Book review
Inspiration for risk professionals

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

The interview
CIR catches up with Adam Ennamli

cirmagazine.com

Q4/2025

CIR

CONTINUITY INSURANCE & RISK

PFAS *So-called 'forever chemicals' have shifted from being a niche environmental issue to a global liability crisis in the making*

Information security *Information security is evolving from defensive discipline into strategic organisational advantage*

Business Continuity Software Report 2026 *Your guide to the business continuity software market, with product highlights*

The nature of risk

As biodiversity losses accelerate, insurance and risk management professionals are under increasing pressure to quantify, disclose and mitigate nature-related risks

View: "A profession that writes off markets as being 'too difficult' to serve will shrink and ultimately be replaced by other methods of managing risk"

Marsh

Foster a culture of wellbeing by unlocking the benefits of psychosocial safety

Download our whitepaper now

A business of Marsh McLennan

Comment

Cyber security – or a lack of it – has dominated headlines throughout the second half of this year. The attack that halted production at Jaguar Land Rover was estimated to have caused losses of around £1.9bn to the UK economy, according to figures from the UK's Cyber Monitoring Centre.

Many of JLR's suppliers faced cash flow problems as a result, with some resorting to loans to sustain operations. Over 5,000 UK organisations were affected by the incident. The CMC described the attack as the most economically damaging cyber event ever recorded in the country, classifying it as a Category 3 systemic event on its five-point scale.

The incident came to light just before the UK's National Cyber Security Centre revealed that the country had faced a record 204 "nationally significant" cyber attacks in the past year – an average of four a week. The figure, released in the agency's annual review of cyber incidents, compares with 89 over the previous year.

Eighteen of the 429 incidents handled by the NCSC were classed as "highly significant", meaning they had the potential to seriously disrupt essential services – a near 50% rise, and the third annual increase in this category. Many incidents involved advanced persistent threat actors linked to hostile states or capable criminal groups.

Nationally significant incidents are defined as those with the potential to affect the UK's national security, economy or critical infrastructure. In an increasingly connected world, such critical infrastructure extends to cloud infrastructure, making the subsequent major Amazon Web Services outage even more alarming. While not a malicious attack, the outage, which disrupted a wide range of online services, including banks and telecommunications providers, illustrates the systemic risks posed by concentrated cloud provider dependencies, and the vulnerability of digital ecosystems to a single region or critical service failure.

It is not the avoidance of service failure itself, or even the risk of customer data loss, that motivates the majority of UK businesses to address the risk, however, according to research carried out by Towergate Insurance. Instead, more than half of the UK businesses it polled fear reputational damage above all else following an attack, putting reputation as a concern ahead, even, of customer data loss (the greatest concern for less than a third of the companies polled), business or revenue loss (the priority for just 13%) – and even regulatory fines (identified by a mere 3% as the major driver).

The insurer said the findings, released to mark Cyber Security Month in October, underline the fact that cyber security has become a matter of credibility and brand integrity as much as technical defence. Others might argue that cyber security efforts may be failing because motivations are misplaced.

For essential public services, including healthcare, water providers, transport and energy, at least, the UK Government is hoping to change those motivations. Its latest digital security effort, the new Cyber Security and Resilience Bill, hopes to use regulation as a lever to strengthen national security and boost cyber protections for some of the country's most essential services.

Under the proposals, medium-sized and large companies providing IT management, IT helpdesk support and cyber security to private and public sector organisations like the NHS will also be regulated for the first time. The new Bill explicitly brings cloud infrastructure, datacentres and managed service providers into scope, recognising that dependence on a small number of digital service providers creates systemic risks.

The legislation introduces fresh reporting requirements for cyber incidents, new powers for regulators to direct organisations to improve resilience, and provisions to designate critical suppliers whose failure could disrupt essential services. Time will tell if the regulation has the teeth to change how organisations – in particular nationally significant ones – think and act on cyber risk.

Deborah Ritchie, Editor

airmic

JOIN US.

Driving transformation in risk and insurance.

www.airmic.com

Take a free membership test drive and see what we have to offer.

Airmic Ltd, Marlow House, 1a Lloyd's Avenue, London EC3N 3AA

COVER STORY

INTERVIEW 12

From compliance to confidence

Deborah Ritchie speaks to Adam Ennamli about how enterprise risk management is embedded into his organisation's growth engine, the shift from bureaucracy to decision enablement, and about how AI and pragmatism are redefining the modern risk function

COVER STORY

The nature of risk 14

As biodiversity losses accelerate, insurance and risk management professionals are under increasing pressure to quantify, disclose and mitigate nature-related risks. Martin Allen-Smith reports

GLOBAL RISKS 18

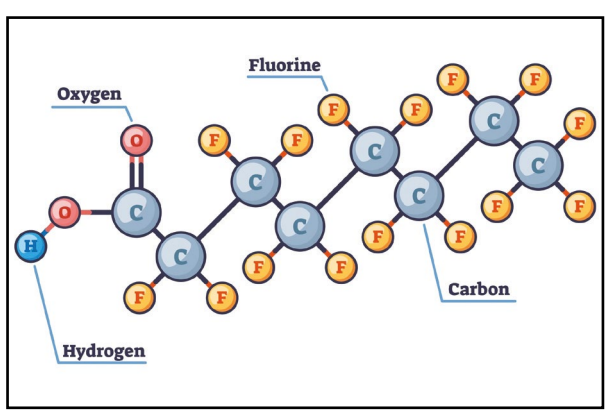
Worlds apart

A major new report portrays a world marked by fragmentation, uncertainty and interconnected crises, revealing widespread anxiety about the future and growing perceptions of vulnerability

PFAS 22

The forever risk

PFAS, the so-called "forever chemicals", have shifted from a niche environmental issue to a global liability crisis. With regulators tightening controls and claimants mobilising, litigation, compliance and insurance exposures are mounting. Laura Madders writes



PERSPECTIVE PUBLISHING

PPA Publisher Member

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

Editorial & features

News, views & regulars

Analysis	8
Book review	9
News in brief	10-11
Industry views: CII, GILC and the IRM	44-45
Executive summary	46
Market Guide	51

From firefighting to foresight **26**
Information security is evolving from a defensive discipline into a strategic advantage. The 2025 *State of Information Security Report* reveals how organisations are shifting focus from fear and prevention to resilience, trust and the ability to adapt under pressure

BUSINESS CONTINUITY SOFTWARE REPORT 2026 **32**

Market analysis
In an ever-changing, complex risk landscape, business continuity software is being brought closer to day-to-day operations and strategic decision-making. David Adams takes a look at how today's enhanced solutions are being used at the coalface

Products and features **34**
Your guide to the best products in the global business continuity software marketplace, with comprehensive features comparison table

CIR
CONTINUITY INSURANCE & RISK

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

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

Production
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 our registration form online at www.cirmagazine.com

CIR Magazine is published by:

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

ISSN 1479-862X
cirmagazine.com

Executive summary

Firms rethink overseas security

Global businesses are re-evaluating their exposure to geopo and political unrest emerge as top growth barriers, according t

Global business leaders now see geopolitical and economic uncertainty as the greatest obstacles to growth, with inflation and political unrest key amongst corporate risks. These are amongst the findings of Beazley's 2025 *Geopolitical and Economic Risk and Resilience Report*, which surveyed 3,500 senior executives across multiple regions and sectors.

The research paints a picture of firms operating in a complex, fast-moving environment where trade tensions, energy costs and policy shifts are converging to test resilience.

"Some 35% report increasing their investment in risk management and loss prevention since early 2024, aiming to ensure that innovation is matched by resilience"

In response, 32% of businesses plan to reassess the security of their overseas operations this year, up from 23% last year. Supply chain disruption has become a [illegible] concern, with 87%

Analysis

Climate risk

Markets underestimate impact of rising temperatures

Companies that are more exposed to temperature fluctuations deliver weaker returns and take greater risks, yet remain highly valued – suggesting that markets are underpricing climate-related financial risks

Firms that are more exposed to rising temperatures consistently deliver lower-than-expected returns, according to new research from the University of Exeter Business School.

The study analysed over five decades of US stock data and introduced a measure of temperature sensitivity to assess how companies' share performance responds to unusual shifts. It found that firms more affected by temperature changes tend to be less profitable, take greater risks, and generate weaker stock returns. Yet these same firms retain relatively high valuations, suggesting that investors are underestimating the impact of climate cha

£64tn energy transition will 'reshape global risk markets'

The accelerating global energy transition is set to transform the risk landscape, according to the latest analysis from Swiss Re. It estimates that total investment in energy transition, climate mitigation and adaptation could exceed £64tn by 2040, signalling a shift from experimental projects to large-scale deployment.

Jimmy Keime, head engineering and nuclear global energy transitio

HORIZONSCAN

RISK - RESILIENCE - READINESS

Award-winning Specialists in Resilience

We provide business continuity, crisis management, and organisational resilience services to the insurance market.

HORIZON SCANNING

OUR SERVICES

- BUSINESS CONTINUITY & CRISIS MANAGEMENT PLANNING
- BUSINESS IMPACT ANALYSIS
- CRISIS SIMULATION TABLETOP EXERCISES
- ISO CERTIFICATION SUPPORT

CONTACT US

SCAN ME

SERVING CLIENTS WORLDWIDE

www.horizonscanbcp.com

Markets underestimate impact of rising temperatures

Companies that are more exposed to temperature fluctuations deliver weaker returns and take greater risks, yet remain highly valued – suggesting that markets are underpricing climate-related financial risks

Firms that are more exposed to rising temperatures consistently deliver lower-than-expected returns, according to new research from the University of Exeter Business School.

The study analysed over five decades of US stock data and introduced a measure of temperature sensitivity to assess how companies' share performance responds to unusual shifts. It found that firms more affected by temperature changes tend to be less profitable, take greater risks, and generate weaker stock returns. Yet these same firms retain relatively high valuations, suggesting that investors are underestimating the financial impact of climate change, according to the report's authors.

The researchers also suggest that local investors familiar with regional conditions are better at pricing in temperature-related risks than non-local institutional investors. Sell-side equity analysts appeared to misjudge the impact of temperature as their forecasts for high-sensitivity firms were less accurate.

A trading strategy that bought stocks of low-sensitivity firms and shorted high-sensitivity ones produced an annualised, risk-adjusted return of about 4% over the 52-year period studied.

Professor Chendi Zhang from the University of Exeter Business School said: "While there is broad consensus about the potential impact of climate change and carbon emissions on firms, surprisingly little has been done to quantify systematically the economic impact of temperature changes for individual firms.

"Our novel, firm-level, market-based measure of temperature sensitivity, which utilises public information available for an extended time period, fills that information gap, and our results show that traditional valuation models do not capture how climate change-induced temperature changes are directly affecting firm performance – despite growing investor attention to climate resilience and environmental sustainability."

£64tn energy transition will 'reshape global risk markets'

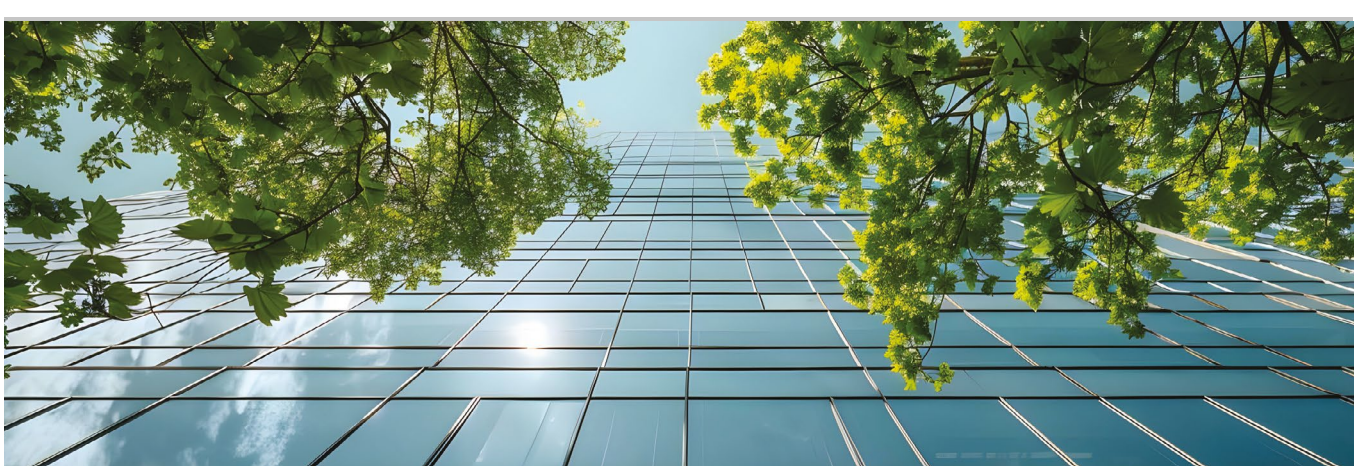
The accelerating global energy transition is set to transform the risk landscape, according to the latest analysis from Swiss Re. It estimates that total investment in energy transition, climate mitigation and adaptation could exceed £64tn by 2040, signalling a shift from experimental projects to large-scale deployment.

Jimmy Keime, head engineering and nuclear at Swiss Re, said: "As the global energy transition continues to accelerate, it's drawing sustained investment into green infrastructure and technologies. Amid this changing landscape, our analysis suggests that industry players should not approach renewables as a commoditised or fully standardised risk class."

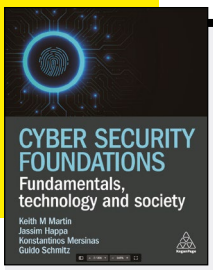
The report, *Market Perspectives: Exploring the State of Play in the Energy Transition*, projects that renewable energy capacity will almost double from 4.4 terawatts in 2024 to 8.5 terawatts by 2030. This expansion could generate up to £21bn in annual insurance premiums, with Asia-Pacific and Europe leading the growth. Swiss Re highlights that shifting technologies and weather-driven volatility are creating new exposures and losses, which in turn demand detailed risk assessment.

As renewable portfolios mature, insurance needs are evolving from the construction phase towards long-term operational resilience, typically supported by standalone renewable energy treaties, while facultative arrangements remain an option for larger or less proven risks.

The report also draws attention to emerging claims trends, including extreme weather damage, battery-storage fires and mechanical failures, stressing the importance of stronger links between underwriting and real-world data.



Inspiration for resilience professionals



Cyber Security Foundations: Fundamentals, Technology and Society

Keith Martin, Konstantinos Mersinas, Guido Schmitz, Jassim Happa
Kogan Page, 2025
koganpage.com

Cyber security has become one of the defining risks of our time.

As emerging technologies expand attack surfaces and cyber criminals grow more sophisticated, organisations face not only heightened risks but also a growing maze of regulatory requirements. As the World Economic Forum notes in its 2025 *Global Cybersecurity Outlook*, the modern cyber landscape is increasingly shaped by geopolitical tensions, intricate supply chains, and the rapid evolution of digital technologies. This evolving environment is further strained by a global shortage of skilled professionals, underscoring the urgent need for more resilient, collaborative and adaptive cyber security strategies.

It is against this backdrop that Kogan Page publishes its latest book on the core topics that all cyber security students and professionals need to understand in order to manage the emerging risks. *Cyber Security Foundations: Fundamentals, Technology and Society* is intended as a textbook for postgraduate and undergraduate students studying cyber security and information security modules, as well as for risk professionals and others seeking to deepen their technical and human-centred digital security knowledge.

Chapters focus on core areas including cryptography, computer security, cyber security management, cyber crime and privacy. An analysis of how the various facets of the discipline interrelate is included, while real-world examples – of which there is a growing catalogue in both the public and private sectors – illustrate the application of ideas throughout. Learning outcomes and activities are designed to help reinforce understanding, and encourage further exploration beyond the core text. Finally, in a world in which terminology matters, a glossary equips readers with the language necessary to make sense of each topic.

Kogan Page's latest book has been compiled by some of the field's foremost academics and experts. Author Keith Martin is a professor of information security at Royal Holloway, University of London, and director of the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday Life; Jassim Happa and Konstantinos Mersinas are senior lecturers in information security at Royal Holloway, University of London; and Guido Schmitz is an assistant professor in computer science and cyber security at Lancaster University, Leipzig.

With their extensive experience of teaching in cyber security, together the authors guide readers through the core principles and their real-world applications.

Cyber Security Foundations provides broad but detailed coverage of the fundamental principles and technology of cyber security, including its important – but often overlooked – societal dimensions.

Despite affecting almost every aspect of modern life, the societal aspects of cyber security are often overlooked

News briefing

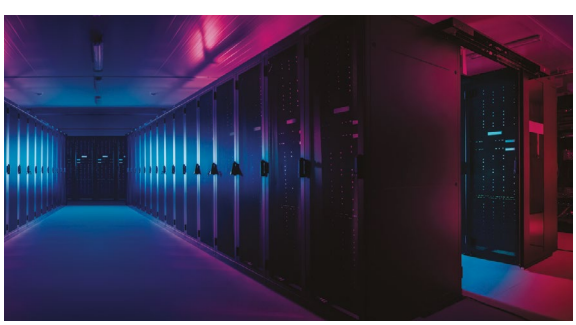
A round-up of the latest industry news

Two men were killed and three others seriously injured in a terrorist attack that took place outside the Heaton Park Hebrew Congregation in Manchester in early October, during the Jewish holiday of Yom Kippur. The assailant, identified as 35-year-old Jihad al-Shamie, drove a car into pedestrians before launching a stabbing spree while wearing a fake explosive vest.

Analysis by the Mineta Transportation Institute showed that vehicle ramming attacks are on the rise. A stark illustration of the threat came in late September in Michigan, when four people were killed, and eight others wounded after a gunman rammed a vehicle into a church, began shooting, and started a fire.

The UK faced a record 204 "nationally significant" cyber attacks in the past year – an average of four a week – according to the National Cyber Security Centre. The figure, revealed in the agency's latest annual review, compares with 89 over the course of the previous year.

The cyber attack that halted production at Jaguar Land Rover has been estimated to have caused losses of around £1.9bn to the UK economy, making the attack the most economically damaging cyber event ever recorded in the UK, according to the Cyber Monitoring Centre.



Boards may often express confidence in their cyber readiness but recent high-profile incidents show how fragile that assurance can be under pressure. According to Willis's *Cyber in Focus 2025* report, based on 4,650 cyber claims, losses tend to be longer, broader and more costly than expected.

Ransomware attacks are forecast to see a sharp rise, with the number of victims publicly named on leak sites projected to grow from 5,010 in 2024 to more than 7,000 by the end of 2026, according to analysis from insurer QBE. This would represent a rise of around 40%, and an almost five-fold increase since 2020, when just 1,412 victims were listed.

The BSIF joined a coalition of trade bodies, consumer groups and safety organisations, led by *Which?*, in urging the government to introduce secondary legislation to support the new Product Regulation and Metrology Act. The group argues that online marketplaces must be made accountable for unsafe products sold through their platforms, ensuring a level playing field with traditional retail.

Most European companies relied on their existing enterprise risk management systems to meet the first wave of CSRD requirements, according to a new study from FERMA and Protiviti. Some 60% used their ERM risk register as the foundation for identifying and evaluating sustainability risks and opportunities.

Preliminary estimates suggested that insured losses from October's Amazon Web Services outage could range between £29m and £436m. Analytics firm CyberCube said the event is expected to have a loss-ratio impact for cyber insurers in the low to mid-single digits, reflecting only a moderate insurance impact.

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

Research carried out this quarter by Clyde & Co suggested that businesses are stepping up their risk management strategies with tighter control of supply chains, enhanced contractual protection, centralised regulatory oversight and more frequent cyber simulations.

Inconsistent AI execution is leaving many "stuck in pilot mode", according to a new report from AuditBoard. An AI adoption gap is being driven by what it calls the "middle maturity trap", where high investment activity fails to translate into sustained resilience. The firm says decision-making times are lengthening as confidence in AI adoption fluctuates, with fewer than 30% of businesses prepared for upcoming governance requirements.

More than half of all new board appointments at UK financial services firms over the past year brought in technology expertise, as companies respond to rapid advances in AI and emerging technologies. According to the latest EY *UK Financial Services Boardroom Monitor*, 52% of directors appointed in the twelve months to June 2025 had technology experience.

UK companies are making progress in gender equity, though challenges remain in achieving leadership parity, according to the 2025 *Women in Work Gender Equity Measure Report*. Compiled by the Women in Work Summit and LinkedIn, the data reflects a 19% rise since 2024 in the number of the UK's largest 400 companies meeting gender equity benchmarks.

NTT DATA acquired Alchemy Technology Services, a specialist insurance technology consultancy based in Northern Ireland, in a move aimed at expanding its capabilities in complex markets.

Special Contingency Risks introduced an enhanced victim support insurance extension aimed at providing assistance to individuals affected by kidnapping, unlawful detention, or critical security incidents.

Global commercial insurance rates fell by an average of 4% in Q3 2025, matching the decline seen in Q2, according to figures from Marsh, marking the fifth consecutive quarterly decrease following seven years of increases. Heightened competition among insurers, favourable reinsurance pricing, and increased market capacity drove the trend.

Firms that are more exposed to rising temperatures consistently deliver lower-than-expected returns, according to research published by the University of Exeter Business School. To draw these conclusions, the study analysed over five decades of US stock data and introduced a measure of temperature sensitivity to assess how companies' share performance responds to unusual shifts.

A new report from global transport insurer TT Club and engineering consultancy Haskoning warned that delaying adaptation risks escalating damage and costs. Nearly 90% of the world's 3,700 major ports are exposed to climate hazards, including hurricanes, flooding, heatwaves and shifting ocean currents, jeopardising global supply chains and infrastructure.

UK businesses are taking a more proactive approach to risk management than their global peers, according to Aon's latest *Global Risk Management Survey*. Nearly 80% of UK respondents said their boards are directly involved in risk oversight, compared with 61% globally, suggesting UK leadership is taking greater responsibility for organisational risk.

From compliance to confidence

Deborah Ritchie speaks to Adam Ennamli about how enterprise risk management is embedded into his organisation's growth engine, the shift from bureaucracy to decision enablement, and about how AI and pragmatism are redefining the modern risk function

How would you describe the General Bank of Canada's approach to enterprise-wide risk management? What distinguishes its structure or culture from other institutions you've worked with?
General Bank of Canada is making enterprise risk a core part of its growth system. We see trust as a competitive advantage in the marketplace, and we have unified our capabilities to reduce friction, crisis response time and costs. At GBC, risk is not seen as a source of bureaucracy, but as a partner for decisions. Easier said than done, I know, but that's where the rubber hits the road. Over the past three years, we have reduced the number of risk assessments by 80 per cent, as risk considerations are now embedded in our business processes, seamlessly.

"Over the past three years, we have reduced the number of risk assessments by 80 per cent, as risk considerations are now embedded in our business processes, seamlessly"

Our risk professionals are connected to their business counterparts through a centralised risk partnering model where understanding the processes in depth is a priority, along with automation. The programme has been right-sized, leading to 60 per cent hard efficiencies and more clarity. Finally, and most importantly, the culture is more durable. We are introducing a microlearning programme that takes the training burden from an average of four hours per domain to 12 minutes of targeted education, where content is generated through AI depending on the audience.

Your background spans technology, compliance and operational resilience. How does that technical grounding shape the way you approach risk decision-making, and communicate with other senior stakeholders?
It helps with being able to understand the reality of each department and adapt the risk function to those realities. A lot of the friction between the risk function and the rest of the organisation stems from theoretical frameworks that cannot be adopted due to operational constraints, due to the high indirect cost that they impose on the first line, or due to their complexity. Speaking multiple sub-languages is a very helpful catalyst to build trust with counterparts, and maximise the effectiveness of risk guardrails, without bureaucracy. For instance, when working with our tech teams on an upcoming transformation, I can discuss concrete integration points of failure previously encountered during ERP implementations or cloud migrations, then translate those risks into business impact terms for mainstream audiences.

Risk management theory can look neat on paper, but the real test is in daily operations. Where do you see the biggest gap between risk frameworks and risk in action – and how do you bridge it?
We need to be pragmatic when we expect a product function to fill out a 10-page risk assessment when their own business case was only a one-pager. Logic has left the room. I am not advocating for a total laissez-faire, but to make risk invisible, effective and embedded into every day operations – less jargon, more connection. For our last three new product and markets, there was no documentation produced by risk; everything was part of one unified, comprehensive business case that addressed any potential challenges or risks at the onset of the project. Concretely, each business case follows a structured template that prompts consideration of key risk domains seamlessly. We've just eliminated the redundancy. For example, strategic risk is addressed through market share and product portfolio considerations, while operational risk is discussed through the execution section.

As a member of the Forbes Technology Council, you've a clear vantage point on emerging tools. How do you see AI and data-driven systems transforming the way risk teams analyse, report and respond?
In the past 15 years, most of the risk teams have executed low-value, necessary but bureaucratic tasks at 60-80 per cent+ of their capacity, leaving very little time and energy for

Adam Ennamli, chief risk, compliance and security officer, General Bank of Canada

high-value thinking that can move the needle and get organisations to be proactive and actually address emerging trends, rather than just react. AI can be used to automate these tasks – to simplify them, so that we can transition that 80 per cent into real decision enablement. We have started to do that, with success, at GBC. For example, our due diligence for third parties has been automated at 77 per cent thanks to a partnership with a US risktech. We have also started automating our risk model validation through another partnership, where our pilot case has yielded 90 per cent cost efficiencies and 70 per cent faster validation compared with traditional use cases.

You're a member of the Risk Management Awards judging panel. Having judged this year's award entries, what struck you most about the next generation of risk professionals? Which capabilities or mindsets stand out?

I see more diversity of thought, and more integration and creativity, which is wonderful. Risk is moving away, slowly, from its ivory tower reputation, with fewer barriers to entry and more openness to other domains. One submission showed how a risk professional applied design thinking to redesign a specific process, cutting resolution time in half without major capital investments or new resources. Everyone has something to contribute, and risk can be a central hub to channel those strengths. More use of technology as well, which is always great as it refocuses efforts where they truly belong.

You lead a complex portfolio, sit on advisory boards and contribute regularly to industry dialogue. How do you manage that spread of responsibility – and what keeps you motivated about the future of the profession?

Advancing mindsets, one idea at a time. Professionally, the first and foremost priority is to support the growth of our bank and to help my colleagues focus on our top priorities as a risk team. My thought leadership work is about modernising the function and exchanging with fellow risk and compliance officers globally to reduce fragmentation, and increase automation and pragmatism. Risk is not about fear, it's about decisions. The more that risk leaders get involved in industry dialogue, the more positively the risk domain will evolve.

Interview by Deborah Ritchie

The nature of risk

As biodiversity losses accelerate, insurance and risk management professionals are under increasing pressure to quantify, disclose and mitigate nature-related risks. Martin Allen-Smith reports

For years, climate risk has dominated the corporate sustainability agenda. But as understanding of natural capital deepens, attention is turning to the quieter, more complex crisis of biodiversity loss. From the degradation of soil and freshwater systems to the collapse of ecosystems underpinning global supply chains, the erosion of nature is now recognised as a systemic financial risk, and one that demands integration into mainstream risk management.

"Over 50 per cent of global GDP depends on natural capital and ecosystem services, but many ecosystems are close to tipping points beyond which they may be unrecoverable"

"We've realised that nature is not an externality, that it is essential to our well-being, so societies are increasingly seeking to protect what remains," says Chandler Morris, a regional head of environmental impairment liability at Allianz Commercial. "For instance, a 2019 report from the OECD estimated that natural ecosystems provide a global value of US$125 to US$140 trillion (£95 to £106 trillion) annually. Indeed, over 50 per cent of global GDP depends on natural capital and ecosystem services, but many ecosystems are close to tipping points beyond which they may be unrecoverable."

Unlike carbon emissions, biodiversity loss is multi-dimensional, localised, and harder to quantify. Yet its implications are no less profound. For insurers, it threatens to reshape exposure models; for corporates, it creates supply volatility, regulatory scrutiny, and reputational vulnerability.

Figures from the European Insurance and Occupational Pensions Authority suggest that around one in five insurance undertakings mention biodiversity in their governance and risk management systems, and risk and solvency assessments. This figure doubles for large undertakings. EIOPA adds that when undertakings explicitly mention conducting a biodiversity risk assessment, most of these are qualitative in nature. A smaller portion combines both qualitative and quantitative elements, while only a few are purely quantitative.

The extremely broad and varied scope of biodiversity risks also adds to the challenge from a risk management and underwriting perspective. Physical risk can arise from damage to nature, changes in natural stocks and flows, or the decline of ecosystem services, which can lead to increased losses in investments or liabilities.

EIOPA says that for underwriting, different lines of business are affected in different ways by some of these physical biodiversity risks. For example, environmental liability risks may be particularly relevant for industrial insurers; maritime biodiversity risks for transport insurers; and biodiversity risks relating to the preservation of natural resources for agricultural insurers. Additionally, health insurers may face risks from invasive species; while property insurers may be concerned with risks associated with water or land use.

In many ways, the industry's experience with climate risk has provided the scaffolding for this new challenge. Enterprise risk management systems already account for long-term physical, transition and liability risks associated with climate change.

Now, the task is to expand those frameworks to include nature dependencies – the ecosystems and resources on which business operations directly rely.

For insurers, that means understanding how environmental degradation might influence claims frequency or asset valuation. For corporates, it involves mapping dependencies within supply chains, assessing exposure to ecosystem decline, and translating those findings into financial metrics.

"Work is underway to expand frameworks to include nature dependencies; the ecosystems and resources on which business operations directly rely"

Some insurers are already exploring how ecosystem resilience could be priced into underwriting models. Others are investing in 'nature-positive insurance' – products designed to incentivise conservation or restoration activity, echoing the early evolution of green insurance

lines seen during the first wave of climate adaptation.

The regulatory landscape around nature-risk disclosure is tightening fast. The Taskforce on Nature-related Financial Disclosure framework, formally launched in 2023, provides a structure for organisations to identify, assess and disclose their nature-related dependencies and impacts. It mirrors the successful architecture of the Taskforce on Climate-related Financial Disclosures, but extends its reach to the broader ecosystem of environmental risk.

"For risk managers, these developments are no longer theoretical. They signal a compliance expectation that requires new data streams, cross-functional collaboration and, in many cases, a cultural shift in how nature is valued"

Meanwhile, the EU Corporate Sustainability Reporting Directive, which came into force in 2024, obliges thousands of companies to report on both climate and biodiversity impacts. Under the CSRD's European Sustainability Reporting Standards, firms must outline their material dependencies on ecosystem services and their plans for mitigation or restoration.

New risks in practice

For risk managers, these developments are no longer theoretical. They signal a compliance expectation that requires new data streams, cross-functional collaboration and, in many cases, a cultural shift in how nature is valued. Professor Ben Groom, Dragon Capital chair in biodiversity economics at the University of Exeter Business School, says: "TNFD is gathering momentum.

CSRD is being taken seriously in the EU. In terms of metrics, there are many tools that measure biodiversity footprints, but these tend to measure impact of activities on nature rather than risk to companies from nature-related losses.

"The problem with these individual company or portfolio-level measurements is that they ignore the public good nature of nature and biodiversity losses. The damages caused by an individual firm affect all other firms or users of the ecosystem in the wider area. Just registering the damages to the single firm, and then acting on that, does not reflect the wider social damages. So, acting on this fraction of the damages caused is just a fractional response. While potentially better than nothing, this is a key challenge to the efficient allocation of capital."

"Quantifying biodiversity loss remains a big challenge. Unlike carbon, there is no single unit of measure for nature. A forest's value can be expressed in carbon sequestration, water filtration, pollination, flood mitigation or cultural significance – often all at once"

Quantifying biodiversity loss remains a big challenge. Unlike carbon, there is no single unit of measure for nature. A forest's value can be expressed in carbon sequestration, water filtration, pollination, flood mitigation or cultural significance, often all at once.

Katherine Lampen, sustainability and climate lead at Deloitte, comments: "Insurers have a big opportunity to innovate in nature-related risk transfer, developing products that help customers manage biodiversity loss. The key challenge lies in measurement – fundamentally, ecological datapoints cannot easily be translated into financial risk metrics.

"Although some progress has been made on sector-level data for corporate products, there is very little data on how personal products depend on or impact nature. However, over the next few years, access to public and corporate data will improve as nature rises in importance on corporate and regulatory agendas, as will the tools and methodologies to make meaningful business decisions."

Risk managers are therefore experimenting with multi-metric assessment models, combining physical indicators, such as land-use change or species abundance, with financial proxies for ecosystem services. Remote sensing technologies, AI-driven environmental monitoring, and partnerships with conservation data providers are helping fill information gaps, but the data remains patchy and difficult to standardise.

New opportunities for cover

While biodiversity loss represents a material risk, it also opens new avenues for innovation. The emergence of nature-based insurance products is one sign of this shift, covering areas such as ecosystem restoration, flood resilience or agricultural diversification.

At a strategic level, businesses that proactively engage with biodiversity management can position themselves ahead of regulatory and market expectations. Those that do not risk facing higher insurance premiums, restricted access to capital, and reputational damage as stakeholder scrutiny intensifies in the future.

In this evolving landscape, the role of the risk manager is becoming both broader and more strategic. Traditional risk models – focused on probability and impact – have to adapt to address interdependence, embracing the way environmental, social and governance risks overlap and amplify one another.

"Businesses increasingly find themselves facing regulations and unlimited fines for harming ecosystems," Morris explains. "For example, in 2023, the UK lifted the cap on environmental fines, allowing for unlimited penalties against polluters. This strengthens enforcement across industries and removes the previous cap of £250,000 on penalties for environmental offences, allowing regulators to impose unlimited fines on polluters.

"This kind of regulatory shift forces companies to re-evaluate their operations and ensure compliance to avoid financial penalties and long-term damage to their reputation. Companies have already started to act ahead of these regulations. One global firm restructured its entire waste management process to meet stricter biodiversity standards."

The transition to nature-aware risk management is not just about regulation or reputation; ultimately it is based around resilience. Businesses that ignore biodiversity dependencies may be unaffected in the short-term but risk facing long-term instability. Those that engage meaningfully can reduce exposure, secure investor confidence, and contribute to systemic resilience in the face of ecological decline.

In that sense, nature-related risk management is not a niche sustainability issue but a core business function for the decade ahead. Just as climate disclosure transformed corporate accountability over the past five years, biodiversity may soon redefine what it means to manage risk responsibly.

NATIONAL INSURANCE AWARDS 2026

BOOK YOUR TABLE
25 March 2026

nationalinsuranceawards.co.uk

Supported by

airmic

ALARM embrace risk

Managing General Agents' Association

Sponsored by

HORIZONSCAN
RISK - RESILIENCE - READINESS

Brought to you by

Insurance Today

In partnership with

CIR

@InsTodayNews @CIR_Magazine #NationalInsuranceAwards

London Marriott Hotel, Grosvenor Square, London

Worlds apart?

A major new report portrays a world marked by fragmentation, uncertainty and interconnected crises, revealing widespread anxiety about the future and growing perceptions of vulnerability

Crises, by their nature, do not arrive in an orderly fashion or even one at a time. They collide, intersect and ripple across societies, exposing the fragility of social, economic and political systems. From climate shocks to geopolitical tensions, technological disruption to public health emergencies, the sense of living and working in an interconnected storm of risks has never been more acute.

It is against this backdrop that communities and nations alike are grappling with uncertainty and a growing awareness of vulnerability, while simultaneously facing pressure to act collectively in the face of unprecedented complexity.

In analysing the risk horizon, Axa's latest *Future Risks Report* reflects a world marked by these challenges, revealing widespread anxiety about the future and a collective sense of urgency to navigate these complex global challenges.

"Social fragmentation has emerged as a central threat, fuelled by demographic changes, geopolitical tensions, misinformation and the indirect effects of climate change"

The 2025 edition of the report, produced in partnership with Ipsos, highlights "a world of rising polarisations confronting the globalisation of risks", where crises no longer occur in isolation but accumulate, intersect and reinforce one another. Social fragmentation has emerged as a central threat, fuelled by demographic changes, geopolitical tensions, misinformation and the indirect effects of climate change, including natural disasters, resource degradation and food insecurity.

These pressures generate compounded vulnerability. Axa's surveys of the general population and risk experts alike perceive public authorities as insufficiently prepared to manage increasingly complex crises, while trust in institutions continues to erode.

As CEO of Axa, Thomas Buberl notes in his foreword to the report: "Whether it's the crisis of liberal democracy or the growing distrust in public authorities' ability to effectively manage crises, the feeling of vulnerability is at its peak, both among experts and the general population."

Despite this trend, attachment to democratic principles and freedom of expression remains resilient, according to the insurer's analysis, suggesting that societies continue to value governance frameworks even amid rising uncertainty.

Emerging technological risks further outline evolving attitudes. AI, big data and related ethical and economic challenges are moving up the priority hierarchy, demonstrating how rapid innovation can both create opportunities and amplify vulnerabilities. Climate change remains the most feared risk, reinforced by tangible impacts on communities and the economy.

Divergent perceptions of risk

In comparing risk perceptions between professionals in the risk field and the general population, the report highlights both convergence and divergence in how risk is understood, prioritised and contextualised. At first glance, the two lists share some core concerns, yet the differences reveal important insights about the interplay between expertise, lived experience and societal awareness.

Both groups identify climate change as the most pressing risk, reflecting its cross-cutting significance and the extensive media coverage and scientific consensus that underscore its urgency. For specialists, climate change sits alongside geopolitical instability and cyber security – risks shaped by systemic complexity, interdependencies and potential for cascading impacts. The general population, however, positions new security threats, including terrorism, immediately after climate change, while geopolitical instability ranks lower, suggesting that personal safety concerns and immediate security narratives are more salient to non-experts than structural political dynamics. This divergence may partly reflect the immediacy heuristic: the general public are more likely to weigh risks they perceive could affect them directly, whereas risk specialists assess threats through lenses of systemic fragility, probability and long-term impact.

Cyber security occupies a prominent position in both lists, ranked third by each group, demonstrating shared recognition of the growing societal and business reliance on digital infrastructure.

Social tensions and movements also feature highly for both

groups, though their positioning differs slightly, reflecting nuanced interpretations: risk specialists perceive social unrest as a driver of systemic instability, while the public may perceive it more through the lens of personal disruption or societal cohesion.

"New security threats, pandemics, pollution and chronic illnesses feature on the public's list of concerns but are largely absent from the experts' list, underscoring the tension between subjective risk salience and systemic risk assessment"

The lists diverge more noticeably with respect to health and environmental risks. Pandemics and infectious diseases appear in the general population's top ten but are absent from the risk specialists' ranking, while natural resources and biodiversity, energy risks and demographic shifts are top concerns for risk specialists but largely invisible to the general public. This discrepancy suggests that risk professionals are attuned to slow-burn, systemic risks – such as resource scarcity and demographic pressures – that may not yet have immediate visibility but carry substantial long-term consequences. Conversely, the general public prioritises risks with tangible, observable impacts or high national media salience, such as infectious diseases, chronic illnesses and pollution. The inclusion of pollution and chronic illnesses by the general public, but not by risk specialists, illustrates the gap between experiential and systemic risk perception: everyday exposures and personal health threats are weighted more heavily outside professional risk circles, where risk assessment tends

to rely on probabilistic modelling, systemic interconnectedness and broader economic or societal implications.

Artificial intelligence and big data occupy mid-ranking positions in both lists, but with slightly higher concern from risk specialists. This reflects an expert understanding of both the transformative potential and the latent threats posed by AI – ranging from operational risks to ethical and governance challenges – while the general public may perceive AI largely in terms of immediate societal impacts, privacy concerns or worries about the automation of jobs.

Financial stability appears towards the bottom of both lists, yet its slightly higher ranking by risk specialists reflects the profession's awareness of systemic vulnerabilities and contagion effects within global financial networks – risks that may not yet feel immediate to the general population. Conversely, new security threats,

"These discrepancies illuminate broader challenges in risk communication and governance. Where a risk appears in one list but not the other, it signals a potential blind spot"

pandemics, pollution and chronic illnesses feature on the public's list of concerns but are largely absent from the risk professionals' ranking, underscoring the tension between subjective risk salience and systemic risk assessment.

The methodological context of the surveys further nuances these findings. The general population survey encompassed 23,000 respondents across 18 countries, weighted for demographic representation, while the survey amongst risk specialists canvassed the views of 3,595 individuals in 57 countries. Differences in country composition compared with previous years – most notably the inclusion of Turkey, Egypt, Ireland and Brazil and the exclusion of Australia – may subtly influence risk salience, as regional experiences with health crises, geopolitical tensions or environmental degradation shape perceptions. Additionally, the broader population may be influenced by local media coverage, recent events and cultural framing, whereas specialists apply analytical frameworks shaped by training, experience and cross-border risk monitoring.

These discrepancies illuminate broader challenges in risk communication and governance. Where a risk appears in one list but not the other, it signals a potential blind spot: experts may underestimate public concern for immediate, tangible threats, while the general public may undervalue slow-moving systemic risks. Understanding these divergences is critical for risk professionals, particularly in designing communication strategies, public policy advocacy and organisational resilience measures, ensuring that both expert assessment and societal perception are integrated in decision-making.

Axa's latest report underscores the gap between professional and public perceptions of risk, reflecting differences in immediacy, visibility and systemic complexity. For specialists, the results underscore the importance of bridging this perception gap, not only to ensure effective risk management but also to foster societal understanding of latent systemic threats. A nuanced appreciation of these divergences can help the profession communicate risk more effectively, align preventive measures with public concern and ultimately strengthen societal resilience against both immediate and long-term challenges. The risk profession is reminded by this report that risk perception amongst the majority is rooted in a much more social paradigm, and to some degree fuelled by fear of the unknown.

CIR

BUSINESS CONTINUITY AWARDS 2026

The pinnacle of achievement in business continuity, security and resilience

OPEN FOR ENTRIES

DEADLINE: 13 FEBRUARY 2026

London Marriott Hotel, Grosvenor Square, London

In association with

CITY OF LONDON

Sponsored by

HORIZONSCAN
RISK - RESILIENCE - READINESS

Supporters

airmic

ALARM
embrace risk

Insurance Today

cirmagazine.com/businesscontinuityawards
@CIR_Magazine #BusinessContinuityAwards

The forever risk

PFAS, the so-called "forever chemicals", have shifted from a niche environmental issue to a global liability crisis. With regulators tightening controls and claimants mobilising, litigation, compliance and insurance exposures are mounting. Laura Madders writes

Per- and polyfluoroalkyl substances are found in thousands of products – from fire-fighting foam to cosmetics, and food packaging to saucepans. In addition to being a considerable environmental concern, PFAS exposure is linked with multiple health risks, including cancer.

As governments and regulators continue to grapple with PFAS regulations, mass litigation and sizeable settlements continue across the US. Meanwhile in Europe, claimants are taking advantage of group litigation developments, and the rise of third party litigation funding to pursue claims against manufacturers of PFAS and PFAS products.

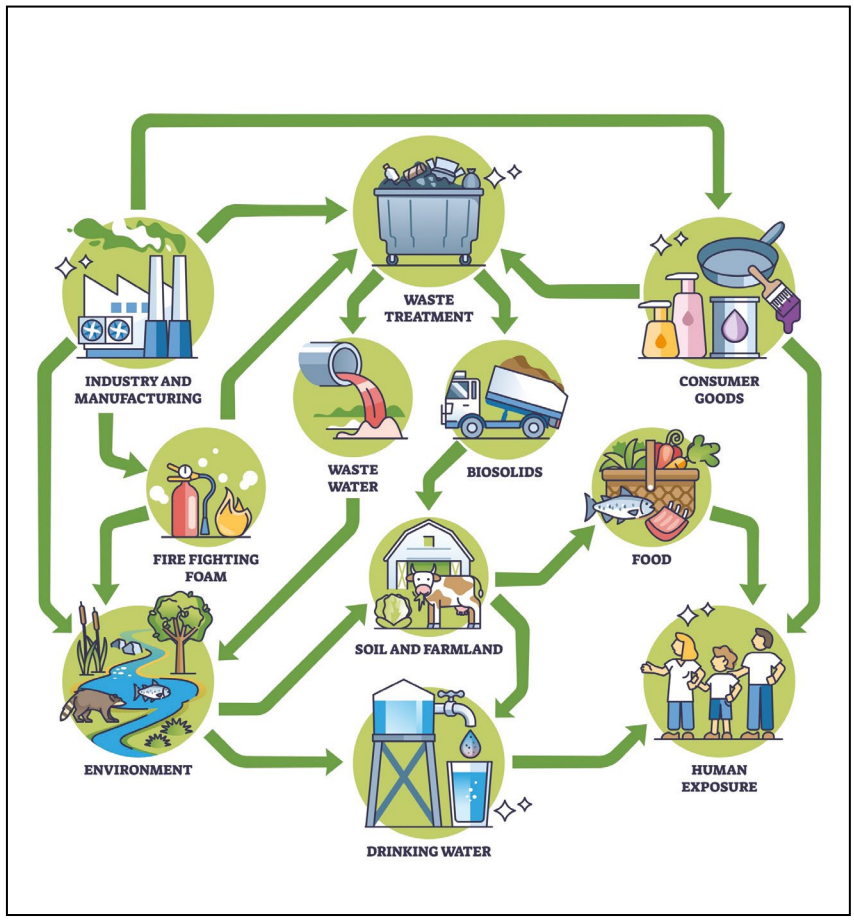
With widespread historical use and a long half-life, PFAS chemicals and their impact on human health and the environment have evolved from a health and environmental concern into a major driver of global litigation and regulatory activity and a significant insurance risk.

Regulatory landscape

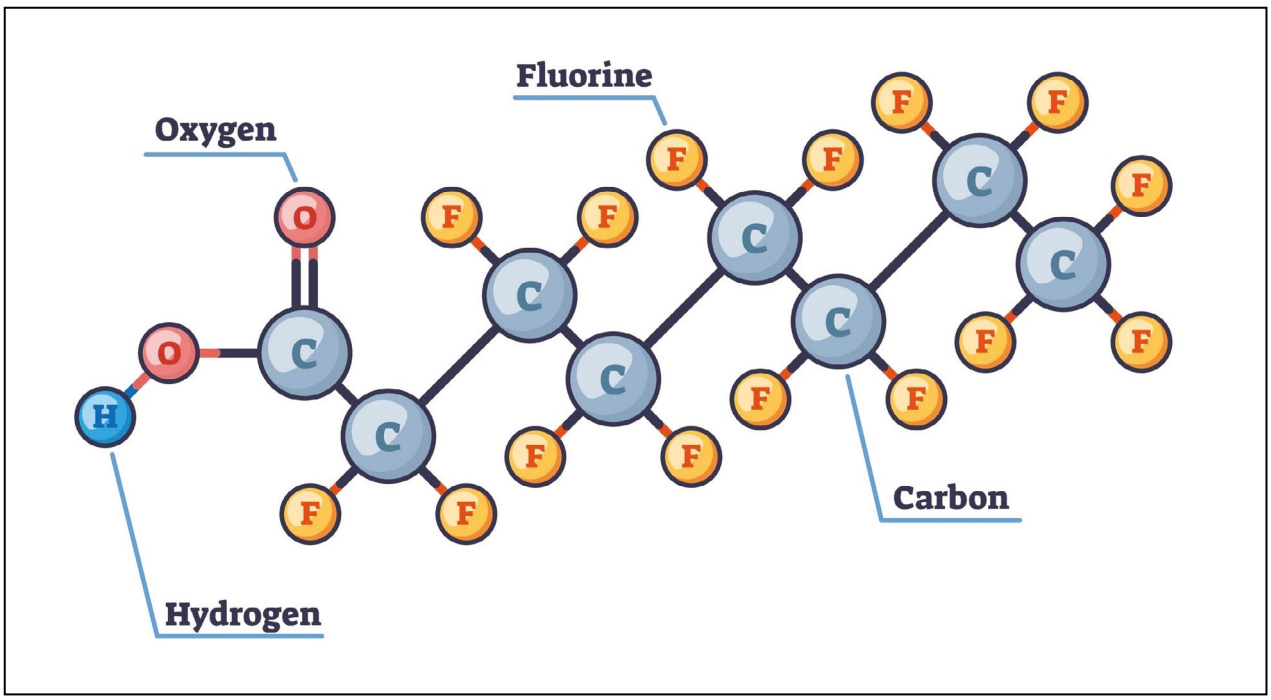
PFAS regulation is arguably most advanced within the EU, with the Drinking Water Directive enforcing low maximum concentration limits and other measures, such as mandatory monitoring of food and baby formula, having already been implemented. In August 2025, the European Chemicals Agency published an update to its 2023 proposal to further restrict PFAS. The proposed restrictions could apply to more than 10,000 PFAS across the EU with the European Chemicals Agency (ECHA) considering a number of regulatory options across different PFAS applications and sectors – from a full PFAS ban to allowing continued use under strict conditions designed to control emissions.

UK REACH requires PFAS manufacturers to understand the hazards associated with PFAS chemicals, and to take steps to minimise risks to human health and the environment. A consultation on a potential restriction on PFAS in fire-fighting foams is currently underway with regulatory tightening likely after the consultation ends in February 2026.

In the US, President Trump had previously vowed to combat the spread of PFAS in the face of mounting litigation and growing concerns over PFAS links to cancer but the Environmental Protection Agency has now pulled back on



PFAS risks flow from industry to humans



PFAS molecular structure

implementing stricter drinking water limits for PFOA and PFOS until 2031, citing economic concerns. The reversal has alarmed scientists and activists who fear it may lead to regulatory inertia. Nevertheless, many manufacturers, such as 3M, have announced that they will stop manufacturing PFAS, despite the lack of clear regulations or restrictions, citing increased regulatory trends and consumer concerns over PFAS health and environmental impacts.

Litigation trends

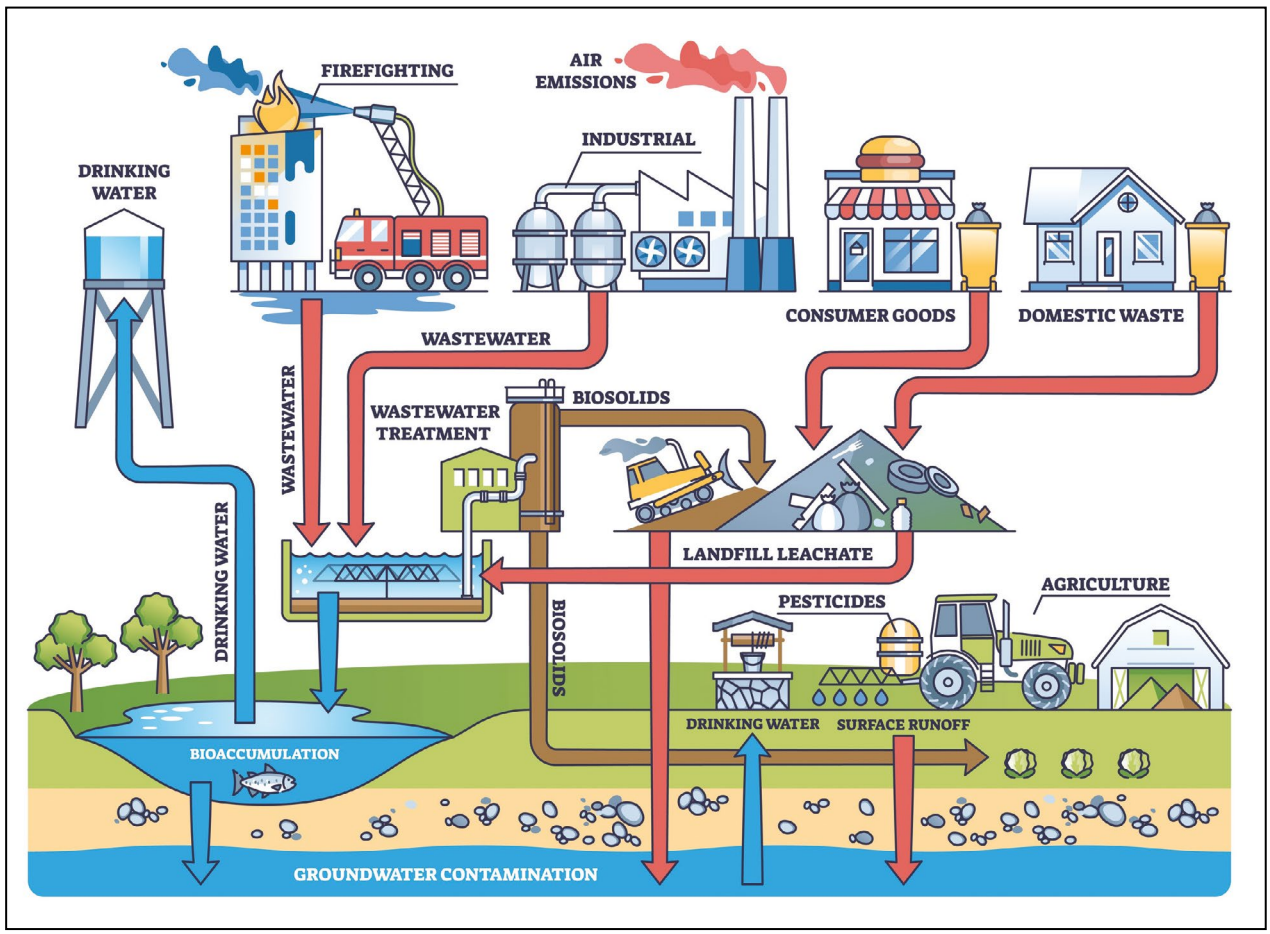
Amid the evolving regulatory landscape, PFAS litigation across the globe continues. Manufacturers 3M and DuPont, for instance, have both agreed settlements worth billions to resolve PFAS claims. In June 2023, 3M agreed a settlement of up to US$12.5 billion to resolve claims from a group of US public water systems for PFAS contamination stemming from AFFF firefighting foam. The settlements were reached in the course of the AFFF Multi District Litigation, the most significant aggregation of PFAS claims globally. The AFFF MDL is now considering personal injury claims from plaintiffs including veterans and military families exposed to AFFF. Rumours of a potential settlement of these personal injury claims have seen a surge in filings with 37,446 new claims filed in just one week in September 2025.

Despite a seemingly endless pool of potential plaintiffs (studies suggest that 97 per cent of Americans have PFAS in their blood) there has been some judicial caution in how broadly the class action net is cast. In Ohio, a court rejected a certification of a class of nearly 12 million residents, making it clear that plaintiffs must identify a plausible pathway between a defendant's products and their illness – a bar that may be more easily met in the context of occupational exposure.

Questions of causation will be a significant hurdle for plaintiffs globally seeking damages arising out of PFAS exposure and the issue is far from settled, despite the extensive PFAS settlements in the US.

US plaintiffs seeking to expand the pool of defendants from PFAS manufacturers to secondary users of PFAS in cosmetics and food packaging are working around the causation issue by basing claims on allegations of fraud or false advertising where companies market products as "all natural" or "non-toxic" despite PFAS content. Such claims avoid the science-intensive burden of proving bodily harm or environmental damage and rely instead on deceptive trade practices laws – a potentially lower bar for plaintiffs to meet.

Outside of the US, EU directives designed to facilitate representative actions have given consumer groups and government entities the standing to bring class actions on behalf of groups of consumers and across



The PFAS problem presents challenges across multiple industries and, by extension, insurance lines

multiple member states. Coupled with the growing use of third-party litigation funding in jurisdictions including the Netherlands, Belgium and France (where major PFAS manufacturers operate), this is expected to lead to an increase in large scale PFAS litigation across Europe.

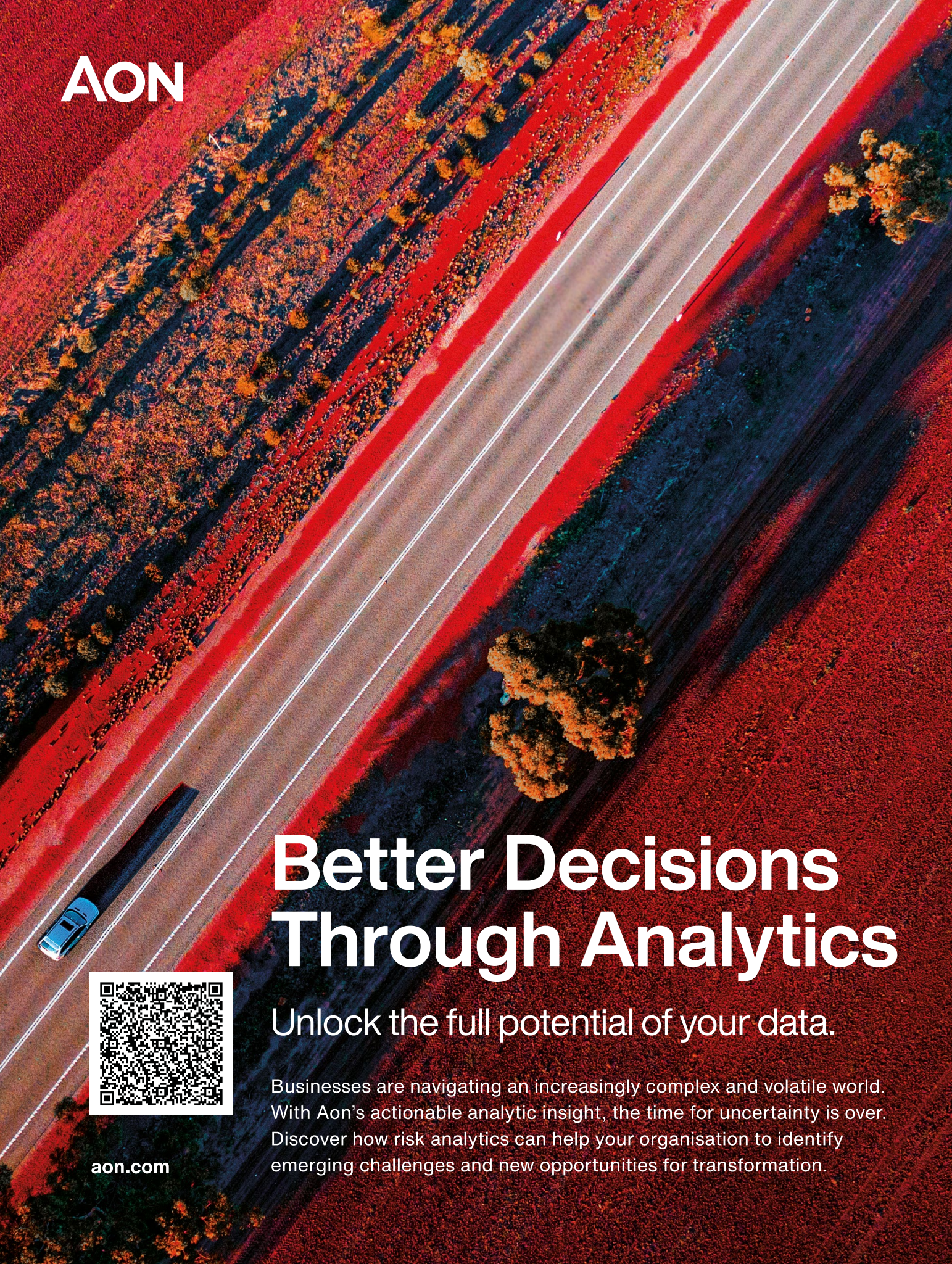
A long-tail, multi-line threat

The PFAS problem presents challenges across multiple insurance lines with claims stretching across time and geography. PFAS contamination may persist for decades after manufacture ceases, raising questions around policy trigger and allocation. One certainty is that the global societal cost of PFAS will be immense, with a report from non-profit Chemsec estimating the annual cost at around US$17.5 trillion, including healthcare and costs of removing PFAS from contaminated soil and water.

The evolving PFAS landscape requires a proactive approach to risk management and underwriting as jurisdictions develop new regulatory standards and the litigation landscape evolves. For claimants, tightening regulation, developing science, class action directives and litigation funding will be powerful drivers of litigation. For defendants, evolving standards mean that compliance today may not insulate them from future claims. Developing testing for PFAS and scientific study may also uncover as yet unknown sources of contamination or damage which will increase liabilities.

PFAS has evolved into a systemic, cross-sectoral risk with implications for litigation, regulation and insurance that will endure for decades. As the "forever chemical" continues to test the boundaries of liability, only those with a forward-looking risk perspective will stay ahead of the liability curve.

Laura Madders is a partner at Kennedys


AON
Better Decisions Through Analytics
Unlock the full potential of your data.
Businesses are navigating an increasingly complex and volatile world. With Aon's actionable analytic insight, the time for uncertainty is over. Discover how risk analytics can help your organisation to identify emerging challenges and new opportunities for transformation.
aon.com

From firefighting to foresight

Information security is evolving from a defensive discipline into a strategic advantage. *The 2025 State of Information Security Report* reveals how organisations are shifting focus from fear and prevention to resilience, trust and the ability to adapt under pressure

For two decades, organisations have defined information security by fear – fear of breaches, fines and reputational damage. But the *State of Information Security Report 2025* from IO (formerly ISMS.online) indicates that information security is undergoing a fundamental change in its approach – not because the risks have diminished, but because business leaders now face them with a clearer understanding and stronger determination.

The report, based on insights from 3,000 professionals across the UK and US, reveals a profession now setting the pace rather than trying to keep up with it. Leaders recognise that attackers move at high speed while regulations multiply and evolve; as a result, organisations need clear structures and systems to achieve effective information security. Preventing incidents remains essential, but the focus for information security professionals is shifting towards the ability to recover, continue operating and prevail despite a breach or cyber attack.

Resilience is now a defining pillar of organisational strength. As IO CEO, Chris Newton-Smith, puts it: "Security isn't a moat anymore. It's a market signal. It tells your customers, your partners and regulators that you're built to last."

Defence becomes diplomacy

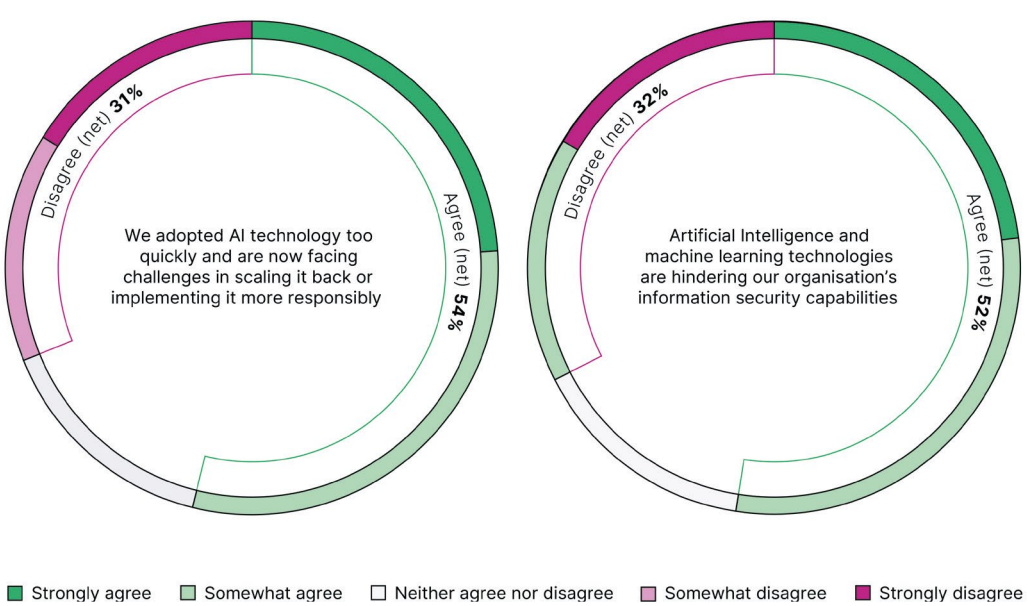
Forty-one per cent of organisations now cite third-party risk as their leading organisational challenge, surpassing ransomware, phishing and even cloud security concerns.

The security discussion is extending past traditional perimeter defence. The new security landscape is focusing on interdependence.

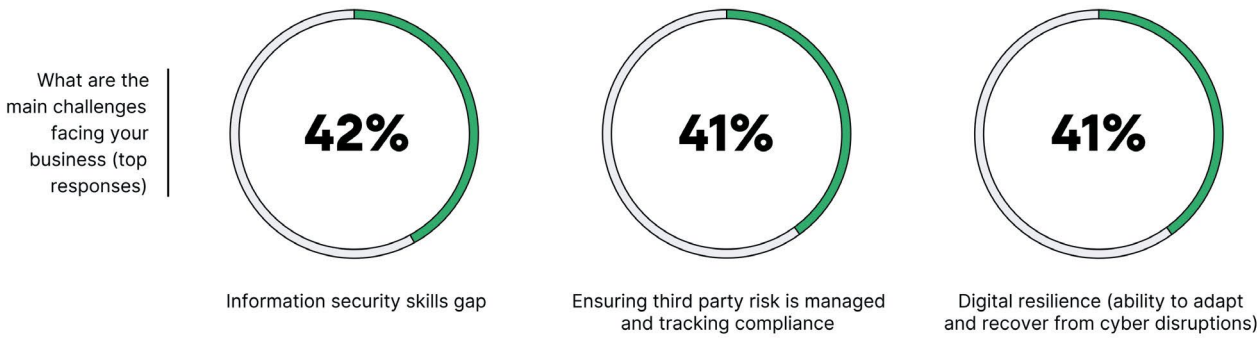
"Security isn't a moat anymore. It's a market signal. It tells your customers, your partners and regulators that you're built to last"

"The supply chain has become the audit trail," Newton-Smith observes. "If you can't prove assurance, you're not just insecure, you're commercially excluded."

That change marks a fundamental shift in how information security



To what extent do you agree or disagree with the following statements about the current state of the information security landscape?



generates value. In a risk-conscious economy, standards such as ISO 27001 and the emerging ISO 42001 are serving as essential entry credentials for businesses seeking to enter, and indeed remain, in the tech supply chain.

Inside the organisation, the challenge appears different but is equally structural. The report reveals that forty per cent of respondents identified shadow IT as their top vulnerability, and 37 per cent pointed to shadow AI. Both speak to innovation that outpaces oversight, highlighting a governance gap rather than a failure of ambition.

As Sam Peters, IO's chief product officer, notes: "Shadow AI isn't the villain. It represents a positive indicator of innovative thinking. The challenge lies in how to govern it without suffocating the potential it can offer."

"Shadow AI isn't the villain. It represents a positive indicator of innovative thinking. The challenge lies in how to govern it without suffocating the potential it can offer"

Information security, in this sense, has become a diplomacy of its own, balancing rapid operations with security, free thinking and management oversight. The results of trust building efforts become quantifiable outcomes when proper procedures are followed.


Chris Newton-Smith


Sam Peters

The age of AI realism

If 2023 was the year of AI hype and 2024 the year of AI panic, 2025 is shaping up to be the year of AI realism.

Seventy per cent of organisations have already deployed AI or machine learning tools and another 19 per cent plan to follow suit within the year. Yet more than half (54 per cent) now admit they moved too quickly and are struggling to retrofit governance.

The result is a surge in the quiet use of unapproved or unvetted tools. IBM data suggests that shadow AI contributed to one in five breaches last year. Yet AI is also fast becoming a cornerstone of defence: 96 per cent of respondents plan to invest in GenAI-powered threat detection, while 94 per cent are adopting deepfake detection and validation technologies.

Newton-Smith captures the duality of AI use in describing AI is both "an amplifier and a stabiliser".

"The differentiator will be who governs it, not who adopts it first," he explains.

The clearest signal of this shift is the extraordinary rise of ISO 42001, the new AI management standard. In 2024, just two per cent of organisations required suppliers to comply. This year, that figure has risen to 28 per cent. In a single year, AI governance has moved from an emerging concern to a supply chain expectation.

It is a reminder that trust, not innovation, may prove to be the ultimate competitive advantage in the age of intelligent systems.

Resilience economics

For all the talk of technology, the most significant trend in the report may be economic.

Information security is no longer a cost centre; it's a performance lever. Forty-four per cent of organisations report that compliance frameworks have improved decision-making. Forty-two per cent say they've strengthened customer retention. Thirty-five per cent have unlocked new business opportunities as a direct result of stronger information governance.

These are the dividends of trust, measurable returns on the hard work of doing things correctly.

But progress comes at a cost. Forty-two per cent of respondents report a widening skills gap, 32 per cent cite burnout, and nearly a quarter still struggle to secure consistent leadership buy-in. Information security may have entered the boardroom, but it hasn't yet solved the resource equation.

"Ninety one per cent of respondents are funding quantum risk-readiness initiatives, an extraordinary statistic given its distance from commercial reality"

Peters sees this as part of the growing pains of maturity. "We're watching compliance evolve into culture," he notes. "Once that happens, resilience stops being a report metric and starts becoming a reflex."

From breach to behaviour

The report suggests that organisations are beginning to internalise that shift. Eighty-one per cent are aligning with recognised standards; 96 per cent list achieving or maintaining certification as a business priority.

The focus is no longer just on preventing incidents, but on institutionalising behaviours that make response and recovery instinctive. It's a pivot from control to coordination, from isolated security efforts to organisation-wide preparedness.

Newton-Smith says: "You can't bolt on resilience after an incident. It has to be lived in every decision, every system, every conversation."

This is where information security starts to blur into culture. The companies that perform best under stress are those that already understand their interdependencies between platforms, people and processes – long before a crisis hits.

The new geopolitics of assurance

The external environment has only intensified that pressure. Nearly nine in ten organisations now fear state-sponsored attacks. Almost a quarter admit they are not prepared for large-scale geopolitical disruption.

That anxiety is pushing investment in new forms of preparedness. Ninety one per cent of respondents are funding quantum risk-readiness initiatives, an extraordinary statistic given the technology's distance from commercial reality. But it underscores a more profound truth: assurance has become the new diplomacy.

As Peters observes: "Information security is now the language of trust between economies. It's how we prove reliability in an unstable world."

The modern business case for information security is therefore not defensive but existential. It's how organisations preserve their licence to operate, not just with regulators, but with customers, suppliers and markets.

The end of fear

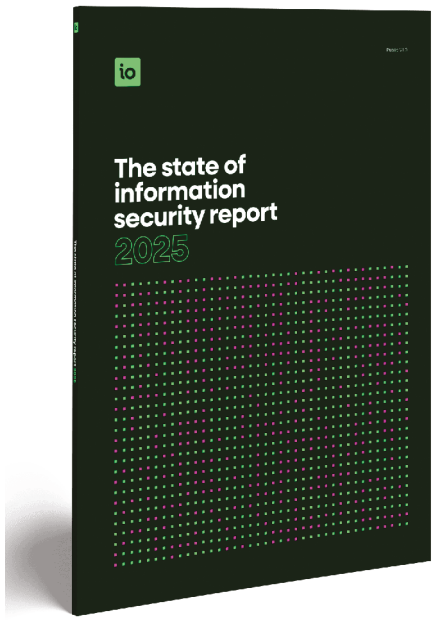
The State of Information Security Report 2025 captures a sector at an inflexion point, moving beyond the reactive era of breach response toward a more composed, anticipatory form of resilience.

Organisations aren't learning to live with risk; they're learning to master it. They know they can't eliminate every threat, but they can build systems that endure, recover and adapt.

Standards once seen as bureaucratic hurdles are now the frameworks that make that agility possible. Compliance has become the architecture of confidence.

As Newton-Smith puts it: "We've spent twenty years defending ourselves from the internet. Now we're learning how to thrive within it."

That shift, from fear to foresight, may be the defining story of information security in 2025: not the fight against threats, but the race to build resilience faster than the world can break it.



Find out more and download *The State of Information Secutity Report 2025* at www.isms.online/the-state-of-information-security-report-2025/

Beat compliance fatigue

As teams grow, so do compliance headaches.

Spreadsheets, scattered evidence, and constant updates slow everyone down. ISMS.online brings it all together, so your people spend less time chasing checkboxes and more time delivering real value.

ISMS.online makes staying compliant easy, efficient, and stress-free.

That's the io way.

isms·online

CIR | Risk Management AWARDS 2025

The 16th annual Risk Management Awards

The pinnacle of achievement in risk management

BOOK YOUR TABLE

20th November 2025
London Marriott Hotel, Grosvenor Square, London

cirmagazine.com/riskmanagementawards

@CIR_MAGAZINE #RISKMANAGEMENTAWARDS

Headline partners

irm
Institute of Risk Management

THE INSTITUTE OF OPERATIONAL RISK
An IRM Group Company

Sponsored by

AON

HORIZONSCAN
RISK - RESILIENCE - READINESS

Supported by

airmic

ALARM
embrace risk

CIR
CONTINUITY INSURANCE & RISK

BUSINESS CONTINUITY SOFTWARE REPORT 2026

CLDIGITAL

FUSION
RISK MANAGEMENT

shadow planner

Market analysis

In an ever-changing, complex risk landscape, business continuity software is being brought closer to day-to-day operations and strategic decision-making. David Adams takes a look at how today's enhanced solutions are being used at the coalface

Day-to-day operations in complex organisations have been transformed over the past 25 years by digital technology and globalised supply chains. These changes have altered the risk landscape too, as new cyber threats and climate risks have emerged. As a result, business continuity planning and management processes have evolved into important strategic tools. In many cases the business continuity function is no longer a largely manual function at the edge of an organisation, but is instead an integral and critical part of operational and strategic processes.

The effectiveness – or otherwise – of business continuity processes and solutions is also now a source of interest – and anxiety – in boardrooms. It's easy to see why: 2025 has seen some hugely damaging continuity incidents, including a cyber attack on Jaguar Land Rover in Autumn that halted production for five weeks and severely disrupted the cashflows and operations of 5,000 businesses in JLR's supply chains. In the year to October 2025, the UK was affected by a record 204 "nationally significant" cyber attacks, up from 89 the previous year, according to the National Cyber Security Centre, among many more damaging incidents affecting businesses and other organisations worldwide.

"The business continuity function is no longer a largely manual function at the edge of an organisation, but is instead an integral and critical part of operational and strategic processes"

But 2025 has also been a record-breaking year for continuity incidents linked to climate risks. For example, during the first half of the year, 14 separate extreme weather events that each caused at least US$1 billion worth of damage hit the US, including the Los Angeles wildfires. Collectively these events cost US$101 billion – a half year record that does not even include the costs of severe flooding in Texas in June.

Leane Willis, a vice-president at Riskonnect who is about to take over management of the vendor's business continuity and resilience team, says the volume, scale and impacts of such high-profile incidents have put business continuity threats at the forefront of many decision-makers' minds.

"There is a focus from boards and executives to make sure they have a solid business continuity platform, being tested regularly," she says.

Tejas Katwala, co-founder and CEO of CLDigital, believes such concerns have also accelerated a shift away from periodic testing and refinement of business continuity plans.

"What organisations are looking for today is a system that helps them run resilience day-to-day," he notes. Yet in many cases, he says resilience leaders are also being asked to do more with less resource and less time. This is one of the reasons why more end user organisations are attracted to software that harnesses automation and AI-based technologies to accelerate risk and business impact analysis processes.

CLDigital's 360 software offers a no code solution that automatically builds relationships between people, processes, technology and assets; and can be integrated with crisis management, disaster recovery and risk management functions. End user organisations include a major UK financial services business for which automation within the business continuity and resilience function has accelerated the process of updating plans each time a business service is changed, "from 40 hours of effort to a couple of clicks and a couple of minutes", Katwala claims.

Regulatory pressures

As ever, regulation is also driving investment in software. For most financial services firms, the primary focus is compliance with the EU's Digital Operational Resilience Act, which mandates stronger ICT and third party risk management, incident reporting, and operational resilience testing. Similar regulations also now apply in many other jurisdictions and are being rolled out in other industries.

"DORA requirements go beyond regulated industries and we're seeing the same impacts in other parts of the world – in some Asian countries, for example," says Dave Vonk, chief revenue officer at Fusion Risk Management.

Regulation is also encouraging smaller businesses to implement business continuity software solutions: Katwala cites a new CLDigital end user in the financial services sector that had previously relied on Word documents and spreadsheets to run its business continuity function.

"It's now difficult for any size of organisation to get away with that,"

he says. "Organisations of all sizes are being asked by regulators to show them their resilience plans, show they are being tested and show the outcomes of those tests." Again, increased use of automation helps to make this possible in a cost-effective way.

It's not just the threat posed by cyber risks and the need to comply with regulation that are encouraging adoption of business continuity solutions, says Gary Lynam, managing director, EMEA, at software vendor, Protecht. There is also a more general desire to gain a better understanding of business resilience to help inform strategy.

He believes improvements to the use of visualisation in business continuity software have helped many senior decision-makers attain a deeper understanding of business resilience. For example, scenario planning is assisted by organisations "looking more horizontally and laterally, so they have a better understanding of where vulnerabilities sit within the organisation".

That includes the supply chain. User-friendly business continuity software that harnesses automation to help plan and test responses to incidents is becoming an ever more attractive and cost-effective option for businesses operating within the supply chains of larger entities.

The influence of AI

Meanwhile, AI-based technologies are exerting more influence over the deployment and evolution of business continuity software.

"Everyone wants to say that AI is helping organisations predict things, or give amazing answers to their risk assessments," says Katwala. "I think all of that will happen, but today what we see more often is AI being embedded into resilience processes to do a lot of the manual work, so that resilience

leaders can focus on strategy."

Fusion is using AI to help design testing scenarios and simulated responses, but is also using agentic and generative AI tools to power a feature called Fusion Intelligence, which it describes as an end-user organisation's "in-house Fusion expert", able to draw on the company's expertise and understanding of best practice to accelerate and enhance business continuity capabilities.

"We are creating agents to provide guidance to executives about what a risk would be, evaluating it and prioritising actions to manage its implications," says Vonk. In the event of a continuity incident, one of these AI agents might act as an "incident commander", advising the company on optimising responses – in order to prioritise restoring services to a specific group of customers, for example.

Vonk says end users adopting Fusion's AI-based capabilities include businesses in the oil and gas industry, in financial services, and in the aerospace, pharmaceutical, and industrial and manufacturing sectors.

"Today we're seeing AI being embedded into resilience processes to do a lot of the manual work, so that resilience leaders can focus on strategy"

Use of AI-based predictive capabilities in business continuity functions will be here soon, says Katwala. He believes machine learning will make this a reality, drawing on large pools of shared, anonymised data supplied from multiple sources. But progress will depend on more collaboration and information-sharing between businesses. Although mandated to some extent by regulations including DORA, this type of collaboration is not yet happening at the scale needed to support this sort of capability.

Of course, any vendor or business working with AI must also do so armed with an understanding of the potential risks it could create, particularly as they relate to regulation.

"One of these AI agents might act as an 'incident commander', optimising responses in order to prioritise restoring services to a specific group of customers"

"The risk is leaning too much on AI and taking out some of that human element," says Riskonnect's Willis. "At the moment, when we do a business impact analysis we have someone looking at the end user organisation's processes and dependencies, then you might use AI to look at it again. Experts are always in control of that, and having an ongoing conversation about it. If using AI were to take some of that conversation away, that might mean a gap in resilience is missed."

With different aspects of AI being harnessed alongside increased use of automation, the future for software certainly looks very positive, and closer to the heart of end user organisations' operations and strategies than ever before.

"We see the future of resilience software and business continuity software as a resilience operating system, where operations continuously validate an organisation's readiness," says Katwala. "Resilience has moved from the basement to the boardroom."

ALIVE-IT CONTROLLER AG

alive IT is designed to automate business continuity management and IT service continuity management simply, efficiently and reliably. The software is designed to support users from analysis and emergency planning through to orchestrated recovery, with the goal of making testing more transparent. With over twenty years experience in the market, this product has been continuously developed and adapted to international standards. With customisation that is designed to be flexible, automated interfaces, and practical features, it promises to help avoid duplicate data maintenance.

CONTINUITY MANAGER 4C STRATEGIES

Continuity Manager (current release v22.4.3.1) is designed to digitalise and automate continuity and resilience management. The software provides an integrated environment for identifying critical services, assessing dependencies, managing risks, developing continuity plans and validating them through scenario-based testing and lessons management.

Available as Core, Pro and Custom editions, the software is designed to scale from departmental deployments to global enterprise resilience programmes.

The Core version provides foundational capabilities, including service identification, dependency mapping, business impact analysis visualisation and plan management. The Pro version extends this with AI-assisted analytics, scenario libraries, regulatory compliance evaluation and workspace collaboration. The Custom version supports enterprise integration, advanced reporting formats and configurable workflows, and is designed to align fully with complex organisational structures and regulatory frameworks.

The next scheduled update (v23 series, early 2026) promises enhancements to the AI-driven scenario testing module, enabling probabilistic stress modelling and automated generation of recovery plan recommendations. Additional development includes expanded Insights APIs for data exchange with third-party risk, audit and ITSM tools and improved user-experience design for large multi-workspace deployments.

Continuity Manager is designed to support cross-sector operational resilience, business continuity and disaster recovery management. It is used by financial institutions to map Important Business Services and test impact tolerances under regulatory frameworks such as the UK PRA/FCA rules; by utilities and government agencies to analyse critical dependencies; and by global enterprises to integrate business continuity with cyber, IT and physical risk programmes.

Standard onboarding is delivered remotely, with Core implementations typically live within five weeks and Pro within seven weeks.

Continuity Manager is hosted in ISO 27001-certified datacentres (Microsoft Azure in North America and Europe) with options for on-premise or hybrid deployment. Information security includes Entra ID SSO, MFA, role-based access control and full audit logging. The software is licensed via annual SaaS subscription, with optional modules including Mass Notification, Compliance and Evaluation and Lessons Management. The Custom edition supports enterprise licence and private cloud models. Pricing scales by user count and feature tier.

BUSINESS CONTINUITY & RESILIENCE RISKONNECT

Riskonnect's Business Continuity & Resilience software is designed to help organisations build operational resilience. Built on ISO 22301, the platform is designed to unite business continuity, crisis management, threat intelligence and notifications in one solution.

Designed with accessibility in mind, Riskonnect combines enterprise-grade functionality with a simple, intuitive interface. The platform is designed so that even the most casual user can engage without recurring training or a dedicated administrator.

Key features include a business model definition tool that is designed to create a consolidated, dynamic view of dependencies across processes, applications, facilities and suppliers.

Operational resilience capabilities are designed to help organisations identify critical products and services, set impact tolerances and map the end-to-end value chain.

Integrated BIA and risk assessments are designed to highlight vulnerabilities, while strategy tools are intended to guide users in reducing disruption and protecting outcomes.

The Reality Risk & Resilience Leaders Face

More regulations. Fewer resources. Higher stakes.

- **Regulations** keep growing, but budgets and tools don't.
- **Disconnected data** and slow reporting create blind spots.
- **Outdated platforms** make programs reactive instead of resilient.

CLDigital helps teams break free from spreadsheets to focus on what matters most — **building lasting resilience.**

CLDIGITAL

SCAN HERE TO FIND OUT MORE

Crisis management and notification functions are designed to transform static plans into actionable playbooks. Exercises, dashboards, What-if analysis, workflow automation, API integration and AI-powered threat intelligence are designed to provide deeper insight and proactive preparedness.

A mobile app connects users with their continuity programme wherever they are, ensuring critical plans, documents and actions remain accessible on-the-go and off-network. Multi-language capabilities and global 24/7/365 support make Riskonnect suitable for complex, multinational organisations.

CLDIGITAL

CLDIGITAL 360
CLDIGITAL

CLDigital 360 is a no-code platform designed to help organisations manage risk, resilience and compliance without vendor reliance. Built for agility, it is designed to allow teams to modify workflows, forms and dashboards as needs evolve.

Reporting tools provide real-time visibility and actionable insights across the enterprise. With integration capabilities and support for emergency notifications, CLDigital 360 is designed to fit into existing systems, while AI-driven automation and analytics streamline processes.

This tool supports a wide range of use cases, including business continuity, operational resilience, crisis management and third-party risk.

Available via cloud, on-premise or FedRAMP environments, it promises secure, scalable deployment while aligning with global standards such as ISO 22301, NIST and DORA.

cldigital.com

CRISES CONTROL
CRISES CONTROL

Crises Control is a critical event management platform designed to help organisations of all sizes plan, prepare for and respond to emergencies and crises. The system is designed to streamline communication, enhance situational awareness and ensure compliance through real-time alerts and coordinated task management.

The platform is designed to manage incidents from initiation to resolution. Users can activate contingency plans, assign tasks and monitor progress in real time to support a coordinated and efficient response. Crises Control automatically records all actions and messages to provide a complete audit trail, support regulatory compliance, and facilitate post-incident analysis and reporting.

Accessible via mobile apps for iOS and Android, Crises Control is designed to allow users to manage incidents and communicate while on the move. The platform also integrates with Microsoft Teams to enable collaboration within existing workflows.

The tool enables rapid communication by allowing users to send alerts via SMS, email, phone calls and push notifications through the app and Microsoft Teams. The platform includes an incident plan builder that is designed to guide organisations in developing effective response plans, creating mitigation strategies and testing preparedness for varied crisis scenarios. It also incorporates CRAiG, an AI-driven crisis resolution guide that is designed to provide real-time recommendations and best practice guidance to support decision-making during emergencies.

24/7 support and training programmes are designed to ensure organisations can use Crises Control effectively and respond to crises quickly. The platform serves sectors including healthcare, finance, transport, education, manufacturing, retail and energy.

Crises Control operates worldwide, including North and South America, Europe, the Middle East and South Asia. It is not currently available for use in China and Russia.

FUSION RISK MANAGEMENT

FUSION FRAMEWORK SYSTEM
FUSION RISK MANAGEMENT

The Fusion Framework System is designed to help organisations build comprehensive and dynamic business continuity programmes. Developed by Fusion Risk Management, it is designed to provide a full understanding of how a business operates, and where it can adapt under pressure without disrupting service delivery.

The platform is designed to remove the barriers that create the need for separate applications across business continuity, disaster recovery and crisis

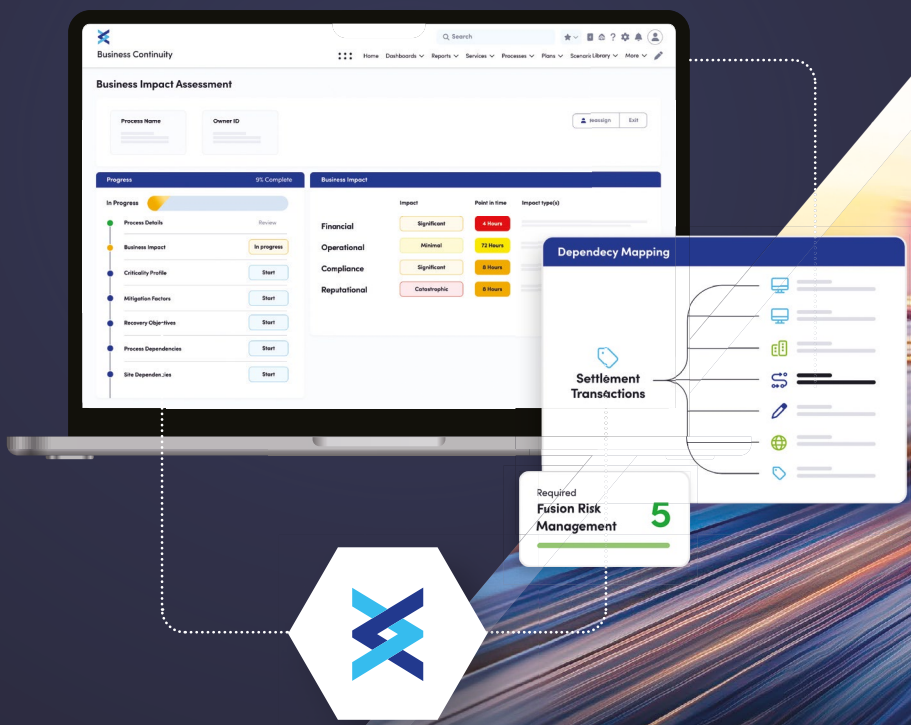
FUSION
RISK MANAGEMENT

FALL 2025
Leader

Readiness You Can See, Prove, and Trust

Fusion unifies and aligns enterprise data to deliver full visibility and control. Intuitive dashboards and AI-led simulations demonstrate real-time readiness, while auto-curated response plans enable faster, more effective recovery.

Discover how Fusion's leading enterprise resilience software keeps you ready for anything. Visit fusionrm.com today.



and incident management. It promises to give users a complete understanding of their organisation through a unified system. Fusion provides a standard framework that integrates data across all disciplines, making it easy to analyse a complete programme in one single place.

Integrated continuity capabilities are designed to help users build and execute plans, carry out risk and impact assessments, and evaluate organisational preparedness and response. Governance and management functions incorporate configurable reference data taxonomies, libraries and scoring methodologies, together with customisable workflows, approvals and notifications that automate administrative tasks. Predictive risk analytics features tolerance-based metrics and configurable thresholds to drive automated notifications, alerts and reports from one integrated dashboard.

The platform includes an AI-powered scenario simulation and intelligence function designed to test likely scenarios, show compounding effects, and provide an holistic view of potential impacts. This functionality promises to help teams make informed decisions and proactively mitigate disruption to key business services. Scenario Simulation and Intelligence can run thousands of variations of a single scenario, enabling early identification and mitigation of potential problems.

Built on the Salesforce Lightning Platform, Fusion is designed to help organisations navigate fast-moving change by mapping how they deliver important services and products, forecasting where value chains are at risk of failure, and managing the risks and events that create disruption. Fusion and its platform have supported continuity programmes for nearly twenty years, and play an active role in advancing operational resilience.

fusionrm.com

INONI 365
INONI

Inoni 365 is a business continuity and resilience management solution designed for small and medium-sized enterprises. It offers a best practice and standards-aligned management system that is designed to be simple to implement and maintain, reducing the need for extensive in-house administration, expertise and resources.

Inoni 365 is a cloud-hosted software service built on the Microsoft Power Platform, which includes comprehensive consulting implementation. This helps users achieve a best practice position quickly and with minimal disruption.

The service is designed to deliver practical, standards-aligned business continuity plans that address all potential threats across all relevant departments and sites.

The solution supports the full business continuity management lifecycle, including a card system that provides focused site, scenario and role responses.

Inoni's consultants assist with implementation through software set-up, discovery workshops, production and delivery of standards-aligned documents, system walkthroughs, and ongoing support.

The software is built using Microsoft Power Apps, and can be hosted within the user's own Microsoft 365 tenancy. This approach is designed to enhance productivity and efficiency; integrating with other Microsoft products and a range of third party services.

The platform's user-friendly interface and extensive templates make it accessible to users of all skill levels, while robust security features promise data protection. AI integrations within Inoni 365 further enhance its capabilities by enabling such features as predictive analytics, natural language processing and automated workflows. These AI-driven functionalities are intended to help businesses make data-driven decisions, automate routine tasks and improve overall operational efficiency.

Inoni 365 is particularly beneficial for organisations in financial services, healthcare, manufacturing, retail and e-commerce, education and technology, as well as for SaaS providers.

LOGICMANAGER
LOGICMANAGER

LogicManager is a cloud-native enterprise risk management platform designed to help organisations apply a risk-based approach across business continuity, cyber security, privacy, compliance, third-party risk, internal audit and incident management.

Core components include configurable taxonomies for processes, business units, assets and vendors, reusable risk and control libraries, and linked assessments designed to ensure programmes share data and evidence

rather than operate in silos.

At the centre of LogicManager is its relationship model, which is designed to map how risks, controls, vendors, applications, processes and continuity plans interconnect. The platform propagates impacts and dependencies to show how an outage, control failure or supplier issue affects downstream operations and objectives. This structure is designed to power scenario analysis and help continuity teams identify affected locations, suppliers or functions. It supports a risk-based approach by linking strategic goals, risks and mitigations across the enterprise.

LogicManager Expert is an in-app, AI-powered assistant designed to accelerate user adoption and configuration. It provides contextual guidance, best-practice recommendations and direct links to wizards or reports, reducing set-up time and enabling users to follow a consistent risk-based framework without requiring technical support.

A Completeness Checker is designed to validate the integrity of each programme by reviewing relationships, workflows and dependencies. It highlights unlinked controls, unmonitored risks or missing recovery dependencies and guides users to close those gaps before audits, exercises or attestations. The tool is designed to ensure completeness and traceability across programmes, strengthening governance confidence.

Organisations use LogicManager to perform BIAs, maintain and test business continuity and disaster recovery plans, and link them to upstream risks and downstream dependencies. Exercises, incidents and corrective actions tie back to plans and controls for assurance. Security and privacy programmes use linked controls, qualitative tests and quantitative metrics to monitor performance and compliance. Policy management supports versioning, attestations and exception workflows through LogicManager's issues and findings process.

Multi-stage, role-based workflows define stages, SLAs, required evidence and notifications to embed accountability into governance processes. Automation rules are designed to trigger actions, reminders and escalations based on time or data conditions.

LogicManager's no-code Integration Hub is designed to connect to identity and business systems for synchronised data and automated assurance. Common integrations include SSO, RESTful APIs, file and SFTP feeds and ticketing handoffs with Jira or ServiceNow. Prebuilt connectors are maintained by LogicManager to reduce IT administrative effort.

Configurable dashboards and reports are designed to give visibility into risk exposure, control effectiveness, plan readiness and dependency coverage. Hierarchical drill-downs allow users to move from enterprise to process or asset level to assess materiality, performance and outstanding actions.

All subscriptions include access to advisory analysts and customer success support for configuration, content tailoring and reporting.

A programmes-based licensing model includes unlimited internal and external users and covers onboarding and advisory services without per-seat fees.

PDRWEB
SERVICES CONSEILS RDI

PDRWEB is a platform designed for business continuity and disaster recovery, supporting organisations of all sizes, from small enterprises to global corporations. The solution provides an interactive dashboard designed to give real-time visibility into plan status, BIA progress, maintenance activities, user activity and related metrics.

Using a configurable web-based survey, PDRWEB automatically calculates recovery time objectives based on activity dependencies and weighting factors. Department-level reports are generated, reviewed and approved, after which the platform creates fully structured continuity and recovery plans.

PDRWEB links activities, resources and dependencies across multiple plans to provide a complete dependency map that supports clarity and readiness. Users receive automated alerts that include the necessary information for task execution such as resources, contacts and diagrams. With AI-driven encryption and an integrated notification module provided by Services Conseils RDI, PDRWEB is designed to help organisations remain secure, responsive and resilient in the face of disruption.

PROTECHT
PROTECHT

Protecht is an enterprise risk management platform designed to help organisations manage operational resilience and business continuity as part of their broader risk framework.

	alive-IT	Business Continuity & Resilience	CLDigital 360	Continuity Manager	Crises Control	Fusion Framework System
Plan navigator	•	•	•	•		•
Dependency mapping	•	•	•	•		•
Graphical call list			•		•	
Location resource manager	•	•	•		•	•
Recovery site layout planning		•	•			
Automated notifications via multiple channels		•	•	•	•	•
Reports - own build	•	•	•	•		•
Process modelling capabilities	•	•	•	•		•
Technology modelling	•	•	•	•		•
'What if' analysis	•	•	•			•
Data collector	•	•	•	•		•
Automatic analysis	•		•	•		•
Simulation capability	•	•	•		•	•
Dynamic updating from database	•	•	•	•		•
User training available	•	•	•	•	•	•
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/Slack/Teams/ modern collaboration integrations	•	•	•	•	•	•
Multi-language capability - interface	•	•	•	•	•	•
Multi-language capability - user data			•		•	•
User roles and groups	•	•	•	•	•	•
Document update management	•	•	•	•	•	•
Comprehensive audit trails	•	•	•	•	•	•
AI support or integration		•	•	•	•	•
Regulatory mapping			•	•		•
Change control and tracking	•	•	•		•	•
Screen customisation	•	•	•	•	•	•
Continuous monitoring and automated insights (eg from cloud services, risk platforms; alerts on deviations or outages)		•	•	•		•
Sustainability / ESG reporting support			•			
Integration with collaboration tools	•		•	•	•	•
Integration with HR systems	•	•	•	•	•	•
Data residency and sovereignty options	•	•	•	•	•	•
Drag and drop	•	•	•		•	•
Offline continuity plan access	•	•	•	•		•
Integrates with EMN software	•	•	•	•		•
Published APIs for data interface	•	•	•	•		•
Deployment options (SaaS, on-premises, hybrid, data residency controls)	•		•	•		

Inoni 365	LogicManager	PDRWEB	Protecht ERM	Shadow-Planner	YUDU Sentinel	
•	•	•	•	•		Plan navigator
•	•	•	•	•		Dependency mapping
•		•	•		•	Graphical call list
•	•	•	•	•		Location resource manager
•		•	•			Recovery site layout planning
	•	•	•	•	•	Automated notifications via multiple channels
•	•	•	•	•		Reports - own build
•	•	•	•	•		Process modelling capabilities
•	•	•	•	•		Technology modelling
	•	•	•	•		'What if' analysis
•	•	•	•	•	•	Data collector
•	•	•	•	•		Automatic analysis
		•			•	Simulation capability
•		•	•	•	•	Dynamic updating from database
•	•	•	•	•	•	User training available
•	•	•	•	•	•	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/Slack/Teams/ modern collaboration integrations
•		•		•		Multi-language capability - interface
•	•	•		•	•	Multi-language capability - user data
•	•	•	•	•	•	User roles and groups
•	•	•	•	•	•	Document update management
•	•	•	•	•	•	Comprehensive audit trails
•	•	•			•	AI support or integration
	•	•	•	•		Regulatory mapping
•	•	•	•	•	•	Change control and tracking
	•	•	•	•	•	Screen customisation
•		•	•		•	Continuous monitoring and automated insights (eg from cloud services, risk platforms; alerts on deviations or outages)
	•	•	•			Sustainability / ESG reporting support
	•	•	•	•	•	Integration with collaboration tools
	•	•	•	•	•	Integration with HR systems
	•	•	•	•	•	Data residency and sovereignty options
	•	•	•	•		Drag and drop
		•	•	•	•	Offline continuity plan access
	•		•	•	•	Integrates with EMN software
	•	•	•	•	•	Published APIs for data interface
•		•		•		Deployment options (SaaS, on-premises, hybrid, data residency controls)

At the centre of the platform is an integrated business continuity and operational resilience solution designed to centralise continuity data across business units and critical services. Continuity plans, tests and recovery tasks are linked to the same users, workflows, risks, controls and assets managed within the broader Protecht environment so that resilience becomes a functional capability rather than a documentation exercise.

The system is designed to deliver visibility of critical services and their dependencies across people, processes, technology and vendors. It supports the full lifecycle of continuity management, including business impact analysis, plan documentation and approval, recovery team coordination, test execution, lessons learned and action management. Pre-built analytics provide reporting for boards and regulators covering continuity status, tolerances, test coverage and outcomes.

Protecht is designed to provide regulatory confidence through pre-configured content and dashboards that support compliance obligations under operational resilience regulations. Business continuity functionality aligns with standards including ISO 22301.

A purpose-built mapping tool ties services to processes, resources and disruption scenarios, highlighting resource health, criticality and RTOs to pinpoint vulnerabilities and communicate recovery design clearly.

The platform maintains a unified data model for risk, resilience and business continuity that removes duplication and delivers connected insights across registers for services, scenarios, processes, resources and recovery tasks. The BCM and Operational Resilience solution integrates with the Vendor Risk Management solution for third-party assets, and the Cyber Risk solution for information/hardware assets.

The company is introducing AI features into the platform with controls to support security, explainability and governance. In the near term, this includes AI-assisted scenario development, business impact analysis, test planning, plan reviews and post-incident updates. Over time, the provider plans to extend this with predictive resilience analytics and automated testing.

shadow planner

SHADOW-PLANNER
WAVENET

Shadow-Planner is designed to help organisations manage disruption effectively, enabling them to stay resilient and keep their business running smoothly.

With this tool, businesses can develop robust plans, assess potential risks and establish proactive strategies to mitigate the impact of disruption.

Designed by business continuity practitioners, this suite of integrated software supports the entire business continuity management and operational resilience lifecycle – from impact analysis through to developing strategies and plans to testing, reporting, and sending out emergency communications.

With this tool, users can map out critical dependencies, understand any gaps in capabilities, create plans and playbooks, and manage testing. It also provides oversight of a business continuity programme's adherence to policy.

shadow-planner.com

YUDU SENTINEL
YUDU

YUDU Sentinel is designed as a secure out-of-band communication platform designed to ensure that critical communications continue uninterrupted if the primary network is compromised or unavailable.

This platform provides secure chat, video crisis rooms, offline documentation and mass notification capability, within an encrypted, audited and independent environment.

CLDIGITAL

CLDigital
Floor 24/25, The Shard,
London Bridge Street, London, SE1 9SG

Tel: +44 (0)20 7770 6446
info@cldigital.com
cldigital.com
Linkedin: linkedin.com/company/cldigital-software
Twitter: x.com/CLDigital360
YouTube: youtube.com/@CLDigital360

CLDigital 360 is a leading no-code enterprise risk and resilience platform that empowers organizations to manage risk, resilience, and compliance while improving operational performance. The platform offers built-in BI for real-time insights, automated workflows, and over 100 integrations, including ServiceNow, Workday, and SAP. It also supports emergency notifications via Everbridge, F24, and Twilio, ensuring effective communication during critical events.

Our AI capabilities, including generative AI, machine learning, and custom models, enhance productivity by automating processes and analyzing complex data for informed decision-making, improved accuracy, and faster response times.

CLDigital 360 delivers comprehensive out-of-the-box solutions, including Enterprise Risk Management (ERM), operational resilience, business continuity, disaster recovery (DR), crisis management, and Third-Party Risk Management (TPRM). The platform supports the entire resilience lifecycle—from Business Impact Analysis (BIA) and strategy development to setting impact tolerances, automating testing, and tracking KPIs and KRIs to meet resilience goals.

Adhering to ISO 22301, NIST, FCA, and DORA standards, CLDigital 360 ensures compliance and best practices. Available via Cloud SaaS or on-premise with FedRAMP options, it provides the flexibility, security, and scalability to navigate exponential risk while accelerating ROI.

FUSION RISK MANAGEMENT

Fusion Risk Management
Floor 3, 108 Cannon Street,
London EC4N 6E, United Kingdom

Tel: +44 (0) 20-3884-3538
marketing@fusionrm.com
www.fusionrm.com/
Linkedin: www.linkedin.com/company/fusion-risk-management/
Twitter: x.com/FusionRiskMgmt

Fusion Risk Management is the leading provider of enterprise resilience software that empowers our customers to be agile in times of cascading crises. We help organizations drive the proactive business continuity and risk strategies they need to face growing threats and ensure their operations can bend but not break when faced with any challenge. More than 400 global organizations rely on Fusion's solutions to unify risk across their enterprise, make data-driven decisions, and work seamlessly with their critical third parties to sense risks and mitigate disruptions.

Our focus is enterprise resilience – encompassing operational resilience, business continuity management, IT disaster recovery, crisis and incident management, third-party risk management, and risk management. Fusion seeks to help companies anticipate, prepare for, respond to, and learn in any situation by equipping them with the software solutions they need to be successful.

With our platform, organizations are able to make confident decisions with speed and precision so that leaders can proactively manage what's to come. And with Great Hill Partners, we have the resources to continue expanding in all areas of the growing market. Learn more at www.fusionrm.com.

---

shadow planner

Wavenet Limited
One Central Boulevard, Blythe Valley Park,
Solihull,
West Midlands B90 8BG

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@wavenet.co.uk
www.shadow-planner.com
Linkedin: www.linkedin.com/company/wavenet_2/
Twitter: X.com/WavenetUK

Shadow-Planner from Wavenet is a multi-award-winning business continuity management platform designed by practitioners, for practitioners. Built around ISO 22301 and the Business Continuity Institute's Good Practice Guidelines, it delivers comprehensive functionality to support the entire business continuity lifecycle, from impact analysis and strategy development to planning, exercising, and reporting.
With powerful dependency mapping throughout your business, including important business services, Shadow-Planner provides a dynamic graphical view of your upstream and downstream dependencies and highlights any capability gaps, enabling you to create plans and playbooks, schedule and track exercises, capture observations, and monitor programme performance through an intuitive dashboard. There is even an emergency communications module providing emergency SMS and emails to all or targeted staff in an emergency.
Its award-winning mobile app ensures critical information reaches the right people at the right time, helping teams act quickly and confidently in any situation.

Developed from decades of real-world experience, Shadow-Planner takes the pain out of continuity management, empowering your teams to work smarter, respond faster, and meet resilience commitments efficiently and cost-effectively.

Core Functionality:
- Business impact analysis (BIA).
- Dependency mapping.
- Real time data gap analysis.
- Strategy design.
- Business continuity planning & playbooks.
- Exercise planning & management.
- Programme management dashboard.
- Mobile application.
- Emergency communications.

wavenet

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.

There has been a lot of talk lately about how wholesale insurance and retail insurance are very different creatures. In the wholesale market, customers are often multinationals with large risk, legal and procurement functions. They often have more capacity to litigate than the brokers they do business with. In the retail market, the David and Goliath dynamic is switched; it's the insurers with all the resources, while consumers enter into potentially life-changing contracts on their mobile phones while watching reruns on TV.

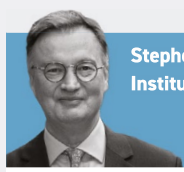
There is a lot of truth in the distinction, and it does support arguments that say that regulation should treat the two markets differently. Nevertheless, all insurance contracts are based on trust. Even multinationals have to trust insurers to have the operational wherewithal to pay claims accurately and efficiently – by the time they litigate, those two prizes have disappeared.

There is no stronger test of trustworthiness than the way in which insurers treat people with the lowest levels of financial capacity or resilience. That is why the government's recent strategy on financial inclusion is crucial to all insurance, not just retail. The areas it addresses are sometimes broad, such as supporting consumers in vulnerable circumstances; and sometimes more focused, as with addressing the needs of survivors of economic abuse, or signposting for people who are struggling to obtain cover.

The way insurers respond to these problems will tell all kinds of customers and investors about the capacity for the entire sector to meet new challenges. If insurers can make home insurance more relevant for renters, it also says something about the ability of insurers to cover commercial cyber risks. Similarly, if insurers can find ways to make their products work for people who have experienced economic abuse, it says something about how insurers can go beyond just transactional services, and supply employee rehabilitation programmes.

As Alex Reynolds, chief claims officer for Marsh, has said about claims management in the London Market: "Technical skills will only get you so far. It's the ability to understand and respond to the emotional state of the client and build trust, even before a claim arises, that differentiates a good claims handler from a great one."

Financial inclusion is not a woke cherry on the top of the insurance cake – it is the essential ingredient. A profession that can find new ways to serve more people will thrive in every potential market. A profession that writes off markets as being 'too difficult' to serve will shrink and ultimately be replaced by other methods of managing risk. Financial inclusion is where insurance lives and dies.



Stephen Sidebottom is chairman of the Institute of Risk Management

In association with

irm

If there's one thing we've learned over the last few years, it's that uncertainty isn't a glitch in the system; it *is* the system. Geopolitics, AI, climate shocks, skill shortages: every business plan assumes some measure of stability that reality doesn't provide. Organisations talk a lot about resilience but when you scratch the surface it often reveals a technical plan built on a very human fault line. The problem isn't uncertainty itself; it's our relationship with it. Most risk frameworks treat uncertainty as a statistical phenomenon or a risk type to be modelled, mitigated or transferred. But uncertainty is also emotional, social and profoundly human in its impact; the way people feel about risk will often determine how an organisation actually performs when things don't go according to plan.

This is where the idea of people risk changes the conversation. The behavioural view is critical: people risk can be seen as the gap between how humans are expected to behave and how they actually do when pressure, bias or fear take over. It's the human volatility that sits within, and defines, organisational systems. Take decision-making. Under stress, cognitive biases are known to surge: confirmation bias makes leaders seek reassurance instead of truth; optimism bias blinds them to downside scenarios; and groupthink rewards agreement over insight. In this way entire institutions can end up misjudging risk because they don't create the psychological conditions necessary for productive dissent. Then there's information risk. Many risk registers list "poor communication", yet few examine why. Often, it's not a lack of data but a lack of candour. People don't escalate issues early because they fear blame. They under-report errors, manage upwards, and rely on

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

informal messaging. The result can be a system that looks calm and informed right up until the moment it isn't.

The most sophisticated organisations realise you can't manage your way out of this with spreadsheets and registers. Instead, they treat people risk as a system of dynamic mitigations. This means investing not only in controls and technology, but in leadership behaviours, ethical awareness and decision quality. It also means building feedback loops that surface weak signals and designing ways of working that make it easier to speak up than to stay silent.

Human behaviour is context dependent. The same employee who cuts corners in one environment may act with integrity in another. That's not because of moral inconsistency, it's because of social logic. Systems shape our behaviour through incentives, workload, norms and role modelling. In other words, if your people are taking reckless risks, the problem may not be them – it may be the system teaching them that that's what success looks like.

The irony is that humans are both the source of organisational fragility and its greatest stabiliser. When conditions collapse, it's not processes that save a system; its judgement, trust and the willingness to improvise together. Managing uncertainty through a people risk lens means recognising that resilience is built through habits, mindsets and relationships that formed long before a crisis hits. We know we can't forecast everything, but we can design cultures where people are less likely to hide bad news, more likely to challenge assumptions, and be equipped to make sense of ambiguity. That's not HR stuff, it's core risk management infrastructure.

Beth O'Connor is special counsel, maritime and transport, at Sparke Helmore, a member of Global Insurance Law Connect

In association with

GLOBAL INSURANCE LAW CONNECT

Plagued by severe weather events, shadow fleets and geopolitical instability, 2025 is a year that the shipping industry and its insurers might prefer to commit to the scrap heap.

The outlook had seemed contrastingly upbeat in the first half of the year, when at the International Maritime Organisation's 83rd session in April, the Marine Environment Protection Committee proposed a world first net zero initiative, the IMO Framework, combining mandatory emissions limits and greenhouse gas emissions pricing in order to increase the uptake of green fuel technology and reach net zero GHG emissions by 2050. Given that the shipping industry generates 3% of global GHG emissions, the news was promising, and had received support from many countries, as well as the International Chamber of Shipping. The IMO Framework was designed to operate through amendments to MARPOL Annex VI, the primary international convention regulating ship emissions. Without agreement on these amendments, the framework cannot be legally enforced, leaving the industry without a unified route to decarbonisation.

It was disappointing, then, that when the MEPC held its second extraordinary session in October, the parties could not reach consensus on the necessary enacting amendments to MARPOL Annex VI. Further negotiations were adjourned to October 2026, thus jeopardising the timeframe for decarbonisation. While the IMO Framework ultimately fell as a geopolitical pawn (with the US administration lobbying widely to ensure it was not adopted), concerns were also raised as to the potential compliance costs associated with its adoption and the viability of green fuels more generally.

The latter concern arises from the fact that no single green fuel has emerged as a frontrunner for global adoption. Indeed, each of the main contenders (ammonia, methanol, hydrogen, biofuels and liquefied natural gas) possesses inherent risks that have the potential to compromise environmental and human safety in the event of a disaster.

Unfortunately, the law does not yet have an answer as to how a catastrophe would be compensated; none of the oil pollution conventions deal with green fuels. Ratification of the International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea is, however, gaining momentum.

Despite the outcome, Australia remains focused on its Maritime Emissions Reduction National Action Plan, establishing a Green Shipping Corridor with Singapore by the end of 2025, and investigating other green corridors with South-East Asian neighbours. At a domestic level, TasPorts is working to position itself as a hydrogen production centre.

Likewise, major global shipping companies are taking it upon themselves to develop green technology and decarbonise the industry. The difficulty, of course, is that in the absence of a unified approach, they are left to dissect a multitude of regulations, regimes and reporting requirements as they traverse the world. It is, therefore, hoped that supporters of the IMO Framework can build consensus over the coming year in the hopes of a successful negotiation in October 2026.

Firms rethink overseas security

Global businesses are re-evaluating their exposure to geopolitical and economic turmoil, as inflation, trade tensions and political unrest emerge as top growth barriers, according to a new report published this quarter by Beazley

Global business leaders now see geopolitical and economic uncertainty as the greatest obstacles to growth, with inflation and political unrest key amongst corporate risks. These are amongst the findings of Beazley's 2025 *Geopolitical and Economic Risk and Resilience Report*, which surveyed 3,500 senior executives across multiple regions and sectors.

The research paints a picture of firms operating in a complex, fast-moving environment where trade tensions, energy costs and policy shifts are converging to test resilience.

"Some 35% report increasing their investment in risk management and loss prevention since early 2024, aiming to ensure that innovation is matched by resilience"

In response, 32% of businesses plan to reassess the security of their overseas operations this year, up from 23% last year. Supply chain disruption has become a major operational concern, with 87% of firms planning to adjust suppliers or reroute operations. Some 35% have increased their investment in risk management and loss prevention since early 2024, aiming to ensure that innovation is matched by resilience.

Despite the pressures, many firms continue to pursue high-risk, high-opportunity frontiers such as AI, fusion energy and lunar exploration.

"Despite the pressures, many firms continue to pursue high-risk, high-opportunity frontiers such as AI, fusion energy and lunar exploration"

Insurance, meanwhile, is being evolving beyond protection, according to the report, becoming a strategic lever. Firms are using cover to expand into new markets, despite regulatory hurdles; to secure access to critical resources; and to protect against emerging exposures, including cyber threats and political disruption.

Bethany Greenwood, chief executive officer of Beazley Furlonge Limited, and group head of specialty risks at Beazley, said: "Resilience isn't just about surviving disruption; it is about turning risk into competitive advantage. Innovative insurance solutions, including political risk coverage, parametric supply chain protection and crisis management services, are helping businesses act confidently in uncertain conditions."

BUSINESS CONTINUITY SOFTWARE

CLDigital
Floor 24/25, The Shard,
London Bridge Street, London, SE1 9SG

Tel: +44 (0)20 7770 6446
info@cldigital.com
cldigital.com
Linkedin: linkedin.com/company/cldigital-software
Twitter: x.com/CLDigital360
YouTube: youtube.com/@CLDigital360

CLDigital 360 is a leading no-code enterprise risk and resilience platform that empowers organizations to manage risk, resilience, and compliance while improving operational performance. The platform offers built-in BI for real-time insights, automated workflows, and over 100 integrations, including ServiceNow, Workday, and SAP. It also supports emergency notifications via Everbridge, F24, and Twilio, ensuring effective communication during critical events.

Our AI capabilities, including generative AI, machine learning, and custom models, enhance productivity by automating processes and analyzing complex data for informed decision-making, improved accuracy, and faster response times.

CLDigital 360 delivers comprehensive out-of-the-box solutions, including Enterprise Risk Management (ERM), operational resilience, business continuity, disaster recovery (DR), crisis management, and Third-Party Risk Management (TPRM). The platform supports the entire resilience lifecycle—from Business Impact Analysis (BIA) and strategy development to setting impact tolerances, automating testing, and tracking KPIs and KRIs to meet resilience goals.

Adhering to ISO 22301, NIST, FCA, and DORA standards, CLDigital 360 ensures compliance and best practices. Available via Cloud SaaS or on-premise with FedRAMP options, it provides the flexibility, security, and scalability to navigate exponential risk while accelerating ROI.

Fusion Risk Management
Floor 3, 108 Cannon Street,
London EC4N 6E, United Kingdom

Tel: +44 (0) 20-3884-3538
marketing@fusionrm.com
www.fusionrm.com/
Linkedin: www.linkedin.com/company/fusion-risk-management/
Twitter: x.com/FusionRiskMgmt

Fusion Risk Management is the leading provider of enterprise resilience software that empowers our customers to be agile in times of cascading crises. We help organizations drive the proactive business continuity and risk strategies they need to face growing threats and ensure their operations can bend but not break when faced with any challenge. More than 400 global organizations rely on Fusion's solutions to unify risk across their enterprise, make data-driven decisions, and work seamlessly with their critical third parties to sense risks and mitigate disruptions.

Our focus is enterprise resilience – encompassing operational resilience, business continuity management, IT disaster recovery, crisis and incident management, third-party risk management, and risk management. Fusion seeks to help companies anticipate, prepare for, respond to, and learn in any situation by equipping them with the software solutions they need to be successful.

With our platform, organizations are able to make confident decisions with speed and precision so that leaders can proactively manage what's to come. And with Great Hill Partners, we have the resources to continue expanding in all areas of the growing market. Learn more at www.fusionrm.com.

Wavenet Limited
One Central Boulevard, Blythe Valley Park,
Solihull,
West Midlands B90 8BG

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@wavenet.co.uk
www.shadow-planner.com
Linkedin: www.linkedin.com/company/wavenet_2/
Twitter: X.com/WavenetUK

Shadow-Planner from Wavenet is a multi-award-winning business continuity management platform designed by practitioners, for practitioners. Built around ISO 22301 and the Business Continuity Institute's Good Practice Guidelines, it delivers comprehensive functionality to support the entire business continuity lifecycle, from impact analysis and strategy development to planning, exercising, and reporting.
With powerful dependency mapping throughout your business, including important business services, Shadow-Planner provides a dynamic graphical view of your upstream and downstream dependencies and highlights any capability gaps, enabling you to create plans and playbooks, schedule and track exercises, capture observations, and monitor programme performance through an intuitive dashboard. There is even an emergency communications module providing emergency SMS and emails to all or targeted staff in an emergency.
Its award-winning mobile app ensures critical information reaches the right people at the right time, helping teams act quickly and confidently in any situation.

Developed from decades of real-world experience, Shadow-Planner takes the pain out of continuity management, empowering your teams to work smarter, respond faster, and meet resilience commitments efficiently and cost-effectively.

Core Functionality:
- Business impact analysis (BIA).
- Dependency mapping.
- Real time data gap analysis.
- Strategy design.
- Business continuity planning & playbooks.
- Exercise planning & management.
- Programme management dashboard.
- Mobile application.
- Emergency communications.

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

wavenet

Wavenet Limited
One Central Boulevard, Blythe Valley Park, Solihull,
West Midlands B90 8BG

Contact Name: Kerry Brooking

Tel: 0344 863 3000
Kerry.Brooking@wavenet.co.uk
www.wavenet.co.uk/
Linkedin: www.linkedin.com/company/wavenet_2/
Twitter: X.com/WavenetUK

You can protect what matters most to your business and recover quickly from any disruption with the help of our 30 years' experience as a business continuity leader. From identifying and managing risks to planning and provisioning for uninterrupted operations, we help you build true resilience.

Consultancy Services
Our certified consultants provide expert guidance across business continuity, operational resilience, IT service continuity and cyber resilience. We help you produce or validate your BIAs & plans, design and run crisis management exercises, benchmark you against best practice and run security health checks, advising on every aspect of your critical operations.

Business Continuity Planning & Supply Chain Risk Management
Powered by our award-winning Shadow-Planner software and BCI-certified specialists, we help you map, mitigate and report on critical dependencies within your organisation, ensuring nothing is overlooked.

Data Protection
Whether you need backup, replication or recovery, self-service, co-managed or fully managed, we deliver flexible solutions via the cloud, remotely or on-site. We also support testing, rehearsals and documentation of your recovery strategy.

IT & Data Recovery
In times of crisis or planned standby, we provide industry-leading recovery and rapid replacement IT infrastructure, delivered physically, virtually or from the cloud.

Work Area Recovery
Our fully resilient UK facilities provide always-ready workspace and infrastructure to keep your teams operational. Whether adapting to hybrid work models or changes in real estate, we ensure continuity, confidence and peace of mind for your customers and stakeholders.

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

F24

F24
Cardinal Point Park Road,
Rickmansworth WD3 1RE

Tel: 01923 437 784
office_uk@f24.com
www.f24.com
Linkedin: www.linkedin.com/company/f24-uk-limited/
Twitter: x.com/F24UKLimited
YouTube: www.youtube.com/@F24AG/

F24 is Europe's leading SaaS provider specialising in emergency management and critical communication solutions. With 25 years of industry experience, F24 has established itself as a trusted partner for organisations, helping them navigate crises with confidence and efficiency.

FACT24 ENS (Emergency Notification Service) and FACT24 CIM (Crisis Incident Management), are designed to streamline communication and incident management during emergencies. These solutions ensure rapid, reliable alerts and comprehensive tools for managing incidents from start to finish. F24's TopEase® is a comprehensive GRC (Governance, Risk, and Compliance) platform that streamlines corporate governance, enhance risk management, and ensure business continuity through intelligent automation and a holistic view of organizational processes.

F24's offer global reach with local support, ensuring that our clients receive the best service and solutions tailored to their needs. Join the many organisations worldwide that trust F24 to safeguard their operations and ensure business continuity.

RISK MANAGEMENT SOFTWARE SOLUTIONS

ORIGAMI RISK

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

Tel: +44 (0)1617 917740

info@origamirisk.com
www.origamirisk.com
Linkedin: www.linkedin.com/company/origami-risk/

Origami Risk provides innovative solutions that break down silos, automate processes, and provide data-based context for the decisions risk management, insurance, and safety professionals make every day.

Delivered from a single platform that is fast, secure, and scalable, Origami Risk's RMIS, GRC, EHS, P&C Policy Administration, P&C 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 systems and the tailoring of solutions that meet client-specific requirements and workflows without the need for costly, time-consuming custom development.

From implementation expertise to ongoing service focused on your success, Origami Risk solutions are supported by an experienced team that works to ensure you get maximum value from your technology investment.

PROTECHT

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®

riskHive Software Solutions Ltd
Cilwendeg Mansion, Newchapel,
Boncath, Pembrokeshire, SA37 0EW

Contact: Sandu Hellings
Tel: +44 1275 545874
sandu.hellings@riskhive.com
www.riskhive.com

LinkedIn: www.linkedin.com/company/riskhive
X: @riskHive information
YouTube: www.youtube.com/channel/UCGDHhXKtohhLbmIM37gzF7w/videos

riskHive ERM is an Enterprise Risk Management (ERM) software solution designed to assist organisations in identifying, evaluating, and mitigating risks across their business operations. It provides a centralised platform for real-time risk monitoring and management, enabling informed decision-making and proactive risk mitigation.

Key features include risk identification and assessment, risk scoring and prioritisation, risk mitigation planning, and incident management. Users can define risk categories, assign risk owners, and track the progress of risk mitigation actions. Customisable dashboards and reports provide a comprehensive view of an organisation's risk landscape.

riskHive ERM is user-friendly and can be tailored to specific industry requirements. It seamlessly integrates with existing systems, facilitating data exchange and collaboration between different projects, departments, divisions and/or even companies in very large company frameworks.

Implementing riskHive ERM enhances risk management capabilities, improves decision-making processes, and safeguards company assets and reputation from potential threats.

CIR Software Reports

CIR's fully interactive online software comparison tool is available across all our reports, in addition to our popular in-depth analysis of products in the business continuity, emergency and mass notification, and risk software markets.

Visit cirmagazine.com

riskonnect

Can your risk management strategies keep up with the new generation of risk?

Riskonnect's 2024 New Generation of Risk Report surveyed more than 200 risk, compliance, and resilience professionals worldwide on today's biggest threats – and what is being done about them.

Scan the code below to find out how you compare.

Riskonnect.com