurope.com/document-library

Nick Fox, senior risk manager, QBE Europe

10 ways to mitigate risk in use and storage of lithium-ion batteries

As a leading business insurer, QBE is aware of the risks that lithium-ion batteries can pose in commercial and industrial environments. Adrian Simmonds, interim practice leader at QBE Europe, outlines the steps employers can take to mitigate the risks



Rechargeable lithium-ion batteries were first introduced in 1991. Today, they're everywhere.

Think about how many rechargeable devices are in your home and workplace – from the fitness tracker on your wrist, cell phone and computer, to e-bikes and electric vehicles. With a growing focus on sustainability influencing many – if not all – businesses, new applications for lithium-ion batteries are being embraced, including for use in energy storage, power tools, forklifts and electric vehicles.

In normal use, lithium-ion batteries are stable and work as intended. However, these batteries are particularly sensitive to high temperatures and are inherently flammable, as well as being sensitive to cold temperatures and over-charging.

In certain circumstances – if the battery has been damaged by dropping, piercing or even heavy jolting, for example – a fault can cause a short circuit and severe overheating leading to thermal runaway: an irreversible pathway to fire.

Lithium-ion batteries can be difficult to deal with because they release a flammable and toxic vapour which helps to further fuel the fire. Fire extinguishers are available that release a water-based solution of a material called vermiculate. This seals around the damaged battery to limit further fire spread but it does not halt the thermal runaway. The thermal runaway process will continue under the vermiculate, and is waiting to accelerate again given the chance. This can reignite the fire even after hours or days or weeks of it seeming to be contained.

Any by-standers should evacuate and stay at least 10 metres away from the fire, as the explosive force of a fire and thermal runaway release can throw hot metal and burning chemicals many metres. No one should attempt to extinguish the fire unless they're trained and are using Lith-Ex extinguishers.

Ten strategies to mitigate risk

Mitigating lithium-ion fire risk can be addressed as part of emergency response plans for businesses. In addition to any contingency plans, general risk control recommendations around lithium-ion battery use and storage could include:

1. Establish a pre-defined emergency response plan to tackle damaged or overheating lithium-ion batteries. Key employees should be trained before lithium-ion batteries are permitted on site.

2. Avoid using lithium-ion batteries/ battery-powered equipment in extreme heat and freezing temperatures. Do not expose the battery to condensation, excessive humidity or water. Employees should be advised to never stack heavy objects on top of batteries or devices containing batteries.

3. Charge lithium-ion battery-powered personal mobility devices or mobile plant (such as forklift trucks and powered pallet trucks) in a fire-rated non-combustible structure, or room located outside the main building or attached to the external wall. Charging inside the main building requires a minimum four metres clearance from all combustibles and charging to be interlocked with localised or premises fire detection to shut off the power to the charger bay and raise a fire alarm.

4. Ensure all charging is completed during working hours. If battery charging is undertaken out-of-hours, additional, expensive control measures are recommended, such as dedicated fire-rated cabinets or battery charging rooms, early alert off-gas detection, and localised automatic fire suppression, such as water mist protection to contain fire spread.

5. If the battery is detachable, remove it from the equipment when it is not in use for extended periods. Lithium-ion batteries not in use must be stored in a cool, dry location, in a charged state. In industrial or vehicle workshop premises, where the state of charge can be checked or changed, the batteries should be stored at 30 per cent SoC if being kept for extended periods, and certainly no more than 50 per cent. This is because the energy in a fire situation has been found to be significantly less at around 30 per cent than if the SoC is above 50 per cent, and it makes fire-fighting much easier.

6. Segregate lithium-ion batteries from other materials if bulk-stored in a warehouse, in a non-combustible, well-ventilated structure/room with sufficient clearance between the walls and the battery stacks. There should be clearance between batteries to allow air to circulate.

7. Control floor stacking of lithium-ion batteries in designated areas with limited stack heights, footprints and separation distances. Rack storage of lithium-ion batteries should not be permitted unless the building and the racks are fully sprinklered with solid metal horizontal and vertical barriers between each storage bay (use FM DS 8-9 Scheme A with horizontal and vertical solid barriers for every bay for an internationally accepted sprinklered rack storage protection standard).

8. Use a hand-held infrared temperature gun to perform thermography inspection for any battery that has, or may have sustained damage. Any deviation from the normally expected general temperature by 3°C or more on any individual lithium-ion battery package should be reported to management immediately so the pre-defined emergency response action plan can be initiated.

9. Maintain a steel bin partially filled with water (or similar arrangements) at least three metres clear of the building, in readiness for any lithium-ion batteries with elevated temperatures to be placed into by a forklift truck. Other fire containment materials such as vermiculite or sand can be used to smother the affected battery. These measures might not stop the chemical fire from continuing but they will assist with fire containment.

10. Never open, destroy or incinerate a lithium-ion battery as it may leak or rupture, and release the ingredients they contain into the environment. Any swollen, dented or otherwise damaged batteries should be recycled or disposed of by a company qualified to do so.

Risk management services for QBE customers

QBE helps businesses build resilience through risk management and insurance.

Depending upon the size and complexity of the business needs, QBE customers can access a wide range of risk management services, self-assessment questionnaires and risk management toolkits which are focused on the key causes of claims, and on generating action plans for improved outcomes – including protecting employees, reducing risk and making claims less likely.

You can find out more about how QBE helps businesses to manage risk at: www.qbeeurope.com/risk-solutions

Adrian Simmonds, interim practice leader at QBE Europe

CIR
CONTINUITY INSURANCE & RISK

FUSION
RISK MANAGEMENT

BUSINESS CONTINUITY SOFTWARE REPORT 2024

Evolutionary vision

Artificial intelligence, remote working, and a rapidly changing business environment are all set to impact on the future direction for business continuity software, but it also marks an exciting time in the evolution of its capabilities, writes Martin Allen-Smith

Complexity can be one of the biggest dangers for any business. With regulatory demands, dramatically different post-pandemic working patterns and cultures, challenging trading conditions and a fast-moving technological environment, organisations have to harness every tool at their disposal if they are to stay on top of a multitude of constantly shifting objectives.

Business continuity software has for some time played a key role in helping to protect firms from some of the biggest threats, and it has come a long way from its humble beginnings.

"Modern business continuity software has evolved far beyond the mere task of generating a business continuity plan," explains Colin Jeffs, head of the business continuity management division at Daisy. "It has become an integral part of operational resilience, which offers a more holistic view of an organisation."

This, he says, encompasses understanding critical elements, their requirements, urgency, potential impacts across defined timelines, and the intricate web of internal and external dependencies involving suppliers, personnel, resources and systems.

"What threats are there both internally and externally that could threaten part of, or all of an organisation?" Jeffs adds. "These complex things need to be brought together cohesively so that management and executives can make sense out of the data to determine, firstly, the right course of action to take when planning for risk and outages; and secondly, to adopt the right strategies...to both protect and recover the organisation."

The working world has changed since the pandemic in many ways and, Jeffs believes, has led to organisations jumping to decisions without giving serious thought to the longer-term impacts on the business – increasing, rather than reducing risk in the process.

Now, more than ever, organisations expect software to provide answers to many of these questions – or at least provide a consolidated view of the data so that they can formulate an opinion themselves.

"Implementing such software presents a challenge: determining the planning level and the data to integrate and extract," Jeffs explains. "The inputs profoundly shape the outputs, making an experienced implementation consultant indispensable to guide the process effectively."

The ability to not just identify issues but to do so rapidly has also become increasingly important. Charlie Forsyth, chief product officer at Noggin, explains: "Business disruption has long been a matter of 'when not if', but now, it has become a matter of 'how soon'. Speed must therefore be a priority.

"This affects software implementations as it puts a premium on getting up and running quickly with best practice out-of-the-box. It also suggests that flexibility and customisation, often through no-code designer tools that allow customers to create or modify their respective workspaces without a single line of code, will be of increasing importance in software implementation as organisations are forced to pivot quickly to address the shifting risk landscape."

In the current threat landscape, global organisations are often faced with multiple simultaneous and cascading crises as well as disruptions to their business operations, meaning that they must be able to respond at a moment's notice. This demands an agile and integrated software solution that is easy to implement and that can help the organisation adapt to evolving challenges, protect itself and its customers from disruption, and enable it to resume critical operations faster than ever.

As Tracey Forbes Rice, senior vice-president at Fusion Risk Management, puts it: "The unrelenting pace of these disruptions and threats makes time to value critical when it comes to implementing business continuity software, which can be difficult in an environment where organisations are forced to do more with fewer people and smaller budgets. Being proactive, while challenging, is still possible with the right software platform that has built-in best practices and harnesses the power of proven subject matter expertise."

Paradigm shift

While organisations simply want software to take care of all aspects of the business continuity planning, when it comes down to the detail, what new functionality and innovation is shaping the way in which it can be used?

Regulatory obligations are one central plank, according to Jeffs, who says that the landscape of operational resilience has ushered in new requirements – particularly for regulated financial service entities and the critical suppliers

"Assimilating essential supplier data into a business continuity tool has become vital. Such integration ensures that pivotal supplier information is seamlessly woven into any gap analysis or planning initiatives"

to such organisations. "[Having] the capability to pinpoint important business services or products and conduct comprehensive end-to-end business impact analyses on them holds utmost significance. This empowers the creation of exhaustive upstream and downstream dependency maps, coupled with gap analysis on critical facets of these services," he explains.

Assimilating essential supplier data into a business continuity tool has become vital. Such integration ensures that pivotal supplier information is seamlessly woven into any gap analysis or planning initiatives, Jeffs adds: "The real-time nature of data gap analysis within the tool is paramount, as the ability to analyse data within the tool eliminates the need for external analysis. A tool's capacity to not only incorporate this information but also scrutinise the sufficiency of suppliers' own business continuity arrangements – think supplier due diligence – while maintaining an auditable record, is an indispensable component of any operational resilience initiative."

He adds that one of the biggest innovations over the years is the ability to deliver critical plans, contact information and data via a mobile app: "This is the cornerstone of any modern software and should be a prerequisite in any comprehensive solution."

As in many other areas of business, AI seems likely to have an increasingly significant role to play in the current and future development of business continuity software. Fusion's Rice explains: "Risk professionals are excited about new functionalities that can drive effective outcomes – such as generative AI, impactful metrics and reporting capabilities – and transform their business continuity programmes. Generative AI can help organisations simplify processes and more efficiently resolve questions, gain deeper insight into incidents, and quickly act on them while enhancing decision-making and reducing time spent on administrative tasks. Impactful metrics, coupled with advanced reporting capabilities, provide greater visibility into key business functions and can increase stakeholder confidence and buy-in."

Usability improvements are also critical, she adds, including prioritising product innovation and developing new features that help organisations build dynamic and data-driven responses that enable them to go beyond static plans to ensure preparedness in times of disruption. In essence, the software needs to be easy to use for both seasoned practitioners as well as those from outside the risk profession and should include training programmes that can be used from the top down.

Business continuity software providers have to be ready to adapt and adopt – but how is the market likely to evolve, and how can organisations use such systems to better manage emerging challenges? Noggin's Forsyth says: "The outlook for business continuity software in the next few years is incredibly positive. Unfortunately, that's because the number of potential disruptions businesses face will not only multiply but interconnect. As a result, we see the market evolving towards integrated resilience of which business continuity is one component – but not the only."

He believes that businesses are likely to use integrated resilience software to tackle emerging challenges across several inter-connected solution areas, such as business continuity, emergency management, operational risk management, crisis and incident management, and operational resilience. "Such systems will be better equipped to manage our emerging challenges as they will facilitate collaboration and stakeholder engagement, automate workflows for planning, response and recovery, as well as consolidate data to unlock insights and increase situational awareness," he adds.

"Generative AI can help simplify processes to resolve questions, gain deeper insight into incidents, and quickly act on them while enhancing decision-making and reduce the time spent on administrative tasks"

Fusion's Rice expects to see an increased focus on simplifying and automating processes. "Streamlined data integration will help effectively break down information and data silos as well as empower the shift to proactive risk management in order to increase team productivity and help mitigate crises before they cause business disruptions. Scenario testing powered by generative AI will take centre-stage across organisations of all sizes," she explains.

"Scenario testing is critical to understand, analyse and mitigate the impact of events on organisations in real time, enabling practitioners and stakeholders to make quicker data-driven decisions. We will see new solutions that leverage generative AI and allow practitioners to run thousands of scenarios in minutes to identify vulnerabilities and inform remediation practices to drive robust business continuity and resilience."

Transforming business continuity programmes in the era of AI

AI provides business continuity professionals the opportunity to drive dynamic data management, planning, and response by embedding generative AI throughout programme workflows. Cory Cowgill writes

The dramatic growth of artificial intelligence and the potential for transformation it will bring to organisations is one of the most significant paradigm shifts since the birth of the internet. The widespread accessibility for organisations to access new generative AI tools, driven by low-cost cloud computing resources, is poised to radically shift how we work and operate.

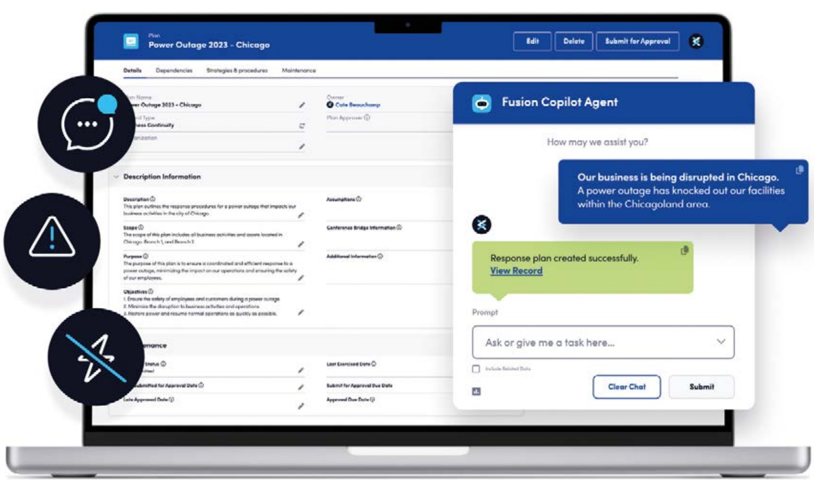
One of the more recent and most valuable innovations is the AI agent, a software that uses this new technology to assist users with various tasks or to provide information relevant to queries. This assistant is designed to understand natural language and interact with users in a way that is similar to how humans communicate. It can ask and answer questions, provide recommendations, and even perform certain actions on behalf of the user. Essentially, it acts as a virtual assistant that uses advanced AI capabilities to assist and guide users through complex processes. When applying generative AI to a business continuity programme, there are three key pillars that have the potential to drive extraordinary value.

Dynamic data and GenAI

Business continuity is uniquely situated to benefit from GenAI given the large amount of critical business process data that is trapped across static plan documents. Before GenAI agents like Fusion Resilience Copilot, it was not possible to efficiently analyse and process this data. The information embedded in the multitude of spreadsheets, PDFs, text documents, and other data repositories had to be manually and laboriously extracted and compiled before it could provide meaningful insight into the people, processes, assets and vendors that are important to an organisation.

Organisations that have hundreds of plans stored in static repositories can now rapidly unlock the value buried deep within those documents. With the power of generative AI, users can better utilise tools including reports, dashboards, and data-driven workflows to add visibility and agility into any programme.

The ability for AI to unlock value through data extends to every aspect of a programme, and assessing business processes and how they may be affected by performing a business impact analysis is one of the most prominent examples. The BIA has been a significant and time-consuming data-gathering exercise across organisations of all sizes for decades and has historically presented fundamental challenges around data quality. Subject matter experts within the organisation that contribute to a BIA typically approach the exercise as a cumbersome



compliance check and something that must be completed so the business continuity programme owner will move on to the next task. This often impacts data quality because the time, energy and thoughtfulness needed to gather the data simply isn't being spent by the contributor. The result is that business continuity programme owners must then spend more time with their BIA SMEs, walking them through the exercise to ensure all questions within the assessment are answered appropriately. GenAI can address the operational inefficiencies and data quality issues that are presented by BIAs by providing an expert GenAI programme manager within the process. With a built-in analyst, powered by AI, the tool can now act as a trusted advisor to the SME and ensure the data is accurate in real time by using best practise-based continuity data that the GenAI tool has been specifically trained on, providing insights and recommendations that were once not so easily available.

The challenge of ensuring timeliness and accuracy of data within a programme is one that many continuity professionals wrestle with. While BIAs can provide important data, this data is often a point-in-time snapshot of the continuity plan. In one BIA cycle, key employees come and go, systems are migrated or retired, critical vendors are onboarded and offboarded, facilities or stores have changed, and business priorities may have shifted. Business continuity programme owners want to ensure the data they are working with can be trusted. GenAI can improve data accuracy by integrating real-time data sources, like HR system records, and prompt for updates where appropriate, like notifying the user when a process owner leaves the organisation. A semi-autonomous data quality and integration assistant powered by GenAI can assist in both integrating systems as well as providing data quality analysis.

Dynamic planning and GenAI

Leveraging a strong information foundation provides continuity professionals with the ability to drive effective responses through data-driven approaches. Traditional static plans have focused on a specific application, scenario or all-hazards planning approach. GenAI provides the ability to take information and make it into an actionable response. As an example, Fusion Resilience Copilot acts as a semi-autonomous agent, taking a prompt from the BC owner to assemble a response plan based on a plain language statement summarising the active situation. The agent combines a best practise data set, a fine-tuned model specific to continuity planning tasks, the business continuity owner's ask, and the organisation's assets that have been identified in their information foundation to automatically generate a draft response tailored to the impact.

Dynamic response with generative AI is providing immediate value to Fusion's incident response team. Fusion Resilience Copilot is saving our resilience team 1-3 hours per day per incident response with greater data accuracy. For example, during live incidents, Fusion's Incident Commander is using it to generate executive summaries and updates that go out to our executive leadership team. In addition to the timeliness of the updates, our leadership team has found the quality of these communications to be vastly improved, as Fusion Resilience Copilot, working with the Incident Commander, can rapidly massage the communication update to speak in language that a non-risk stakeholder can understand. For example, in the update, instead of stating objectives being met with RTO or RPO values, Fusion Resilience Copilot would naturally weave the narrative of the response objective without confusing acronyms and 'continuity-speak'. Fusion Resilience Copilot also reviews procedures and steps that have been planned and executed to provide real-time assessments and recommended improvements to incident response plans.

Data-driven executive reporting

The need for quickly delivered, comprehensive after-action reports is another area where GenAI offers significant response improvement. What once took our team a week or more of calendar time can now be done in less than a day. Fusion Resilience Copilot analyses the incident data, leverages custom data sets that include almost two decades of proprietary best practises for incident response and after-action reporting, and synthesises a draft of an after-action report for the BC programme manager to leverage. Multiple meetings with various stakeholders are streamlined with the AI-powered analyst's assistance to quickly provide an impactful after-action report with identified areas of improvement.

Fusion has found that leveraging GenAI across our continuity programme has already greatly improved our resilience posture. By applying GenAI to dynamic data management, planning and response, we have raised the operational efficiency of our programme and provided management with increased confidence in our organisation's operational resilience initiatives.

Cory Cowgill is chief technology officer at Fusion Risk Management

FUSION FRAMEWORK SYSTEM
FUSION RISK MANAGEMENT

In a world of cascading crises and ever-changing disruption, having a true understanding of how your business works is crucial in limiting disruption for your customers. The Fusion Framework System is the platform on which Fusion Risk Management helps organisations build comprehensive and dynamic business continuity programmes.

Get a clear picture of your organisational risk posture

Fusion offers an intuitive and integrated platform where you can see how your business works and how it can bend but not break when faced with challenges.

The Fusion Framework System breaks down the barriers that create the need for separate applications across business continuity, disaster recovery and crisis and incident management, allowing continuity programme managers to get a complete understanding of their organisation. Fusion provides a standard framework that inherently integrates your data across all disciplines, making it easy to analyse your complete programme through one single pane of glass.

The framework's integrated continuity capabilities help users intuitively build and execute plans, and run risk and impact assessments while seamlessly evaluating organisational preparedness and response.

Prepare for anything because you can't plan for everything

The Fusion governance and management component offers configurable reference data taxonomies, libraries and scoring methodologies as well as customisable workflows, approvals and notifications to automate administrative tasks. A predictive risk analytics component features tolerance-based metrics and configurable thresholds that drive automated notifications, alerts and reports – all from a single, integrated dashboard.

In a post-pandemic world, it's no longer acceptable for customers to experience extended disruption in the delivery of goods and services. To mitigate the potential for disruption, Fusion users can run through thousands of simulations and plausible events to uncover potential weak spots and vulnerabilities, which, when coupled with the ability to dynamically create response plans, ensures that your organisation is prepared for when the inevitable happens. The Fusion Framework System allows users to address these potential problems before they even occur. The platform helps organisations better anticipate, prevent, prepare for, simulate, respond to, and learn from the risks and events that continue to threaten disruption of important services and products.

Build the power of AI into your continuity programme framework

The latest addition to the Fusion Framework System's list of capabilities include its AI-powered assistant Resilience Copilot, which operationalises Fusion expertise to create an advisor within the system. Resolve questions, gain deeper insight into incidents, and quickly act on information from directly within your integrated dashboard. Resilience Copilot offers outputs like identifying gaps in your risk posture, recommending best practice improvements, and generating executive summaries to drive support from senior leadership cross-functionally within an organisation.

Built on the Salesforce Lightning Platform, the way in which Fusion works with organisations is simple: the Fusion Framework System helps organisations navigate fast-moving change by mapping how they deliver important services and products to customers, forecasting how those value chains are at risk of breaking, and helping them manage the risks and events that cause disruption.

Fusion has been helping organisations deliver comprehensive continuity programmes for nearly 20 years.

For more information about the Fusion Framework System visit fusionrm.com or call:
+1 224 571 0050 (US)
+44 (0)7379 829814 (UK)

BC IN THE CLOUD
INFINITE BLUE

BC in the Cloud was designed to automate and streamline business continuity and disaster recovery programmes.

US-based provider Infinite Blue bills this tool as a "single, comprehensive solution that empowers organisations to mitigate risks, assess impact and prepare, manage and recover from incidents".

infiniteblue.com

BCP BUILDER
MINERVA CORPORATION

BCP Builder is a user-friendly, online business continuity planning template designed to empower small and medium-sized companies with the essential tools they need to create their own comprehensive business continuity plan.

Key features of the tool include guided templates with step-by-step guidance through a structured template, ensuring that users cover all critical aspects of a plan.

Plans can be customised to the unique needs of the organisation, reflecting specific risks and resources.

Risk assessment can be carried out with the tool to identify potential threats and vulnerabilities that could impact operations, from natural disasters to cyber attacks.

Recovery options can be explored, and strategies developed to minimise downtime and financial losses. Communication plans can be developed with this tool to ensure that employees, clients and stakeholders stay informed during a crisis with a well-defined communication strategy, while the resources required for each recovery strategy can be clearly defined.

BCP Builder emphasises the importance of regularly assessing the plan's effectiveness through drills and simulations.

A simple approach to documentation and maintenance helps users keep plans up-to-date, to reflect changes in the organisation and evolving risks.

bcpbuilder.com

CENARI
INFINITE BLUE

Cenari is Infinite Blue's first fully integrated, intelligent enterprise resilience solution, which was designed to help companies synchronise incident planning, mass notification, threat intelligence and organisation-wide responses.

infiniteblue.com

CLDIGITAL

CLDIGITAL 360
CLDIGITAL

CLDigital 360 is a comprehensive no-code business management platform engineered to unify enterprise risk, resilience and performance.

This platform aims to modernise enterprise risk management, operational resilience, business continuity, technology recovery, organisational resilience and crisis management, while eliminating data silos and onboarding and user adoption friction.

The CLDigital Enterprise Risk Management solution delivers a robust framework for identifying, assessing and managing risks across the enterprise.

CLDigital 360 Operational Resilience supports FCA, DORA and other operational resilience requirements by identifying important business services, setting and monitoring impact tolerances, and mapping these to relevant processes, technology, third parties and data with ease.

The CLDigital 360 Technology Recovery and Business Continuity solutions promise to ensure user organisations remain agile and functional, minimising downtime and seamless recovery from disruptions and significant outages.

With CLDigital Crisis Management, users can respond to and manage crises quickly and effectively with Microsoft Teams, Everbridge, Twilio and other collaboration and messaging platform integrations.

CLDigital 360 was built on three foundational pillars: no-code, business process management and data-centricity. No-code accelerates solution development, promoting operational agility that aligns with a dynamic pace of change. CLDigital's business process management engine orchestrates complex processes and critical workflows, reducing operational bottlenecks and swiftly responding to crises and operational disruptions.
This data-centric platform aims to

deliver real-time insights and actionable intelligence through user-friendly, customisable visualisations and dashboards, empowering informed decision-making.

CLDigital 360 offers built-in data management services, business intelligence capabilities and over 100 connectors to enhance operational readiness across all modern business environments. CLDigital 360 supports cloud and on-premise deployment models to support diverse organisational infrastructures.

For government clients, the CLDigital FedRAMP Cloud promises a secure, compliant environment that meets stringent federal requirements.

cldigital.com

4C STRATEGIES

EXONAUT BCM SOFTWARE
4C STRATEGIES

Exonaut BCM Software is a customisable, end-to-end solution for maintaining operational resilience and ensuring effective recovery during a business outage. Developed with practicing resilience experts and used in over 100 countries, the tool promises to help users digitalise, scale and integrate their entire business continuity and resilience programme.

This tool connects business and IT continuity plans, risk assessments, disaster recovery plans, crisis management and capability development in one system to ensure resilience teams can act quickly, communicate decisions and reach objectives more effectively.

4C Strategies highlights this product's ability to map, view, filter, analyse, prioritise, develop and visualise critical processes, activities, resources and their tolerances and dependencies in a powerful real-time BIA mapping tool with smart filtering capabilities.

This tool also integrates with third-party service management systems and configuration management databases to connect with the digital landscape. Custom reports can be autogenerated and real-time dashboards provide situational awareness on continuity plan status and risk exposure.

Exonaut BCM Software is used by organisations and armed forces globally to test capabilities, identify gaps and train to improve. Desktop scenario exercises can be created, run, logged and analysed as part of a continuous cycle of improvement.

4C Strategies can also provide consultants to manage training and exercise programmes.

4cstrategies.com

INONI ESSENTIALS
INONI

Inoni Essentials is a business continuity and resilience management solution for SMEs that require a best practice and standards-aligned management system. The service provides a simple to implement and maintain programme, minimising the need for in-house administration, expertise and resources.

Essentials is a cloud-hosted software service that includes full consulting implementation, getting users to a best practice position quickly, and with minimum disruption. It aims to deliver practical, standards-aligned business continuity plans, addressing all business continuity-threatening scenarios for all in-scope departments and sites.

Inoni's standard delivery model provides easily accessible documents that download to PDF and Word or can be viewed from a user's mobile phone; as well as dependency mapping functionality, user-configurable dashboards and a card system providing focused scenario and role responses.

Inoni's consultants will support users with the implementation through software set-up, discovery workshops, production and delivery of standards-aligned documents, system walkthrough and business continuity manager support.

An advanced delivery model extends Essentials' mapping and reporting functions to provide operational resilience and supply chain continuity capability.

inoni.co.uk

NOGGIN RESILIENCE
NOGGIN

The Noggin Resilience "integrated resilience workspace" was designed to unify operational risk management, operational resilience, business continuity management, and crisis and incident management activities, as well as security operations. This tool is designed to connect the people, processes and tools required for organisations to enhance operational resilience, so they can minimise the impact of disruptions and still deliver critical products and services to

meet obligations to customers and stakeholders.

Noggin aims to simplify business continuity by unifying all activities and data from business impact analyses, dependency mapping, exercises and recovery strategies within an integrated resilience workspace to enable streamlined and centralised management of the entire business continuity programme.

With this tool, Noggin promises to simplify the BIA process and drive engagement from stakeholders, using a built-in BIA tool that guides users through the process step-by-step, ensuring BIAs are rich with insightful data.

The software aims helps users apply a consistent recovery approach that defines strategies, response plans, roles and responsibilities and pre-assigned checklists. These it promises to deploy in seconds when disruption hits, to ensure the best response. The tool can also automatically suggest which plans to activate based on location and assets impacted.

Noggin Resilience will also help users manage exercises and be confident that teams are prepared to handle any situation.

Noggin's data analysis and visualisation tools can help users monitor and evaluate critical metrics, and tailor reports with customisable print templates, ensuring the delivery of valuable information. The tool's mapping functionality also helps users to gain a comprehensive visual understanding of assets within the organisation, and their relationship to events. Users can monitor and respond to threats and risks to people, assets and reputation, with real-time, actionable intelligence.

Noggins helps users identify emerging threats and impacted people and locations, communicate with stakeholders and escalate into full incident management. Messaging and emergency notification features help facilitate communication channels including email, SMS, voice and app notifications, based on event impact, location or any other factor.

Noggin can be integrated with existing technology stacks through its range of integration options, helping users to connect and synchronise data via import, export and API capabilities. It offers a consistent interface across desktop, tablet and mobile, each with their own familiar apps.

noggin.io

PARASOLUTION
PREMIERCONTINUUM

ParaSolution is a business continuity management solution that has been helping organisations increase their resilience for two decades. This tool has been developed to help organisations effectively manage risks, crisis plans and continuity programmes, enabling them to meet compliance and governance standards, including ISO 22301 and ISO 27001.

Developed by Premier Continuum's experts and certified BCI trainers, ParaSolution addresses the entire business continuity management lifecycle, including BIA, risk assessment, IT disaster recovery, plan development and activation, exercises and crisis and incident management. The tool promises intuitive user pathways, promoting all contributors' engagement in the resilience process.

Solutions modules include business continuity, operational resilience, IT disaster recovery, integrated risk management, crisis management and emergency notification system and vendor risk management.

Each module features easy to capture forms, roll ups and dashboards that provide current state of readiness and requirements; while gap reports support informed decision-making.

ParaSolution offers advanced features, such as bi-directional data connectivity, linking the tool to multiple data sources within the client's organisation and making processed information available in data analysis and reporting tools. This tool also features a notification component with the capability to reach internal and external stakeholders via voice, SMS and email.

This tool can be configured according to the strategic objectives, culture, language and structure of the user organisation, and is used by hundreds of consultants and trainers globally, in financial services, energy, technology, manufacturing and the public sector.

ParaSolution is available online and through a mobile app, continuously enhanced in-house. It features four levels of support. Support is available 24/7/365 in English and French.

premiercontinuum.com

PDRWEB
SERVICES CONSEILS RDI

PDRWEB can be tailored to suit a range of users, from SMEs to large multinational organisations. It features a dashboard showing the status of different plans, BIA progress, plan maintenance and status, message centre, logged in users and completed activities.

This tool has a web-based customised survey form, which, once completed, will automatically establish RTOs using customised weight factors and activity dependencies. Reports are then generated by site departments. Upon review and acceptance of all reports, PDRWEB automatically creates different business continuity and disaster recovery plans. During the creation of plans, the product links the different activities using prerequisites and a decision tree. The software also links the required resources to activities. It can also link multiple plans and produce dependency mapping.

Users can also opt to receive automated alerts that notify them of their respective activities, providing all the information required for the execution of the task, including resources, contact information and diagrams. PDRWEB uses advanced AI-generated encryption. Services Conseils also offers an integrated notification module.

rdiinc.ca

RISKONNECT BUSINESS CONTINUITY AND RESILIENCE RISKONNECT

Riskonnect Business Continuity and Resilience software helps users prepare for threats and minimise disruption to operations, with the goal of replacing uncertainty with confidence. Built from decades of experience and in alignment with ISO 22301, Riskonnect uses SaaS-based automation and intelligence to address operational resilience, business continuity, crisis management, threat intelligence and emergency notification in one platform.

The solution's straightforward user interface promotes engagement and consistent programme execution. It is accessible to even the casual user with no need for extensive, recurring training or a dedicated administrator.

Key features include a business model definition tool, through which users can create a consolidated data model – from supplier to customer – enabling preparedness and timely response. An operational resilience module helps users identify their most critical products and services and define impact tolerance while linking to the end-to-end value chain. BIA and risk assessment tools help users establish requirements, document dependencies, and highlight vulnerabilities.

Users can also establish strategies to achieve continuity and decrease disruptions. The built-in crisis management and emergency notification capabilities help users quickly turn plans into actionable checklists, mobilise response teams and communicate with employees, contractors and partners in real-time.

The solution also supports exercising, AI-powered threat intelligence, dashboard-style reporting, gap and 'what if' analysis, situation reporting, workflows, API integration and compliance with policies, SLAs, regulatory requirements and standards. The mobile app connects users to their business continuity programme, critical plans and documents, even when off-network or on-the-go.
Users can access the solution in a wide range of languages, and receive support by customer service teams 24/7/365, globally.

riskonnect.com

SHADOW-PLANNER DAISY CORPORATE SERVICES

SHADOW PLANNER

Deployed by SMEs and enterprise customers alike, Shadow-Planner is a SaaS-delivered modular based business continuity and operational resilience management tool.

This tool has been designed by industry practitioners, specifically to make easy work of managing business continuity and operational resilience programmes of any size.

Encompassing modules such as business impact analysis, strategy, planning and reporting, exercising, contacts and contact groups and incorporating a powerful records library, mobile app and imports and exports functionality, Shadow-Planner has been specifically designed to follow and enable best practice. The BIA module features powerful dependency mapping capabilities that combine to provide a graphical dependency map showing upstream and downstream dependencies, along with coloured real time data gap analysis. In addition, the tool can clearly track and identify areas of the business that are supporting important business services or products.

A graphical dependency map tool allows users to query any record to see what its upstream and downstream dependencies are at the click of a button, along with the risk areas. BIA data is automatically transferred to the strategy module, enabling users to define the strategies for recovering critical dependencies such as IT systems, processes, locations and suppliers; and to define both high level strategies for total loss of IT systems or staff; or more detailed level strategies by process or IT systems.

Almost any data from within Shadow-Planner can be used in the planning and reporting module. Building plans and reports is designed to be as simple as possible. The exercise module is designed to do everything a business continuity professional of today would expect from planning the exercise, establishing mandatory and non-mandatory objectives, scope, success criteria, participants and roles and responsibilities, to capturing issues, observations and actions during the exercise, and creating a consolidated view of the exercise and its outcomes.

If an incident was to occur, then Shadow-Planner's own mass communication module allows business continuity and crisis managers to send out emergency communications via two-way email and SMS using either pre-defined messages or those created at the time of an incident. In addition, a mobile app puts critical information, such as playbooks and emergency contact information, in the hands of those that need it.

daisyuk.tech

SHIELD
KINGSBRIDGE BCP

KingsBridge's Shield business continuity planning software was designed by business continuity professionals to provide a simple and secure SaaS tool. With more than 30 years' history, Shield is designed to ensure a smooth workflow as users' business continuity plans mature, and are invoked. Shield Silver is designed for SMEs with less than 100 employees. Shield Gold is designed for businesses with up to 1,000 employees; while for organisations with more than 1,000 employees, Shield Platinum is the provider's recommended option.

kingsbridgebcp.com

Business Continuity Software Report
Supplier Directory


Great Leaders See
Risk Differently

4C STRATEGIES

4C Strategies
Nova North, 11 Bressenden Place
London SW1E 5BY

Tel: + 44 (0) 203 318 2706

info@4cstrategies.com
www.4cstrategies.com

Linkedin: www.linkedin.com/company/4c-strategies/
Twitter: twitter.com/4c_strategies
YouTube: www.youtube.com/@4cstrategies523

Exonaut Business Continuity Management is a customizable, end-to-end solution for maintaining operational resilience and ensuring effective recovery during a business outage. Used in over 100 counties by leading organizations, it enables you to digitalize, scale, and integrate the entire business continuity program.

Develop, test and activate continuity plans and connect risk assessments, disaster recovery plans, crisis management, and capability development in one system. Utilize the powerful BIA tool to map, view, dynamically filter, analyze, prioritize, and visualize critical processes, activities, resources, and their tolerances and dependencies.

Connect your digital landscape by integrating third-party services. Gain a strategic advantage in disruptions with data-driven insights and intuitive dashboards providing situational awareness on continuity plan status and risk exposure. Streamline processes and save on resources with automated workflows, functions and report creation. Ensure resiliency teams can act quickly, communicate decisions, and reach objectives more effectively.

CLDIGITAL

CLDigital
55 Lane Road, Fairfield NJ 07004

Support: +44 (0)20 7770 6446
info@cldigital.com
cldigital.com/risk-leadership
Linkedin: www.linkedin.com/company/cldigital-software

CLDigital 360 is a no-code business management platform engineered to unify enterprise risk, resilience, and performance management. Designed to meet the high standards of modern enterprises and dismantle silos, CLDigital provides an advanced ERM solution for comprehensive risk identification, assessment, and management. Its operational resilience solution ensures compliance with regulatory standards that include FCA and DORA, enabling organizations to define and monitor Important Business Services (IBS) and their impact tolerances. The technology recovery and business continuity capabilities of CLDigital 360 ensure organizational agility and automate the BIA and plan development process. The crisis management solution integrates with Microsoft Teams, Everbridge, Twilio, and others, enhancing collaborative response capabilities to facilitate recovery from disruptive events.

The CLDigital 360 platform includes an intuitive, drag-and-drop solution builder, workflow, rules engine, BI, reporting, and data management, and it supports cloud and on-premises deployments. Services include current state assessment, program design, implementation, migration, data, and BI development.

SHADOW PLANNER

Daisy
20 Lindred Rd, Brierfield, Nelson BB9 5SR

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@daisyuk.tech
www.shadow-planner.com
Linkedin: www.linkedin.com/showcase/daisycorporate-services
Twitter: twitter.com/Daisy_Corporate

Shadow-Planner from Daisy is a multi-award-winning business continuity management software tool, with an award-winning, mobile app to drive business continuity planning for the digital age.

Daisy's Shadow-Planner enables you to map out your critical dependencies (including important business services), understand any gaps in capabilities, create plans, manage testing, and manage and monitor your business continuity/resilience programme.
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 resilience commitments efficiently and cost effectively. Designed by BC practitioners for BC practitioners, this suite of integrated software supports the entire business continuity management lifecycle: from impact analysis through developing strategies and plans to testing, reporting and even mass communications.

Shadow-Planner is based on the BCI's Good Practice Guidelines and currently covers the following modules:

- Business Impact Analysis (BIA)
- Strategy
- Business Continuity Planning
- Testing & Exercising
- Programme Management
- Mobile Application

daisy.

SHADOW PLANNER

SCAN TO FIND OUT MORE

Multi-Award Winning
Business Continuity Management Software

At Daisy, our BCI certified practitioners understand the importance of maintaining operational and cyber resilience in today's interconnected and rapidly evolving digital landscape. Shadow-Planner is designed to help organisations effectively manage operational or cyber disruptions, enabling them to stay resilient and keep their business operational. By leveraging the capabilities of our planning tool, businesses can develop robust plans, assess potential risks, and establish proactive strategies to mitigate the impact of disruptions.

Programme Management

Gain insights into the status of your programme in relation to policy compliance. Monitor updates, upcoming deadlines, and areas that require attention.

BIA

Define your important business services and comprehensively map their critical dependencies both upstream and downstream.

Strategy

Define your recovery strategies for important business services, critical business areas, product, suppliers, IT services, locations and any other factors.

Planning & Reporting

Create step by step playbooks, integrate system data such as BIA, strategies and more into your BC plan, and generate program reports for enhanced visibility and analysis.

Exercising

Develop your testing and exercising programme, define scope, objectives and capture outcomes and actions for thorough evaluation.

Contacts & Contact Groups

Efficiently manage staff contact information and establish emergency contact groups with assigned roles and responsibilities.

Records Library

Establish a comprehensive library containing essential information about your business areas, IT services, suppliers, resources, locations and more.

Admin

Access an administration area that allows you to configure policies, set timescales, define risk levels and more.

Import

Establish and configure scheduled import profiles to seamlessly import data, such as contacts, on a regular basis.

www.shadow-planner.com

	Fusion Framework System	BC in the Cloud	BCP Builder	Cenari	CLDigital 360	Exonaut BCM Software	Inoni Essentials
Plan navigator	•	•	•		•	•	•
Dependency mapping	•	•	•	•	•	•	•
Graphical call list		•	•		•	•	•
Location resource manager	•	•	•	•	•	•	•
Recovery site layout planning			•		•		•
Reports – preformatted	•	•		•	•	•	•
Reports – own build	•	•	•		•	•	•
Process modelling capabilities		•		•	•	•	•
Technology modelling		•		•	•	•	•
'What if' analysis	•	•		•	•	•	•
Data collector	•	•		•	•	•	•
Automatic analysis	•	•		•	•	•	•
Simulation capability	•	•		•	•	•	•
Dynamic updating from database	•	•		•	•	•	•
Education and training	•	•		•	•	•	•
Test and exercise	•	•		•	•	•	•
Test scripting	•	•		•	•	•	•
Dynamic incident management	•	•		•	•	•	•
Dynamic question setting/reviews	•				•	•	•
RTO/RPO desired/actual analysis	•	•		•	•	•	•
Standards compliance	•	•			•	•	•
Integrates with GIS mapping	•	•		•	•	•	•
Workflow management with email alerts and reporting	•	•		•	•		•
Multi-language capability – interface	•	•			•	•	
Multi-language capability – user data	•				•		•
User roles and groups	•	•		•	•	•	•
Document update management	•	•	•		•		•
Comprehensive audit trails	•	•		•	•	•	•
Mobile device support	•	•		•	•	•	•
Templates available	•	•	•	•	•	•	•
Change control and tracking	•	•		•	•	•	•
Screen customisation	•	•			•	•	•
Help	•	•		•	•	•	•
24/7 live support					•	•	
Internal search engine	•	•			•	•	•
Charts, reports, graphs	•	•		•	•	•	•
Filters	•	•		•	•	•	•
Personal filter	•	•		•	•	•	•
Drag and drop	•	•	•	•	•	•	•
Mobile app for offline viewing	•	•			•	•	•
Integrates with EMN software	•	•		•	•	•	
Published APIs for data interface	•	•		•	•	•	
Remote hosting		•			•	•	•
SaaS option	•	•	•	•	•	•	•

Noggin Resilience	ParaSolution	PDRWEB	Riskonnect Business Continuity & Resilience	Shadow-Planner	Shield	
•	•	•	•	•	•	Plan navigator
•	•	•	•	•	•	Dependency mapping
	•	•				Graphical call list
•	•	•	•	•	•	Location resource manager
	•	•	•			Recovery site layout planning
•	•	•	•	•	•	Reports – preformatted
•	•	•	•	•	•	Reports – own build
	•	•	•	•		Process modelling capabilities
	•	•	•	•		Technology modelling
	•	•	•	•		'What if' analysis
•	•	•	•	•	•	Data collector
•	•	•		•	•	Automatic analysis
	•	•				Simulation capability
•	•	•	•	•	•	Dynamic updating from database
•	•	•	•	•	•	Education and training
•	•	•	•	•	•	Test and exercise
	•	•	•	•		Test scripting
•	•	•	•			Dynamic incident management
	•	•	•		•	Dynamic question setting/reviews
•	•	•	•	•	•	RTO/RPO desired/actual analysis
•	•	•	•	•	•	Standards compliance
•	•	•			•	Integrates with GIS mapping
•	•	•	•	•	•	Workflow management with email alerts and reporting
•	•	•	•	•	•	Multi-language capability – interface
•	•	•			•	Multi-language capability – user data
•	•	•	•	•	•	User roles and groups
•	•	•		•	•	Document update management
•	•	•	•	•	•	Comprehensive audit trails
•	•	•	•	•	•	Mobile device support
•	•	•	•	•	•	Templates available
•	•	•	•	•	•	Change control and tracking
•	•	•	•	•		Screen customisation
•	•	•	•	•	•	Help
•	•	•	•			24/7 live support
•	•	•	•	•		Internal search engine
•	•	•	•	•	•	Charts, reports, graphs
•	•	•	•	•	•	Filters
•	•	•	•	•	•	Personal filter
•	•		•	•	•	Drag and drop
•	•		•	•	•	Mobile app for offline viewing
•	•	•	•	•		Integrates with EMN software
•	•	•	•	•		Published APIs for data interface
	•	•		•	•	Remote hosting
•	•	•	•	•	•	SaaS option

Industry views

Dr Matthew Connell is director of policy and public relations at the Chartered Insurance Institute

In association with

Chartered Insurance Institute
Standards. Professionalism. Trust.

The Government's AI summit at Bletchley Park put artificial intelligence at the top of the agenda recently, with the summit's declaration listing regulation as one of the 'critically important' factors needed for it to 'transform and enhance human well-being, peace and prosperity'.

The truth is, AI already is regulated in many ways, but not always directly. Take insurance, for example. AI is already being used in a wide range of activities, from calculating premiums to processing claims and identifying fraud. None of these actions are controlled by an AI-specific regulator, but they don't need to be.

Underwriting decisions, for example, are already regulated by the Equality Act 2010, which forbids discrimination on the basis of ethnicity and gender, and only allows exemptions based on age and disability when underwriters can show that their risk assessments are based on sound information.

The Financial Conduct Authority has emphasised the role the Consumer Duty will play in underpinning the Equality Act, saying it requires firms to "monitor whether any group of retail customers is experiencing different outcomes than other customers and take appropriate action where they do".

The use of data to educate machines to make decisions about fraud or claims is also regulated. The General Data Protection Regulation and the Data Protection Act 2018 already require firms to use data responsibly, and the Consumer Duty requires firms to "regularly monitor the customer support they provide to make sure there are no systemic issues that create unreasonable barriers or costs for customers".

So, while it is important for politicians to ensure that there is a consistent international approach to AI policy, for firms that want to be known for being responsible innovators, standards of good practice are already clear: establishing clear, auditable processes, being alive to the potential of bias, and operating in a culture of continuous improvement in which ethical humans are always in control.

The innovators at Bletchley Park did not wait for governments to tell them precisely how to do their job. Nor should professionals working with AI.

Stephen Sidebottom is chairman of the Institute of Risk Management

In association with

irm

Imagine corporate governance as the guiding star for a company's ship. When this guiding light flickers, it's like sailing into a storm. This system of rules, processes and practices directs and controls how things work, and is crucial for maintaining trust and confidence, as well as being the bedrock of effective enterprise risk management.

Governance can make or break an organisation, and the consequences of failure can be significant. Despite this many organisations operate under the illusion that their governance works. I've been around long enough to remember the shock of the Enron scandal when a once respected energy company filed for bankruptcy in 2001 – the largest bankruptcy in US history at the time. The company's executives manipulated financial statements to hide massive debts and losses. Failure of oversight by the board and external auditors left this practice unchecked and led to the swift collapse of Arthur Andersen – then one of the world's largest audit and consultancy practices.

In the following year, 2002, WorldCom, a telecommunications giant, experienced a catastrophic governance failure and filed for bankruptcy due to an accounting scandal involving billions of dollars in fraudulent earnings. Internal control failures and the board's apparent inability to ask the right questions played a significant role and demonstrated the illusion of control provided by an ineffective audit committee.

More recently Volkswagen admitted cheating on emission tests for diesel vehicles. The company's corporate governance structure allowed this behavior to persist, highlighting the importance of ethical leadership, risk management, and a corporate culture that values integrity. Wells Fargo hit the headlines in 2016 when it was discovered that its employees had opened millions of fake accounts in customers' names. The root of the debacle? Weak internal checks and the relentless pressure on staff to meet sales targets. It ended in an expensive disaster for the bank.

Boeing faced one of the most notable aviation crises of the century when two 737 MAX planes tragically crashed in 2019. The culprit was a faulty MCAS system, but behind that lay a

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

corporate culture that prioritised profit over safety. Boeing's reputation nosedived. Finally, remember that the Red Cross, a name we all trust, recently faced scrutiny for its handling of funds raised for disaster relief. Allegations of mismanagement and a lack of transparency rocked the organisation. Charitable sector governance flaws can shake donors' trust and impact the very people they aim to help.

So why does this happen? There are several common themes about failures of governance oversight. These include missing red flags, group think, focusing on the wrong things, or even some version of willful blindness. Misdeeds go unnoticed or ignored. Safety issues escape attention. Checks and balances fail. Wells Fargo's aggressive sales targets and Boeing's race to outdo the competition prioritised short-term results over sustainable performance. In many organisations, including some charities, the belief in the virtue of the people, organisation, or mission can create blind spots about risks and culture.

Failures in corporate governance have far-reaching consequences, including financial ruin, reputation damage, legal issues and erosion of stakeholder trust. These cases emphasise the need for a deep understanding of the key risks associated with ineffective governance, and focus on creating cultures based on transparency, accountability and ethical leadership.

Editorial credit: diamant24 / Shutterstock.com

Giorgio Grasso is leader of GILC's Cyber Special Interest Group and a partner at BTG Legal

In association with

GLOBAL INSURANCE LAW CONNECT

Growing consumerism, the globalisation of supply chains, the emergence of new technologies, and the need to innovate are driving an increase in product liability claims around the world.

In particular, electronics, software and digital devices are now subject to a wider range of claims, including those involving cyber security and data privacy.

The emergence of new technological platforms and tools, such as artificial intelligence, and their increasing integration into daily life – both at home and at work – has presented issues for legislators and regulators alike.

Despite the recent spike in interest in AI, this exciting sphere is still poorly understood; and, although technology and data protection legislation is becoming more common globally, regulations that are specific to AI are still a work in progress.

Given how quickly AI technologies have become commonplace, product liability concerns for the companies that make and sell AI-powered technology seem likely to arise in the very near future.

The scope of claims in many industries, not least in the technology-driven sectors, can be expected to increase considerably as a result of the proposed changes to the European Union's Product Liability Directive. The directive, as it currently stands, imposes effectively strict liability on manufacturers for defective products that cause physical harm to consumers. However, due to complex nature of AI and the blurring of lines between products and services, its role has been a challenge to establish. If the EU directive is passed, it would ensure the definition of AI as a product that the hardware or software producer is accountable for, while easing the burden of proof placed on claimants for damage it has caused.

In this rapidly evolving market, insurers in my own country, Italy, and around the world will need to be alert to new exposures and opportunities alike.

See the next issue of *CIR Magazine* for more on the European Union's Artificial Intelligence Act.

AI and data rise on list of top risk concerns

For the first time, artificial intelligence and data risks feature not only in the top 10 areas for concern for UK risk experts, but also amongst the general public, according to a new report. CIR takes a look at the headline findings

Risks relating to artificial intelligence and data feature in the top 10 areas of concern for both UK experts and the general public for the first time, according to a new report. The research, conducted by Axa, also suggests that members of the public in the UK are more worried about the impact of AI than their European counterparts, who do not rank it amongst of their top 10 concerns.

UK experts and the public also ranked cyber risks in their top three, alongside those surveyed in America, Asia-Pacific and the Middle East.

From a list of potential risks that could impact the world over the next 10 years, risks related to AI and big data were ranked fifth by UK experts and 10th by the UK's general population. The report highlights general concerns about technology, with the top four rapidly emerging risks all focused on this topic. In the UK, half of those questioned believe that technological advances create more risks than they solve.

UK experts and the public both ranked climate change as the most significant risk for the third year in a row. Globally, both groups agreed that climate change has the potential to have the biggest impact on society in the next five to 10 years.

The findings are revealed in this year's Axa Future Risks Report, the 10th edition of the global study measuring and ranking changes in the perception of emerging risks via a survey of more than 3,200 risk experts and 15,000 members of the public.

In the UK, 86% of those questioned believe there is risk of a cyber attack that would cripple the UK, with 79% concerned about the risk of them personally suffering from identity theft, bank account fraud or social media hacking. Experts are equally concerned about cyber risks, with 96% believing there is risk of a cyber attack in the UK.

Looking to the future

The findings also show that UK experts (70%) and the general public (74%) believe that individuals, economies and society have what it takes to manage future risks. When it comes to the insurance industry, three-quarters (77%) of the UK general public believe insurers will play an important role in limiting future risks, alongside 93% of UK experts.

Tara Foley, CEO at Axa UK, said: "With the rapid evolution of disruptive technologies and the digitisation of our daily lives, it's perhaps no surprise that people are increasingly concerned about risks related to artificial intelligence and cyber security. It's also worrying to see so many people feeling more vulnerable and a continuing lack of confidence in the authorities to manage these types of future risks, and we renew our call on the government to mirror Labour's recent announcement and create a taskforce to focus on these issues.

"More positively, the report confirms that people do recognise the important safety net that insurance provides and demonstrates the essential role the sector plays in providing risk management advice and solutions. This gives the industry a great foundation to build on in coordination with other organisations to help mitigate these risks and provide reassurance to those who are concerned about an uncertain future."

Axa's *Future Risks Report* was produced in partnership with research institute IPSOS.

BUSINESS CONTINUITY SOFTWARE

Fusion Risk Management
2 North Riverside Plaza, Suite 1000,
Chicago, IL 60606

Tel: (224)571-0050

www.fusionrm.com

Linkedin: www.linkedin.com/company/fusion-risk-management/

Fusion Risk Management is a leading industry provider of cloud-based operational resilience software, encompassing business continuity, risk management, information technology and security risk, crisis and incident management, and more. Its solutions empower organizations to make data-driven decisions with a holistic, agile approach and enable them to deliver on their brand promise through disruption. For more information, visit www.fusionrm.com.

Daisy
20 Lindred Rd, Brierfield, Nelson BB9 5SR

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@daisyuk.tech
www.shadow-planner.com
Linkedin: www.linkedin.com/showcase/daisycorporate-services
Twitter: twitter.com/Daisy_Corporate

Shadow-Planner from Daisy is a multi-award-winning business continuity management software tool, with an award-winning, mobile app to drive business continuity planning for the digital age.

Daisy's Shadow-Planner enables you to map out your critical dependencies (including important business services), understand any gaps in capabilities, create plans, manage testing, and manage and monitor your business continuity/resilience programme.
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 resilience commitments efficiently and cost effectively. Designed by BC practitioners for BC practitioners, this suite of integrated software supports the entire business continuity management lifecycle: from impact analysis through developing strategies and plans to testing, reporting and even mass communications.

Shadow-Planner is based on the BCI's Good Practice Guidelines and currently covers the following modules:

- Business Impact Analysis (BIA)
- Strategy
- Business Continuity Planning
- Testing & Exercising
- Programme Management
- Mobile Application

BUSINESS CONTINUITY SOFTWARE

RecoveryPlanner
101 Merritt Boulevard, Trumbull, CT
06611 USA and Dartford Kent, UK

Contact Name: Jeff Goldstein, Sales Director

Tel: +1 (203) 455-9990
jgoldstein@recoveryplanner.com
www.recoveryplanner.com
Linkedin: www.linkedin.com/company/recoveryplanner.com/
Twitter: @RP_BCM

Resiliency Solutions Since 1999

RPX BCM Software
Depth, Flexibility & Scope for a Planner, Simple Enough for the Casual User
RecoveryPlanner's all-in-one **RPX** software brings together compliance, resiliency, operational risk and continuity to deliver a mature, integrated solution.

Key Features:

- One Complete Mature Software
- Cloud-based, Strong Security
- SaaS or On-premise License
- Unlimited, Concurrent Licensing
- Multi-lingual UI & Support
- Support in all Time Zones
- Native App - iOS & Android
- Rapid Implementation
- Customizable & Flexible
- Crisis Communications
- Leader in all Gartner's MQ's for BCMP Software

Continuity Consulting
Also available are integrated consulting services to help develop effective Plans and Programs that are tailored to each organization's culture, structure and maturity. Direct representation, support and professional services are available throughout Europe, EMEA and APAC.

Contact us today to see what RPX can do for you!

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

Daisy
20 Lindred Rd, Brierfield, Nelson BB9 5SR

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@daisyuk.tech
www.daisyuk.tech
Linkedin: www.linkedin.com/showcase/daisycorporate-services
Twitter: twitter.com/Daisy_Corporate

Protect what's most important to your business and recover from any disruptive event with Daisy. From identifying risks, managing them effectively and planning how you can continue to operate through all manner of disruptions. Daisy is the UK's business continuity industry leader with more than 30 years' experience.

Consultancy Services: From business continuity and operational resilience, through to cyber resilience. Our accredited consultants can work with you to produce and review your BIA, CSA, and security health checks. Advising and consulting on all aspects of your important and critical business service needs.

Business Continuity Planning and Third-Party Supply Chain Risk Management: Utilising our award-winning BC software Shadow-Planner, alongside our BCI accredited industry-leading advice and support. We can help you map, mitigate and report on all the dependencies within your risk profile.

Data Protection and Recovery: Whether you require backup, replication, or a combination of both - with or without recovery, self-service, co-managed, fully-managed, in the cloud or any other location – we have the capability to provide it. We also help in conducting regular testing, rehearsing, and documenting your data protection and recovery strategies.

Disaster Recovery: In times of crisis or for standby situations, we provide on-site delivery of physical IT solutions to your doorstep. We also provide expert support, from our pool of experienced business continuity engineers. We're able to deliver the right equipment and support, should disaster strike.

Work Area Recovery: Whether you need alternative workplaces or standby infrastructure, we offer 5,600 always-ready workplace positions throughout the UK. Our fully resilient buildings and facilities are designed to accommodate both simple and complex working environments. If adjustments to your work-from-home policy or changes to your real estate footprint have impacted your recovery plans, we are here to provide support in times of crisis!

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

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

The FortressAS team are expert in the provision of Operational and Cyber Risk and Resilience services.

Working along the lines of the NIST Framework, we focus on reducing the risk of disastrous events and mitigating the impact of these events when they do happen.

Our services span:

- Advisory (BC and Cybersecurity)
- Managed Services (Endpoint Detection and Response – ED&R, Virtual CISO)
- Solutions (ED&R, Threat Correlated Vuln Management, Identity, Insider Threat)
- Infrastructure Services (DRaaS, BaaS and Workplace Recovery)

We focus on delivering high quality services and those with a high ROI.

BUSINESS CONTINUITY LOGISTICS

CMAC Business Continuity TRANSPORT

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.

RISK MANAGEMENT SOFTWARE SOLUTIONS

12th Floor, St Clare House,
30-33 Minories,
London
EC3N 1DD

Tel: +44 (0)1617 917740
info@origamirisk.com
www.origamirisk.co.uk
LinkedIn: www.linkedin.com/company/origami-risk/
Twitter: twitter.com/origamirisk

Origami Risk provides integrated SaaS risk, insurance, and safety solutions to insured corporate and public entities, brokers and risk consultants, insurers, TPAs, and more.

Delivered from a single platform that is fast, secure, and completely scalable, Origami Risk's RMIS, GRC, EHS, Policy Administration, Claims Administration, and Healthcare Risk Management solutions incorporate easy-to-use analytics and digital-engagement tools — including portals, dashboards, and reports.

The multi-tenant Origami Risk platform is highly configurable, allowing for seamless integrations with third-party enterprise software systems and the tailoring of solutions that meet client-specific requirements and workflows without the need for costly, time-consuming custom development.

Origami Risk solutions are supported by an experienced service team that possesses a balance of industry-specific knowledge and technological expertise.

Protecht
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

Tel: +44 (0) 20 3978 1360
info@protechtgroup.com
www.protechtgroup.com

LinkedIn: www.linkedin.com/company/protechtgroup

Twitter: www.twitter.com/protecht_risk
YouTube: www.youtube.com/user/protechtptyltd

Protecht is an integrated software-as-a-service enterprise risk management solution, supported with training and advisory services, for organisations of any size or geography. Currently on release R11.1, Protecht allows users to dynamically manage all their risks – compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, BCP, health and safety – in a single platform.

Protecht delivers interconnected, structured data through dashboards and reports that can be categorised and documented, allowing users to spot trends and identify areas that require actions. Its reporting tools allow effective and professional communication to risk committees, boards and business stakeholders using customisable visual reports.

The platform is designed to be used across the organisation, with the MyTasks personal dashboard keeping every user on top of their responsibilities, and a mobile app to provide access wherever it's required. Registers can be customised and deployed without the need for coding, and the system's user management functions allow organisations to onboard users and precisely control their access.

With features including a dynamic form builder, the capability to automate notifications and email alerts, and customisable risk assessment scales, Protecht has the flexibility to meet an organisation's specific risk profile. It also includes a wide range of preconfigured dashboards, taxonomies, workflows, registers and analytics relevant for organisations for all levels of risk maturity.

Rather than just being a software company, Protecht is a risk company, incorporating training and advisory services delivered by leading experts in risk management. The product itself, the client implementation process, and the training and advisory services provided to customers are all directly informed by Protecht's understanding of how to manage risk.

www.protechtgroup.com

---

riskHive Software Solutions Ltd
Dilkush, Farlers End, Bristol, North Somerset, UK BS48 4PG

Contact: Ian Baker or Rebecca Cope-Lewis

Tel: +44 1275 545874 or +44 781 8898 997
info@riskhive.com
www.riskhive.com
Linkedin: www.linkedin.com/company/riskhive
Twitter: @riskhive
YouTube: www.youtube.com/channel/UCGDHhXKtohhLbmIM37gzF7w

riskHive's IRM platform is a 'no-compromise' solution to the challenges of implementing agile Integrated Risk Management with apps that will start working NOW, not in 2 years' time

With the mature and award-winning ERM v6 application at its core, you can very rapidly specify and design any number of integrated applications, workflows, functions and dashboards.

More can be added very quickly as your regulatory risk process evolves or changes in response to new requirements.

We know that developing a capability means going on a journey which is different for every company and 'one size' does not fit all.

That's why our flexible solution is the only one which is trusted by some of the worlds' biggest and most significant organizations to be hyper-configurable to meet your needs; whatever they are now and in the future.

Please get in touch to free yourself from the costs and constraints of regular GRC.