irm

IRM Risk Trends 2026

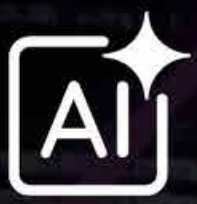
RISKY BUSINESS

IRM AI
AI Risks. Managed.

irm

Build your AI risk expertise with our new learning programmes

Award in Managing AI Risks
A practical, career-boosting qualification in managing AI risks.



Enterprise-wide AI Risk Management
A short, high-impact training course built for immediate application.

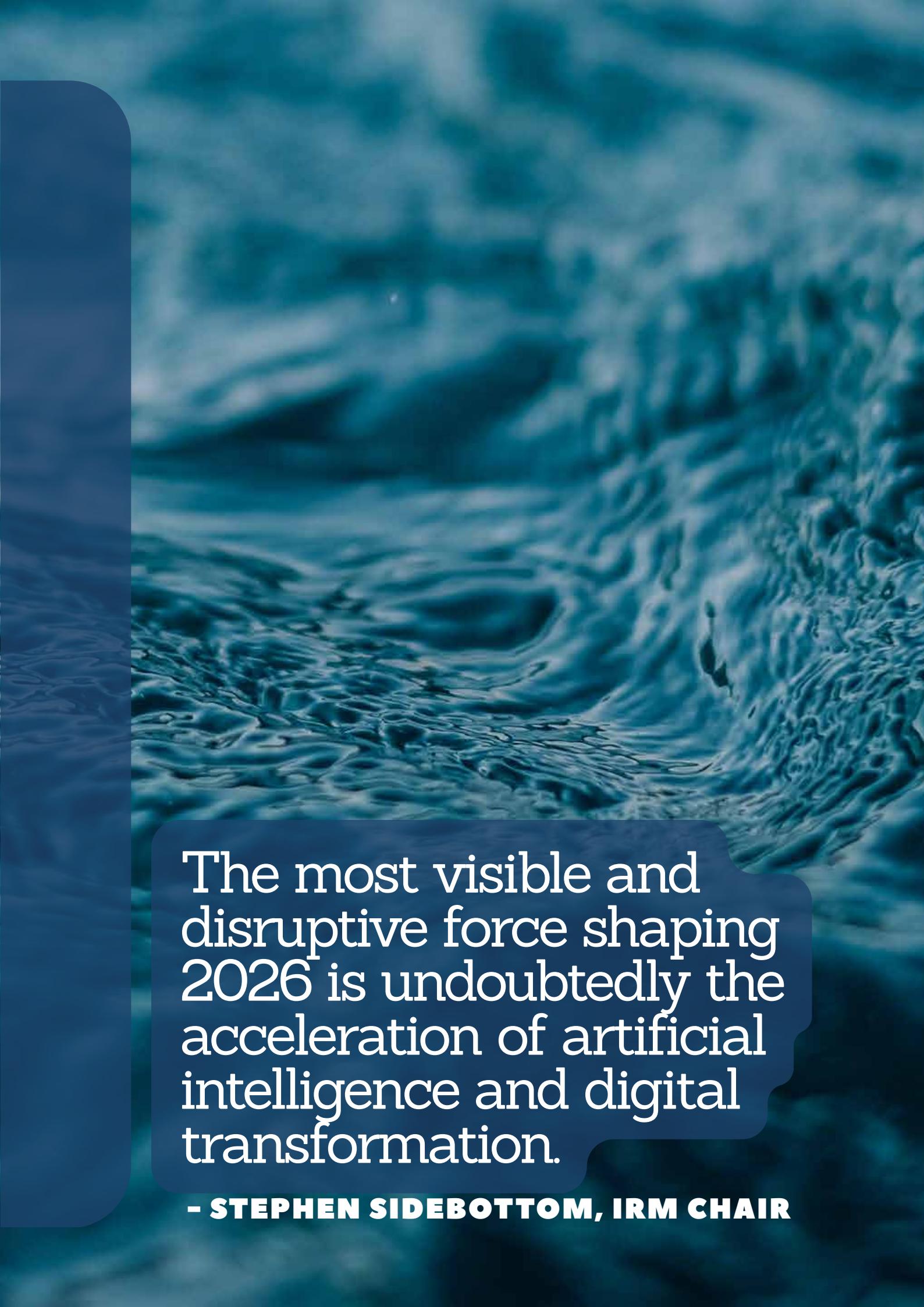
Scan to find out more

Contents

Introduction

Regional Interest Groups

Special Interest Groups



The most visible and disruptive force shaping 2026 is undoubtedly the acceleration of artificial intelligence and digital transformation.

– STEPHEN SIDEBOTTOM, IRM CHAIR

Convergence

RISK MANAGEMENT IN 2026

by Stephen Sidebottom, IRM Chair

Risk management is being reshaped by forces that are broader and more interconnected than ever before. 2026 stands at a pivotal point in the evolution of traditional risk categories and the transformation of how organisations will perceive and respond to uncertainty.

Across industries, risk leaders are reporting the same reality: the environment in which they operate is more complex and less predictable. This is not just an increase in risk, but a risk that becomes systemic, with each new vulnerability compounding others in unpredictable ways. Artificial intelligence (AI), climate volatility, geopolitical fragmentation, and shifting social expectations are colliding to create a new type of risk landscape.

The Digital Reckoning

The most visible and disruptive force shaping 2026 is the acceleration of digital transformation. AI has moved beyond experimentation into mainstream deployment, potentially touching every business process from decision-making to customer engagement. Yet with that maturity comes risk exposure. Machine-learning models trained on opaque data can produce hidden biases and unexplainable outcomes. Automation introduces new classes of operational failure and control gaps. The same algorithms that generate business value also generate cyber risk at scale. The result is a paradox: organisations are becoming both more capable and more vulnerable.

For risk professionals, the task is no longer to treat digital risk as an "IT issue", but to recognise it as a strategic risk that is altering the very business model. The governance, ethics, and accountability of AI systems are now board-level concerns. Risk functions must adapt, developing fluency in data science and algorithmic assurance while maintaining a strong line of sight on the human judgment that ultimately governs technology use.

A Fragmented Geopolitical and Regulatory Landscape

At the same time, the geopolitical and regulatory environment has become increasingly fragmented, and the notion of a stable, predictable global regulatory regime is fading. This fragmentation multiplies the operational burden for risk managers, who must monitor not only economic indicators but the shifting values of global governance. The strategic challenge is to design resilience that can withstand political and regulatory volatility. For many, this means expanding scenario planning, embedding horizon scanning into governance processes, and strengthening localised compliance capabilities. It also demands a renewed focus on transparency and adaptability as the qualities that enable organisations to maintain trust in uncertain times.

The Climate Imperative

Climate and environmental risk are now an immediate business issue. Transition policies are accelerating, exposing industries to potentially abrupt shifts in asset valuation, carbon pricing, and consumer demand. Physical climate impacts such as extreme weather events, resource scarcity, and migration pressures are intensifying, disrupting supply chains and requiring a shift in long-term planning. The debate has moved from whether climate change will affect business to how it already does. Regulators are embedding climate disclosure into mainstream reporting frameworks, while investors and customers are scrutinising authenticity in sustainability claims. For risk management, this means integrating climate risk into enterprise frameworks, quantifying both transition and physical exposures, and linking ESG performance directly to financial and operational resilience.

The Human Dimension of Risk

While technology dominates the headlines, human factors remain central to organisational resilience. Talent scarcity and the erosion of trust within institutions present risks that are less visible but no less material. As organisations digitise, the human element of ethical decision-making grows even more critical. The most advanced algorithms still rely on human oversight; the most sophisticated control systems still depend on human vigilance. Building a culture that promotes transparency, ethical reflection, and shared accountability is therefore a strategic imperative. The success of any risk framework ultimately hinges on the behaviours and values of the people who apply it.

The Next Frontier: From Periodic Review to Continuous Insight

Traditional risk management cycles, including annual reviews, static registers, and backward-looking reports, are increasingly out of date. The speed of disruption demands continuous monitoring and agile decision-making. Data analytics, AI-driven early-warning systems, and real-time dashboards are enabling a more dynamic approach to risk oversight. This evolution does not mean replacing human judgment with automation but rather, enhancing it. The risk function of 2026 will be characterised by its ability to interpret signals amid noise, convert data into foresight, and embed risk thinking into everyday operations.

A Profession in Transformation

For the risk profession, these changes amount to a reinvention. Risk managers are moving from guardians of compliance to architects of resilience, from control specialists to strategic advisors. They are required to understand technology, geopolitics, climate science, and behavioural psychology. This is an interdisciplinary challenge that demands continual learning and cross-functional collaboration. At the same time, the expectations placed upon risk functions are growing. Boards want assurance that emerging risks are being understood and managed; regulators demand evidence of governance and accountability, and stakeholders expect ethical and sustainable conduct. The credibility of the risk profession will depend on its ability to provide insight, foresight, and clear communication under pressure.

Looking Ahead

The year 2026 will test the agility and foresight of every organisation. The most successful will be those who treat uncertainty not as a disruption to be avoided but as a dimension of strategy to be mastered. Integrating risk into decision-making, strengthening resilience across digital and physical domains, and nurturing cultures of trust and adaptability will define the next phase of risk management maturity.

In this edition of IRM Risk Trends 2026, we explore these dynamics in depth. We examine how technology, geopolitics, climate, and culture are converging to redefine the risk landscape and how organisations can respond with intelligence and integrity. The challenge before us is not merely to manage risk, but to lead through it.

big data

BIGGER RESULTS

As part of the Institute of Risk Management (IRM) Risk Trends Report, over 350 risk practitioners were surveyed a series of questions covering all things risk. We asked our members about the past year, the coming year, and to look five years ahead and predict what they think will have the greatest impact on their industry.

The findings point to a closely contested risk landscape, dominated by both macroeconomic pressure and escalating digital threats.

It should come as no surprise that the significant growth in Artificial Intelligence is consistently highlighted as one of the biggest emerging risks. Alongside this, a key insight is how many IRM members noted 'Economic Slowdown' as an emerging concern, cited by 22% of respondents (to the question 'Which of the following risks do you expect to pose the greatest challenge to your organisation in the next year?'), reflecting ongoing uncertainty around growth, inflationary pressures, and constrained investment environments.

This highlights continued sensitivity to external economic conditions and their knock-on effects on revenue stability, cost control, and strategic planning.

Our report this year will break down many of these key insights and provide you with a clear outlook on what is on the minds of risk practitioners around the world, not just for 2026, but for the coming years.

With technology and cyber risk being one of the biggest talking points of this report, we asked our members to share which technology horizon risks they are most concerned about. These are their direct insights into technology risks:

"An increasing number of medical devices running on unsupported versions of Windows without the ability to update"

"Near term (0–12 months): Cloud/SaaS concentration & identity/IAM outage risk; software supply-chain exposure; third-party API changes. Mid term (12–36 months): Data-centre/energy constraints affecting cloud SLAs and cost; AI infrastructure/vendor lock-in; network resilience for hybrid work. Long term (36–60+ months): Quantum-safe cryptography transition; legacy decommissioning/technical-debt risks."

"AI being relied upon by inexperienced teams with little knowledge and wisdom"

"Agentic AI to replace the current generative AI - knowledge on digital transfer is still minimal to non-existant and the technology is developing much faster. The emerging development may see the loss of the ability for fact-checking, and data could become generic. On a wider scale, information publicising use of AI does not carry enough warning about the content, and people's lack of understanding around data is exposing significant risk of personal data being stolen through a lack of knowledge."

"Malicious use: AI tools are lowering the barrier for entry into cyberattacks, fraud, and the creation of large scale misinformation/disinformation campaigns"

"A long-term outage from a major supplier, e.g. AWS, Microsoft"

"The use of AI to provide technical data to a non-technical audience, and the impact of those searches on the perception of what is real"

"Cyber warfare and the prepositioning of state actors in preparation for conflict"

Emerging Risks Ranked

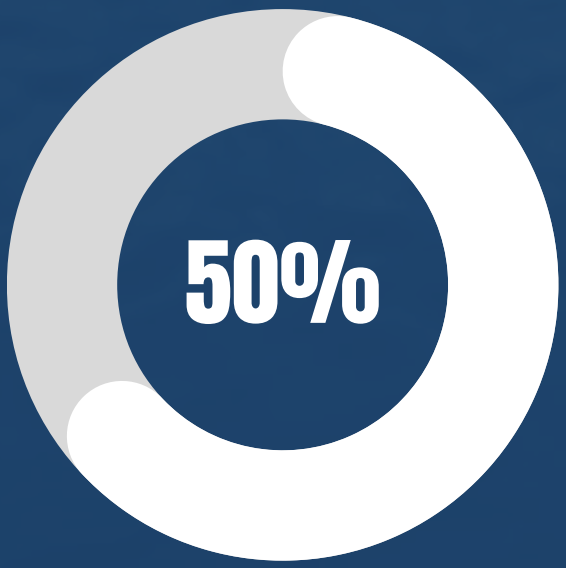
Here's a ranked list of the Top 5 Emerging Risks for 2026, with estimated likelihood and impact based on the IRM Risk Trends Report 2026 Survey*.

Rank	Emerging Risk	Estimated Likelihood	Estimated Impact	Key Description
1	AI & Digital Disruption	High (80%)	Very High 	Rapid AI deployment causing governance, bias, and model-risk issues; automation errors; data-integrity failures; AI-driven cyber threats.
2	Cyber & Data Resilience	Very High (85%)	Very High 	Sophisticated cyberattacks exploiting generative AI; rising regulatory expectations on data privacy and resilience.
3	Geo-political Fragment-ation	High (75%)	High 	Trade bloc competition, sanctions, resource nationalism, election volatility; uncertainty affects supply chains and regulatory alignment.
4	Climate & Transition Risk	Medium - High (70%)	Very High 	Physical weather events, carbon-transition policy shocks, stranded-asset exposure, supply-chain vulnerability to extreme events.
5	Third-Party & Supply-Chain Interdependence	High (70%)	High 	Deep-tier supply-chain visibility gaps; systemic disruptions through vendor failure or geopolitical tensions.

* The IRM Risk Trends Report 2026 surveyed over 350 risk practitioners and IRM Members globally.

CRO INSIGHTS

Explore the key risk trends influencing CROs in 2026, and how high-performing teams are adapting without sacrificing growth. Each insight breaks down what's changing, why it matters now, and how CROs can respond with smarter experimentation, stronger signals, and risk-aligned conversion strategies.



We asked CRO's around the world what risk they expect will pose the greatest challenge to their organisation this year, and 50% of CRO's said:

1. **Talent retention and skills gaps**
2. **Cybersecurity and ransomware attacks**

44% indicated that AI and Climate Change related risks will be the most significant emerging risk in the next 5 years.

35% identified ISO 31000 as the frameworks their organisation relied on most in the last year

47% of CROs felt their organisation would be sufficiently resilient in the face of a cyber incident

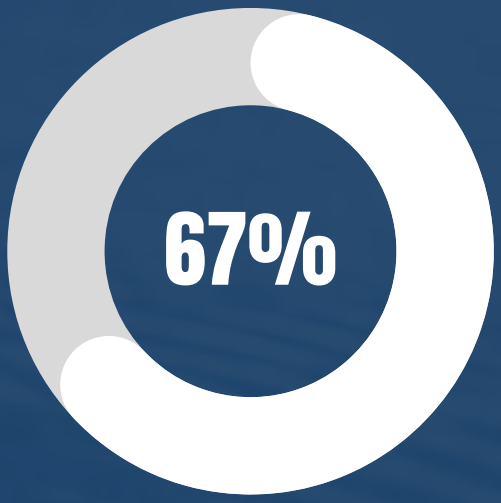
52% see the greatest clinical risk currently facing healthcare organisations staffing shortages or clinician burnout

66% highlighted energy prices having had an adverse affect on financial performance in the last 12 months

37% identified Misinformation and Deepfakes as the AI risk to grow most in the next 3 years

96% of CROs believe their supply chain does not pose a threat to their business activites.

30% describe the culture around risk in their organisation as cautious and compliance-driven



Rising energy prices have emerged as a material risk factor for organisations over the past year, with direct implications for financial performance and strategic decision-making.

According to our survey, 67% of Chief Risk Officers report that increases in energy costs have had either a slight or severe effect on their organisation's financial performance over the last 12 months.

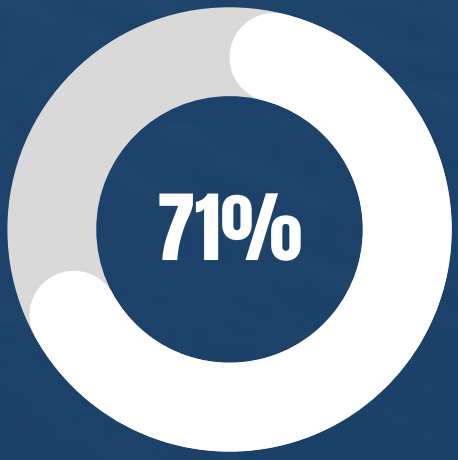
This impact spans both operating margins and longer-term investment capacity, particularly for energy-intensive sectors and businesses with complex supply chains. For many organisations, higher energy prices have amplified existing cost pressures, forcing difficult trade-offs between efficiency initiatives and customer experience investments. Even where the impact has been described as "slight," the cumulative effect has increased sensitivity to risk across budgeting, forecasting, and growth planning.

ONLY 1 in 10 CROs

AI-related risk is emerging as one of the most significant and least understood challenges facing organisations in 2026. Despite rapid adoption, only 1 in 10 CROs (5% of those surveyed) say they feel prepared to effectively manage AI-related risks in the year ahead.

This confidence gap highlights a growing disconnect between how quickly AI is being deployed and how slowly governance, controls, and accountability frameworks are maturing. For most organisations, AI risk extends well beyond model accuracy. Issues such as regulatory compliance, data privacy, algorithmic bias, explainability, and over-automation are increasingly influencing both operational stability and brand trust.

The lack of preparedness suggests that many risk functions are still reacting to AI implementation rather than shaping it, often without clear visibility into how AI-driven tools are influencing customer journeys and conversion outcomes. As risk tolerance tightens, CRO teams will need closer alignment with risk and compliance leaders to ensure experimentation remains controlled, transparent, and defensible.



71% of Chief Risk Officers identify limited resources across time, budget, and staffing, as the biggest challenge to embedding risk practices, closely followed by a lack of risk culture and insufficient leadership buy-in.

Resource constraints are forcing risk teams to prioritise immediate regulatory and operational demands over longer-term capability building. This often leaves limited capacity for proactive risk integration or the development of scalable frameworks that can keep pace with evolving threats. At the same time, where leadership buy-in is weak, risk initiatives are more likely to be viewed as blockers rather than strategic enablers further limiting their influence.

AI INSIGHTS

We asked practitioners what they see as the most significant risk associated with Artificial Intelligence (AI) adoption in their organisation/sector?

45% **Data privacy and security breaches**

35% **Over-reliance on AI leading to operational failures**

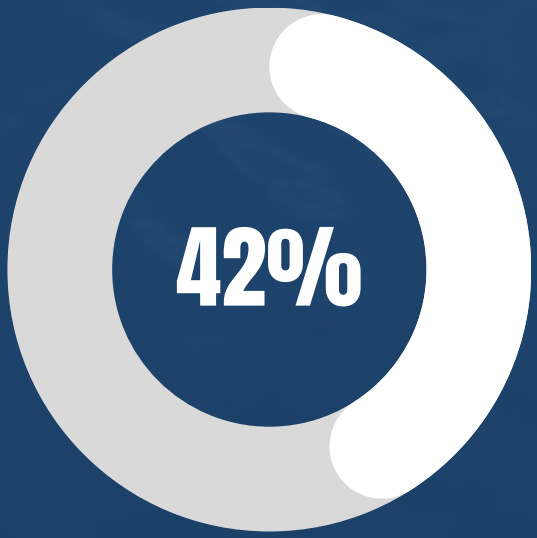
20% **Ethical concerns (bias, discrimination, lack of transparency)**

3 in 10 also highlight their concerns over AI being used in an educational context, for example, students using AI to complete their assigned work.

When asked which AI-related risk do you expect to grow most in the next 2–3 years, our audience shared some insightful thoughts:

"Over reliance of staff on AI tools rather than their own expertise"

"The pervasive, but often unrecognized, societal and organisational impact of LLM hallucinations and their ability to generate convincing but factually incorrect 'consensus' based on probabilistic rather than contextual truth."



42% of Risk Professionals feel prepared to identify and manage AI-related risks within their organisations.

Whilst 16% felt they were completely unprepared to deal with any looming AI related risks.

While they understand that artificial intelligence is reshaping operational, legal, and ethical landscapes at speed, many feel their tools, frameworks, and training haven't kept up. The pace of AI adoption often outstrips governance, leaving professionals to manage opaque models, uncertain regulations, and novel failure modes with limited guidance.

As a result, there's a growing sense that traditional risk approaches are being stretched beyond their comfort zone just as the stakes get higher.

We asked practitioners which approach best describes your organisation's current governance of AI risks?

40% Policy framework led by risk/compliance functions

32% No governance framework currently in place

28% Formal governance structure with board-level oversight

6 out of 10 risk practioners say AI and machine learning have had the most significant impact on improving risk management practices over the past year

According to our survey results, AI and machine learning have had the most significant impact on improving risk management practices over the past year. These technologies are enabling faster risk identification, better pattern detection, and more dynamic scenario analysis, helping teams move from reactive to more predictive approaches.

However, this progress comes with a paradox: while AI is strengthening risk capabilities for some, it is also introducing new, complex risks that many professionals feel underprepared to manage. The survey highlights a growing gap between the benefits AI delivers and the confidence risk professionals have in governing its ethical, regulatory, and operational implications. Our research shows a stark contrast between the value AI and machine learning are already adding to risk management and how prepared professionals feel to govern the risks they introduce.

6 out of 10 respondents said AI has had the greatest impact on risk management practices in the past year, yet 4 out of 10 admitted they lack confidence in their ability to identify and assess AI risks with current resources, highlighting a significant preparedness gap. This disparity means that while, for some, AI and ML are improving predictive analytics, scenario planning, and operational insights, many risk professionals still struggle with governance frameworks, technical explainability, and risk-specific training, leaving organisations exposed even as they harness these powerful tools.

Africa 2026

RISK OUTLOOK AND PROFESSIONAL IMPERATIVES

Heading into 2026, Africa's operating environment is shaped by interlocking risk drivers rather than isolated issues. Tight financing conditions, public-debt pressures, and escalating climate impacts increasingly interact, creating second-order effects that can move quickly from localised disruption to multi-sector risks.

These dynamics manifest differently across regions. West Africa continues to face acute insecurity linked to persistent violence in the central Sahel, with destabilising spillovers affecting parts of coastal states, while maritime insecurity in and around the Gulf of Guinea trade corridor remains a material operational concern. East Africa combines high climate exposure, including recurrent cycles of drought and flooding across the Horn of Africa, with a tightening fiscal landscape in several economies where elevated public debt and debt-service pressures constrain budgets and reinforce reliance on IMF supported adjustment and financing, including in Kenya and Ethiopia.

Southern Africa continues to manage the operational consequences of constrained power supply and grid reliability, with significant implications for investment planning and energy-intensive sectors. North Africa faces structural water scarcity pressures that intersect with economic and political stressors. Central Africa, particularly eastern DRC, remains exposed to conflict dynamics linked to governance constraints and the political economy of mineral resources.

Across these regions, several cross-cutting themes are consistently emphasised in authoritative reporting. Digital ecosystems can rapidly amplify the spread of information, including misinformation and disinformation. In 2025, the rapid spread of information through digital platforms contributed to situations where some jurisdictions implemented internet restrictions and shutdowns during protests, elections, and periods of conflict. Supply chains remain vulnerable where climate extremes and maritime insecurity disrupt logistics. Cybercrime continues to grow in scale and sophistication as digital adoption expands. ESG-related disclosure and due diligence expectations continue to shape investor requirements, access to capital, and counterpart assessments, even as sustainability reporting and related regimes remain under active policy revision and political negotiation.

The Risk Management hub in Africa

Empowering Africa's risk professionals through globally recognized IRM certifications, strategic collaborations, and a thriving pan-African network. IRM Africa is the official regional hub of the Institute of Risk Management (IRM), dedicated to advancing the risk profession across the African continent. Headquartered in Nairobi, Kenya, we serve as the authoritative voice and convening platform for risk professionals across East, West, Central, Northern, and Southern Africa.

This entry has been authored by:

- Sheila Mueni Mulinge
- Joyce Ndirangu

In this context, risk management is most effective when positioned as decision support embedded in strategy rather than treated as a stand-alone compliance function. This approach aligns with widely used frameworks that emphasize integrating risk into governance, strategy-setting, and performance management. Achieving that shift requires five practical moves:

- Contextualised intelligence gathering: Complement quantitative indicators with structured local insight from communities, operational contacts, and sector specialists to strengthen early warning and interpretation in fast-moving environments.
- Pragmatic technology deployment: Prioritise scalable tools that improve situational awareness and shorten the time from incident detection to decision-making, including secure mobile reporting, cloud collaboration, and geospatial or open-source monitoring where appropriate.
- Targeted capability building: Invest in Africa-relevant competencies such as political economy analysis, climate risk and adaptation literacy, and stakeholder engagement so risk judgments are context-aware rather than template-driven.
- Cross-functional collaboration: Reduce silos across political and security, operational, climate, finance, and cyber risk so interdependencies are assessed through combined scenarios rather than separate checklists.
- Unwavering ethical commitment: Preserve transparency and independent judgment, especially where commercial incentives exist to minimize exposures that may later become material under scrutiny from regulators, investors, and affected stakeholders.

The assessments in this overview provide structured analysis of priority risks, sectors, and countries to support operational planning and strategic decisions. They include thematic coverage of cyber risk, climate exposure and adaptation constraints, supply-chain resilience, and political and security dynamics, alongside sector and country profiles tailored to African operating environments. Across the collection, the approach is consistent. Each assessment identifies key drivers and linkages, highlights regional and sector variation, defines forward indicators to monitor, and proposes mitigation options that reflect institutional capacity, stakeholder dynamics, and implementation constraints.

Africa in 2026 will continue to present both risk and opportunity for organisations that can convert uncertainty into structured choices. Professionals who combine contextual intelligence, integrated analysis, and credible communication of business impact are better positioned to help institutions operate responsibly and competitively across the continent. This outlook is intended as a foundation for disciplined judgment rather than a substitute for local validation. Users should test assumptions against on-the-ground signals, update scenarios as conditions change, and document decision trade-offs clearly in anticipation of governance scrutiny, investor expectations, and regulatory inquiry.

References

https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2024/
https://acleddata.com/report/conflict-watchlist-2024-sahel-deadly-new-era-decades-long-conflict
https://www.coso.org/enterprise-risk-management
https://www.eskom.co.za/loadshedding-remains-suspended-for-170-days-achieving-efficiencies-of-r12-54-billion-in-year-on-year-reduction-on-diesel-expenditure-due-to-ongoing-structural-improvements-in-the-generation-fleet/
https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en
https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng
https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng
https://www.gov.za/sites/default/files/progress_on_EAP.pdf.pdf
https://d3cpegos94401u.cloudfront.net/publications/documents/2024---jan---dec-imb-piracy-and-armed-robbery-report.pdf
https://www.imf.org/en/-/media/files/publications/reo/afr/2024/april/english/text.pdf
https://www.imf.org/en/Publications/CR/Issues/2024/11/01/Kenya-Seventh-and-Eighth-Reviews-Under-the-Extended-Fund-Facility-and-Extended-Credit-556994
https://www.imf.org/en/news/articles/2025/12/10/pr-25416-ethiopia-imf-reaches-staff-level-agreement-on-the-4th-review-of-ecf
https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet.pdf
https://www.iso.org/standard/65694.html
https://www.reuters.com/sustainability/climate-energy/eu-strikes-deal-further-weaken-corporate-sustainability-laws-2025-12-09/
https://www.swissinfo.ch/eng/international-geneva/un-experts-warn-congos-conflict-minerals-slipping-into-global-market/89978793
https://main.un.org/securitycouncil/en/sanctions/1533/panel-of-experts/expert-reports
https://www.worldbank.org/en/topic/water/publication/beyond-scarcity-water-security-in-the-middle-east-and-north-africa
https://openknowledge.worldbank.org/entities/publication/7c0dbf75-2bd7-4ae3-9db9-91318290c781
https://wmo.int/publication-series/state-of-climate-africa-2024

Africa in 2026 will continue to present both risk and opportunity for organisations that can convert uncertainty into structured choices.

– SHEILA MUENI

Continued Impact

INCREASED THREATS

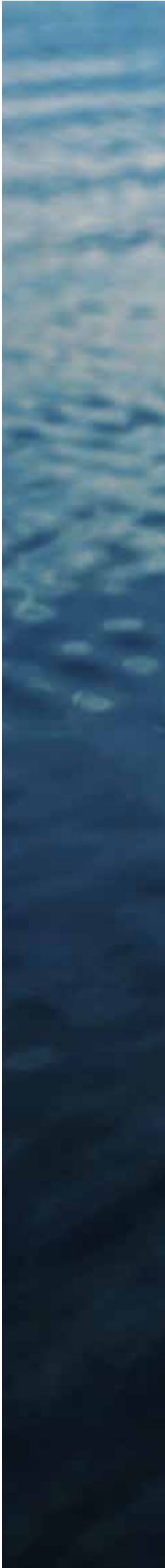
Introduction

Reflecting on the 2025 risk trends for Australia, many of the risks we highlighted as a threat, impacted and continue to do so in some way, shape or form. The increasing use of artificial intelligence (AI) in Australia has seen a greater need for AI guardrails and regulation applied. While there were increasing concerns on AI's implementation affecting the jobs security of the Australian workforce, particularly in the clerical and administrative type roles, the actual number of jobs lost in 2025 due to AI is lower than predicted. Cybersecurity threats continued at a high frequency, resulting in a greater need for investment from industry. This increased the financial burden on businesses and organisations.

Australia released its first National Climate Risk Assessment in 2025 highlighting the key climate risks the county faces from sea-level rise, mounting threats to health, infrastructure, and food security. The Australian Accounting Standards Board has introduced mandatory reporting standards, requiring organisations to develop climate related risk and opportunities and include as part of the reporting from 2025 onwards. The Sino-US trade war increased tensions in APAC, adding fuel to Australia's geopolitical concerns. Impacts on Australia's supply chain have resulted in a need for adjustments to ensure resilience.

Australia did not escape the impact of global conflicts with political alliances globally and domestically becoming strained. Sharp rises in major protests, including the largest political protest in Australia's history took place which tested Australia's previously strong multicultural democracy.

For Australia, 2025 has been one where the country has needed to be resilient to multifaceted and increasing threats and challenges.

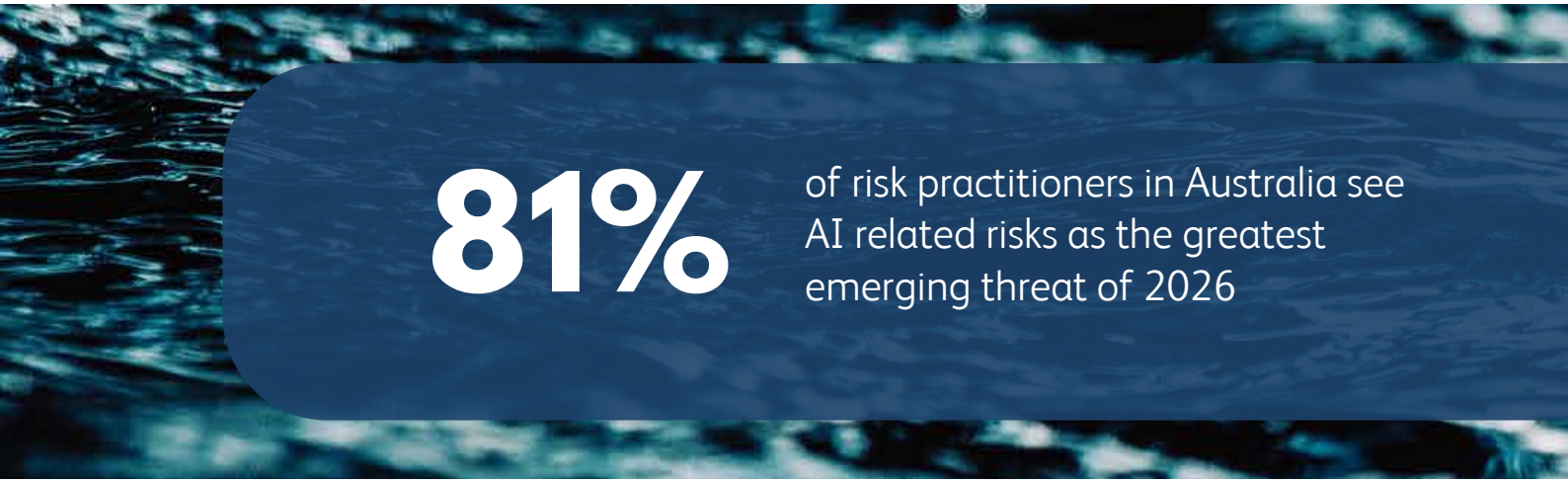


Australia Group

With the current landscape in Australia focusing on high-value and once-in-a-lifetime projects, our group has a unique opportunity to establish IRM best practices and cultivate the next generation of risk professionals with the institute's guidance. We believe in the power of collaboration and aim to create a regional forum where risk professionals and those interested in risk management can connect, share experiences, and further the principles of risk management across the Australian region.

This entry has been authored by:

- Colin McCrorey
- Rynier Brandt
- Anh Dinh
- Carl Fernando
- Mark Platt
- Cuong Quang
- Jon Boyle



Looking ahead to 2026, whilst the risk landscape has evolved significantly over the last 12 months, the common themes remain unchanged. As a group, we see AI, cybersecurity, climate, geopolitical, and socioeconomic risks as key opportunities and challenges for our region. Specifically, with the acceleration in the use of AI as well as the application of AI governance frameworks, we have also looked beyond Australia and into the wider Asia Pacific Region and how Australia can position itself in the AI race.

The interconnectedness between AI and cybersecurity has also been explored, where the threats of adversarial AI-driven exploits are expected to increase, resulting in more severe consequences.

AI

Artificial Intelligence is accelerating across the APAC region, but so too are economic, operational and societal risks that are expanding faster than governance and operating models can keep pace with. While security related AI threats draw significant attention, non security risks impacting talent, productivity, regulation, workforce transformation, fairness, and trust will shape enterprise resilience just as profoundly.

The following risks represent the most material strategic exposures that Australian enterprises must now anticipate and manage.

AI Skills and Talent Crisis

Across APAC there is a severe shortage of AI capable talent. 79% of employers are prioritising AI hiring, yet 75% cannot find qualified candidates and 79% lack the knowledge to implement meaningful AI workforce training programs. Skill requirements evolve 25% faster than traditional roles and fewer than half of applicants meet the baseline for AI positions. Australia faces an even more pronounced challenge. With strong domestic demand for AI capability and intense global competition for talent, Australian organisations risk slower AI deployment and weaker governance maturity. The gap between grassroots employee adoption and formal enterprise AI capability is widening, with many Australian workers experimenting with generative AI tools weekly despite limited organisational training or oversight. This mismatch increases operational risk while eroding potential productivity gains.

The AI Productivity Paradox and Poor ROI

APAC organisations are adopting AI at speed but often without the operating model changes required to realise actual business value. Across the region, 81% of organisations report heavy data silos and only 28% say their applications are adequately integrated, leaving enterprise AI systems underperforming. Australian enterprises mirror these challenges. 67% are purchasing AI from multiple vendors but struggle to integrate systems effectively.

73% of risk practitioners in Australia identified climate change risk as requiring the greatest investement in 2026

This results in a productivity paradox where capital investment in AI increases while measurable returns remain limited. Without improvements in data governance, skills development and workflow redesign, Australian organisations risk perpetual experimentation instead of genuine transformation.

Regulatory Fragmentation and Uninsured Liability Gaps

Across APAC the regulatory environment is highly fragmented. China maintains strict AI registration requirements with penalties up to CN¥50 million, South Korea requires comprehensive assessments in critical sectors, Japan relies on voluntary guidelines and Singapore uses soft-law frameworks. Insurance markets are also lagging, with traditional indemnity and product liability policies either silent or exclusionary on AI-related harms, leaving organisations exposed to claims from biased underwriting, discriminatory hiring or flawed automated decisions.Australia lacks dedicated AI legislation and scored between 78 % and 93 % inadequate across five AI threat categories in a national stress test, with loss-of-control scenarios rated the weakest. The country relies on a combination of voluntary frameworks, sector-specific rules and existing non-AI specific laws such as the Privacy Act. Liability for AI decisions remains ambiguous, particularly when systems operate across borders. Insurance coverage for AI exposures is uncertain for both large and mid-market organisations.

Workforce Displacement Exceeding Social Safety Nets

APAC economies are facing accelerating automation and heightened workforce anxiety. Surveys show workers across the region fear job loss at significantly higher rates than global averages, with many operating in sectors where up to 88 % of roles are at risk of automation.

The disconnect between employee adoption of AI and limited organisational upskilling increases the likelihood of displacement without offsetting productivity or wage growth. Australian enterprises often lag regional peers in workflow redesign for AI, meaning automation pressures materialise before new value pathways or retraining programs are fully in place. This creates social and organisational risks that may overwhelm existing workforce transition mechanisms.

Algorithmic Bias and the Deepening Digital Divide

Algorithmic systems used for credit decisioning, hiring and customer service frequently embed bias. Liability frameworks remain unclear because laws assume human intent and struggle to address harms caused by autonomous systems. Large populations in the region also face connectivity and skills barriers that limit their ability to participate in AI-enabled economic growth.

Cybersecurity

Current State Challenges

Cybersecurity awareness and maturity have improved among medium and large corporates and government agencies, while smaller organisations and small businesses have made targeted efforts but still have substantial gaps. Many may not fully appreciate their current level of exposure.

The rapid expansion and complexity of information technology environments demands ongoing enhancement of cyber defences, incident detection, and response capabilities. Resilient security now depends on continuously improving SIEM processes, risk-based vulnerability management, and progressive hardening of systems, network architectures, and endpoints.

Hostile activity is increasing as malicious actors continue to benefit from successful compromises, with a relatively low likelihood of prosecution even when state or criminal groups are identified. Attackers are increasingly using AI to refine exploit strategies and probe attack surfaces more efficiently. In 2026, organisations will need to lift their resilience significantly as these AI-enabled threats grow in sophistication and begin to outpace the defences of major corporations and government agencies.

Emerging technology and identity risk

Escalating exploit sophistication targeting infrastructure and security architectures is expected. What is changing is the use of AI to accelerate both the volume and success rate of attacks.

User identity, both human and non-human, has become a central pillar of modern cybersecurity strategy. The rapid proliferation of applications, automation, and machine identities has created substantial identity-management debt, making it harder to protect access privileges and monitor anomalous behaviour at scale.

Existing cybersecurity controls

Many organisations have substantially matured their cybersecurity controls, supported by standards such as ISO 27001 and ISO 42001, NIST frameworks, network security architectures, robust firewall configurations, recognised endpoint-hardening practices, vulnerability assessment tools, and established SOC processes. These tools and systems now require faster processes and more responsive, SOC-driven decision-making.

Cyber teams increasingly need AI-assisted capabilities that can continuously monitor, correlate, and respond to events in line with security policies while preserving legitimate business operations and continuity.

Enterprise IT and cybersecurity teams will also need to strengthen encryption to resist emerging post-quantum decryption capabilities. The design and use of VPNs and related secure-channel solutions must be reviewed to protect a workforce that is more mobile, remote, and reliant on BYOD than ever.

Demand on directory services to manage both human and non-human credentials and permissions is growing rapidly, particularly for privileged access used in administration, automation, and legitimate AI operations. Reporting and analytics requirements for compliance and least-privilege enforcement are pushing beyond the practical limits of human-only analysis, making behavioural and pattern-based approaches essential except in narrow forensic investigations.

Preventive and reactive control evolution

Adversarial, AI-driven attack techniques are likely to mature quickly in the coming years. As agentic AI systems trained on specific technology stacks emerge, organisations will need strategic controls that verify the legitimacy of non-human identities, detect adversarial AI agents, and lock them out while tracing their origin so associated agents can also be identified and blocked.

Reliance on default platform security capabilities is becoming less sufficient as threat actors innovate.

Defence will increasingly depend on robust identity and access management for both human and non-human users and on strong privileged access management as a core control layer.

There is also a growing need for state and industry level repositories of cybersecurity intellectual property and defensive patterns. Such repositories would capture reference architectures, reusable security design components, and proven tool deployment models, helping enterprises accelerate and standardise their own cyber capabilities.

Over time, high-performance, AI-enabled or quantum-capable platforms may be trained specifically to generate and adapt countermeasures against adversarial AI systems.

Key emerging threats for 2026 and beyond

- Progressively more capable, infrastructure-aware adversarial AI platforms and agentic AI systems that imitate legitimate user behaviour to obtain privileged access and exfiltrate data, steal intellectual property, cause disruption, or extort organisations.
- AI poisoning attacks that corrupt or manipulate data and models underpinning enterprise AI systems, causing skewed, unreliable, or malicious outputs.
- Intensifying state-sponsored use of AI and data-driven intelligence to influence geopolitical outcomes and conduct cyber operations, followed by downstream adoption of similar techniques by other states or criminal networks.
- An emerging contest between AI systems designed to protect and benefit society and adversarial AI systems developed for financial gain, coercion, or strategic advantage.
- Heightened tension in the Asia-Pacific region driven by resource competition and strategic rivalry, which is likely to underpin greater use of AI and more frequent, sophisticated cyber intrusions and subversive campaigns.

Climate Risk

The Australian Accounting Standards Board (AASB) has formally issued two Australian Reporting Standards (ASRS) in September 2024, namely AASB S1 General Requirements for Disclosure of Sustainability-related Financial Information and ASB S2 Climate-related Disclosures, aligning with the standards issued by the International Financial Standards Board standards. The first reporting cycle is for the 2025 financial year and requires companies that meets relevant criteria to disclose climate-related risks and opportunities (CRROs).

As directors are taking accountability for the quality of information and the need to avoid 'green washing', a need for benchmarking and assurance over the information disclosed have been identified. The development and disclosure of CRROs, internal quality assurance processes and assurance over the disclosures remains a significant focus area requiring a collaborative approach between enterprise risk, finance and sustainability functions.

A very topical issue is disinformation about the impacts of climate change. Organisations are basing scenario planning and risk assessments of climate predictions over the short, medium and long term. This may vary over time and requires careful scrutiny of available climate forecast data and the impact on physical and transition risks. Climate risk is and will continue to be a key risk for Australia to manage in 2026 and well beyond.

Geopolitical Risk

Geopolitical risk is defined as 'threat, realisation and escalation of adverse events associated with wars, terrorism and any tensions among states and political actors that affect the peaceful course of international relations'. Whilst this is not a new risk, globally geopolitical risk has intensified since 2021 and has resulted in increasing pressure on both governments and business sectors.

This risk impacts diplomatic relationships, economy and investment decisions. It is acknowledged that geostrategic shifts pose major challenges for risk-based decision-making. Australia's prosperity is inextricably intertwined with the global economy.

Despite anticipation, global growth demonstrated its resilience for the first half of 2025. However, the threats from further tariff hikes, policy changes and increased inflation could spark economic uncertainty and market volatility.

Deterioration of trade relationship between the US and China has led to a flourish of investment restrictions damaging the global supply chain as well as the rise of cyber and military threats. Australia has been able to manage its relationships with both the US, which relationship is characterised by cultural similarities and robust bilateral arrangements, and China, Australia's largest trading partner. China's increasing influence on the Pacific Region has required the Australian government to step up its commitment in military, investment, and infrastructure development. Russia's on-going full-scale invasion to Ukraine and persistent aggression to its neighbouring countries poses cyber threats and the energy market. Australia's digital infrastructure is heavily reliant on global supply chain. Along side the benefits of staying ahead with the latest technological advancements, Australia and its business has become more vulnerable to malicious actors over the past 12 months. Geopolitical risk is now a reality and Australia's need to be resilient against fickle global situations is now paramount.

Australia's Socioeconomic Risks

As much of the world faces an increase in the cost of living, Australia is no different, with its socioeconomic pressures. It does, however, have a unique problem with three Australian cities: Sydney, Melbourne & Adelaide within the Top 10, and Brisbane in the Top 20 most expensive cities around the world to buy property.

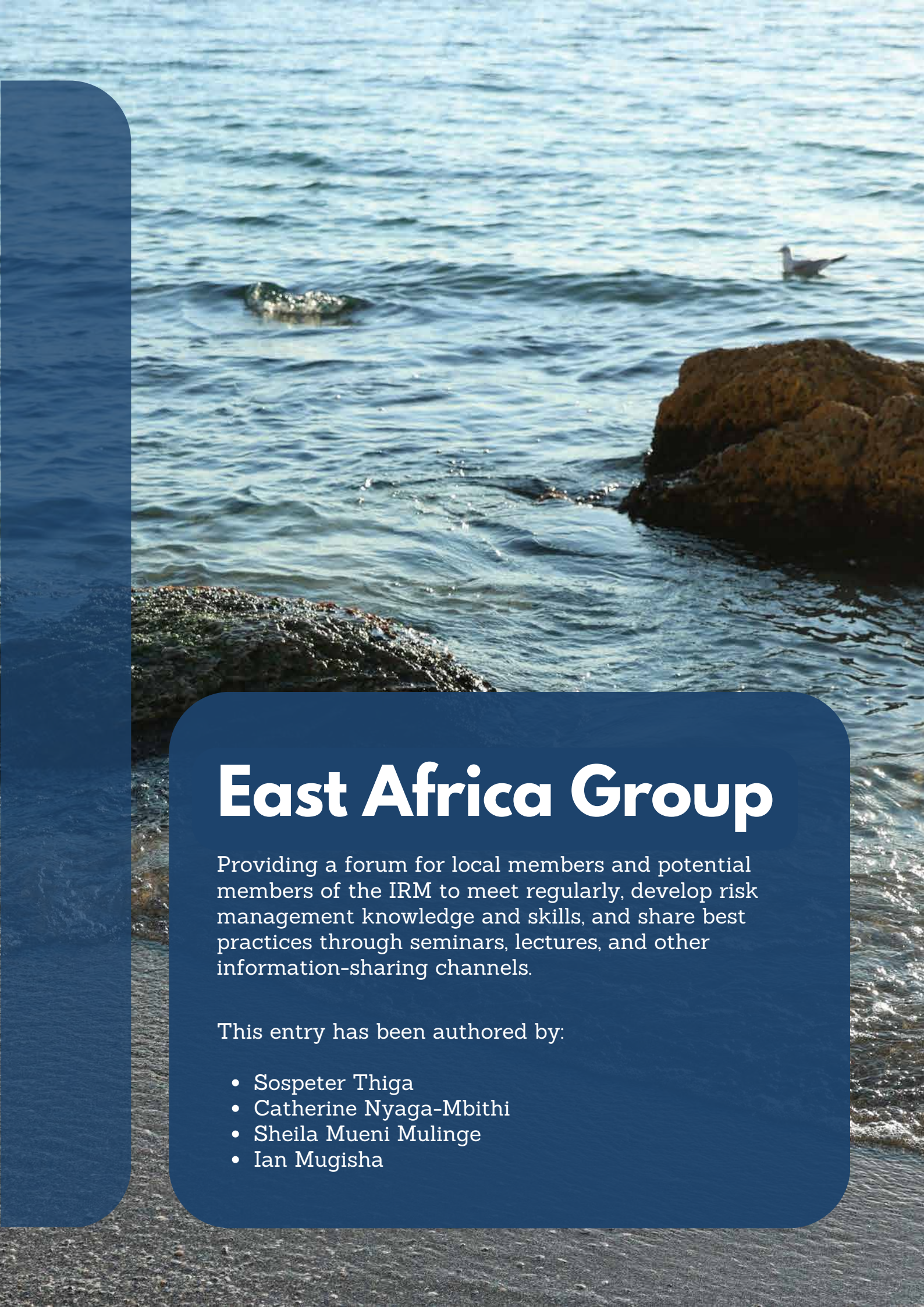
There are two elements to property ownership: firstly, Australians see property as one way to build wealth through asset ownership, working towards retirement, and secondly, the perception of success, feeding into the Australian dream of home ownership. It is worth noting that the ever-growing difficulty to get on the property market, for both individuals and families, increases the threat of forcing people into a position of having to rent for a longer period of time or potentially face renting forever. This trend has created a feeling of hopelessness among younger generations and has increased pressure on renters who face soaring rent prices coupled with a reduction in available properties.

With a lookahead to 2026, the pressure on the Australian Government will only increase as this socioeconomic risk continues to grow. In a bid to combat the housing crisis, the Government announced the planned construction of 1 million homes and later revised and increased the target to 1.2 million by 2029, supporting local governments through improved planning capability, delivery enabling infrastructure such as roads, water, and power, and building more social housing. Even so, this ambitious target isn't without challenge, as the current workforce requires an additional 90,000 workers in order to raise housing construction rates to meet the target of 60k homes per quarter.

Despite this, as 2025 comes to a close, the challenge to meet the 2029 target faces fresh scrutiny as analysts now estimate that Australia commenced 60k fewer homes, with construction needing to reach 64k homes per quarter from next year. The Australian Government will have to address the shortfall, with a stronger focus on the increased workforce through various measures.

The 2029 vision still holds value, but without decisive action, housing affordability will severely impact current and future generations.

https://www.chapman.edu/communication/_files/Demographia-International-Housing-Affordability-2025-Edition.pdf https://www.news.com.au/finance/real-estate/housing-in-four-major-aussie-cities-rated-impossibly-unaffordable-by-new-study/news-story/2bc4a805032e41fc9b6c51ede8b6669b?amp
https://www.theaustralian.com.au/breaking-news/great-australian-dream-slipping-away-from-aspiring-homeowners-in-one-state/news-story/5e7fcf58bbd610c2d390bed460cbeb9f?
https://www.theaustralian.com.au/subscribe/news/1/?
mode=aod&offerset=ta_default&utm_medium=GooglePerformanceMAX&int_source=GooglePerformanceMAX&int_campaign=2023_National_Paid_Media&int_content=GooglePerformanceMax&sourceCode=TAWEB_WRE170_a_MAX_P&gclsrc=aw.ds&gad_source=1&gad_campaignid=21811745493&gbraid=0AAAADshBGXafT77jea7SfHJ00Oh3R4gY&gclid=CjwKCAiAz_DIBhBJEiwAVH2XwDXzKuSQyt4Bfagm3ebtFbMojob2DFlrajIQJ5SDBl-R72H2KISbYBoCdm4QAvD_BwE https://www.abc.net.au/news/2025-03-27/australians-forever-renters-housing-crisis-property-market/105051202
https://www.swinburne.edu.au/news/2024/10/Overwhelmed-hopeless-crushed-Swinburne-report-reveals-how-housing-crisis-is-reshaping-young-peoples-lives/
https://www.news.com.au/finance/economy/australian-economy/grim-warning-about-renting-in-australia/news-story/1564311f862627b6cbcd16101eb33f23?amp
https://budget.gov.au/content/03-housing.htm https://www.abc.net.au/news/2024-03-24/90-000-extra-construction-workers-needed-to-be-on-track-for-goal/103625934
https://hia.com.au/our-industry/newsroom/economic-research-and-forecasting/2025/10/1-2-million-target-too-important-to-abandon?
srsltid=AfmBOorODfKkJ3QzPsdTBtwfO2WydZqc40BSD-ef9WcYMSYFMo-bWo-x
https://buildskills.com.au/news/90m-to-get-more-workers-into-building-trades Artificial Intelligence and machine learning - supply chain risks and mitigation (ASD & ACSC Oct 2025) AI SECURITY CONCERNS IN A NUTSHELL German Federal Office for Information Security (Mar 2023) Information Security Manual September (ASD 2025) Adapting Cybersecurity to the AI Era - How US Organisations are Reshaping Cybersecurity Programs (2024 Infographic C1 Edge Research) Cybersecurity Information Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era (Jan 2025) Convoluted Layers: An Artificial Intelligence (AI) Primer (ASD current Cyber.gov.au) ASD Joint Cybersecurity Information AI Data Security (May 2025 V1) ASD Joint Cybersecurity Information Deploying AI Systems Securly (Apr 2024 V1) Guidelines for secure AI system development (Nov 2023) Agentic AI: Understanding Its Evolution, Risks, and Security Challenges (Mar 2025) Agentic AI - Threats and Mitigations OWASP Top 10 for LLM Apps & Gen AI Agentic Security Initiative (HAL Open Science Mar 2025)
https://www.bankingsupervision.europa.eu/framework/priorities/html/geopolitical-risk.en.html https://www.matteoiacoviello.com/gpr.htm https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2025.pdf
https://www.oecd.org/en/publications/2025/09/oecd-economic-outlook-interim-report-september-2025_ae3d418b.html https://www.dfat.gov.au/geo/united-states-of-america/united-states-of-america-country-brief
https://www.dfat.gov.au/trade/agreements/in-force/chafta/negotiations/background-paper-the-australia-china-trade-and-investment-relationship
https://www.bankingsupervision.europa.eu/framework/priorities/html/geopolitical-risk.en.html https://www.afr.com/policy/foreign-affairs/china-to-step-up-pacific-push-after-australia-png-defence-treaty-20251003-p5mzu9
https://www.cdotrends.com/story/3805/apac-businesses-poorly-equipped-leverage-ai
https://www.forbes.com/sites/anjanasusarla/2025/08/25/productivity-paradox-redux-what-leaders-need-to-know-about-incentives-in-genai-adoption/
https://nanda.media.mit.edu/ai_report_2025.pdf
https://www.korumlegal.com/blog/evolving-ai-laws-in-asia-regulations-and-key-challenges
https://amplyfi.com/blog/why-australias-ai-laws-fail-the-stress-test-five-threat-categories-assessed/ https://iapp.org/resources/article/global-ai-governance-australia/
https://www.kennedyslaw.com/en/thought-leadership/article/2025/emerging-silent-ai-risks-in-asia-pacific-apac/ https://hdff.org/bridging-the-digital-divide-human-centered-innovation-and-inclusive-growth-in-southeast-asia/ https://www.fairplaytalks.com/2025/10/31/asia-pacific-leads-the-world-in-ai-adoption-but-workers-fear-job-loss-survey-shows/
https://aiasiapacific.org/our-work/2025-ai-and-workforce-transformation-unlocking-pathways-to-inclusive-growth-in-asean-developing-economies/
https://finance.yahoo.com/news/asia-pacific-leads-world-ai-030100826.html?guccounter=1
https://www.cliffedekkerhofmeyr.com/en/news/publications/2025/Practice/Employment-Law/Combined-employment-law-and-knowledge-management-alert-26-sept-How-algorithmic-bias-in-AI-hurts-your-business-and-what-you-can-do
https://www.thoughtspot.com/data-trends/artificial-intelligence/ai-concerns
https://ablawyers.com.au/resources/articles-downloads/bias-by-algorithm-can-ai-make-you-liable-for-discrimination https://www.eftsure.com/en-au/statistics/deepfake-statistics/
https://corpgov.law.harvard.edu/2025/05/12/misinformation-and-disinformation-in-the-digital-age-a-rising-risk-for-business-and-investors/ https://www.resolver.com/blog/ai-generated-misinformation-brand-risks/



East Africa Group

Providing a forum for local members and potential members of the IRM to meet regularly, develop risk management knowledge and skills, and share best practices through seminars, lectures, and other information-sharing channels.

This entry has been authored by:

- Sospeter Thiga
- Catherine Nyaga-Mbithi
- Sheila Mueni Mulinge
- Ian Mugisha

Critical Juncture

EAST AFRICA IN 2026

East Africa stands at a critical juncture in 2026. The region, comprising Kenya, Uganda, Tanzania, Rwanda, Burundi, South Sudan, Somalia, Ethiopia, and the Democratic Republic of Congo (DRC), faces a complex and evolving risk landscape shaped by economic pressures, political transitions, climate volatility, and rapid technological transformation. This report represents the culmination of a comprehensive virtual consultation conducted by the Institute of Risk Management Africa, bringing together risk practitioners from together to identify, analyse, and prioritize the most significant risks facing East Africa in 2026.

The risks outlined are not isolated threats but interconnected challenges that amplify one another. Economic instability fuels political tensions; climate shocks exacerbate social inequalities; weak governance undermines regulatory effectiveness; and rapid digitalisation without adequate safeguards creates new vulnerabilities even as it offers transformative opportunities. Understanding these interconnections is essential for developing holistic risk management strategies that address root causes rather than symptoms. This report aims to provide East African organizations, governments, and risk practitioners with a realistic yet forward-looking assessment of the risk environment, along with practical recommendations for building resilience, seizing opportunities, and navigating uncertainty in the year ahead.

Critical Risk Themes for East Africa 2026

Economic and Financial Risks: Debt Burden, Aid Pressures, and Liquidity Strains
East Africa's economic landscape is dominated by mounting sovereign debt, foreign exchange shortages, persistent inflation, and, critically, sharp reductions and increasing uncertainty in Western aid flows threatening decades of progress. Kenya faces acute debt servicing burdens consuming an increasingly large share of government revenues, while Tanzania, Uganda, and the Democratic Republic of Congo grapple with similar pressures amid currency depreciation. Significant funding cuts and shortfalls affecting programs supported by USAID, UK aid, and the World Food Programme have exposed dangerous dependencies, particularly impacting HIV/AIDS treatment programs, vaccinations, food security, and humanitarian assistance. Countries hosting large refugee populations (Uganda and Kenya together host well over two million refugees and asylum seekers) face acute challenges as international support diminishes or becomes more unpredictable while needs remain high or increase. These liquidity and foreign-exchange pressures extend beyond government finances to affect the broader financial sector and real economy.

In many countries, banks are experiencing tightening conditions as foreign exchange reserves decline and capital flows become more volatile, directly impacting businesses reliant on imported inputs and consumers facing rising prices for essentials. Construction and manufacturing sectors have been particularly affected, with projects stalling due to the inability to access foreign currency. Small and medium enterprises, forming the backbone of East African economies, are especially vulnerable, often lacking the financial buffers needed to weather extended economic stress.

Kenya's role as the regional trade hub and port of entry for landlocked neighbours amplifies economic contagion effects significantly. Kenya exports manufactured goods, agricultural products, and services throughout the region while serving as the critical gateway for imports destined for South Sudan, Uganda, Rwanda, Burundi, eastern DRC, and beyond. Economic disruption in Kenya (whether from currency devaluation, debt distress, or liquidity shocks) ripples across borders, affecting supply chains, market access, and regional trade flows. Similarly, instability in DRC or South Sudan creates refugee flows and security challenges affecting neighbouring countries' fiscal positions.

A financial sector crisis in one country can trigger bank runs and capital flight in neighbours as depositors and investors lose confidence in regional financial stability. The interconnected nature of these economic risks means a shock in one area could trigger cascading failures throughout the regional economy, affecting employment, business viability, social stability, and ultimately political legitimacy across multiple countries simultaneously.

Fiscal constraints are forcing countries to become more frugal and demonstrate better governance in fund management, a silver lining that could strengthen long-term economic sustainability if properly institutionalised.

2. Political and Governance Risks: Electoral Cycles and Institutional Fragility

Political risk dominates East Africa's 2026 landscape, with electoral cycles in Uganda and Tanzania creating environments of heightened uncertainty. Tanzania's October 2025 nationwide internet blackout during elections exemplified how political events directly disrupt business operations and fundamental freedoms. The challenge extends beyond elections to encompass weak institutions, limited checks and balances, concerns about electoral integrity, and potential for disputed outcomes triggering civil unrest or authoritarian responses.

Regional security dynamics add complexity, with cross-border tensions involving Somalia, South Sudan, and eastern DRC generating refugee flows, disrupted trade routes, and security incidents affecting neighbouring states. Armed groups in eastern DRC impact security in bordering areas of Uganda, Rwanda, and Burundi. Ongoing conflicts in Sudan and South Sudan create humanitarian crises with regional implications. The interconnected nature of East African economies means political instability in one country can quickly affect neighbours through trade disruptions, refugee movements, and shifts in investor sentiment.

3.Regulatory and Compliance Risks: Navigating Rapid Change and Inconsistency

East Africa's regulatory environment is characterised by rapid change, limited stakeholder consultation, and significant enforcement inconsistency. Organisations face evolving requirements in taxation, labour law, environmental standards, data protection, financial regulation, and ESG expectations. Despite regional harmonisation efforts, regulatory frameworks across East African Community member states remain substantially different. Kenya's mature mobile money regulatory framework contrasts sharply with more restrictive or underdeveloped frameworks in neighbouring countries, creating challenges for consistent regional service delivery.

Data protection regulations vary significantly, with some countries having comprehensive laws while others lack clear frameworks, creating uncertainty about cross-border data flows.

Enforcement inconsistency adds another dimension. Even where regulations are clear, application can be unpredictable depending on officials, political context, or other factors unrelated to actual compliance status. The emergence of new regulatory areas including climate disclosure, beneficial ownership transparency, and digital taxation creates additional burdens when many organizations are already stretched managing existing requirements.

4.Climate Change and Environmental Risks: From Crisis to Catastrophe

Climate change has moved from future threat to present crisis, with 2026 projected to bring continued climate volatility threatening lives, livelihoods, and economies. The region experiences both extremes: prolonged droughts devastating agriculture and depleting water resources, and intense flooding destroying infrastructure, displacing communities, and spreading waterborne diseases. Kenya, Tanzania, Uganda, and DRC have experienced severe climate events with impacts ranging from failed harvests and livestock deaths to damaged infrastructure disrupting supply chains. Agriculture (employing the majority of East Africa's population and contributing significantly to GDP) is particularly vulnerable. Changing rainfall patterns disrupt traditional planting calendars while temperature increases affect crop yields and livestock productivity.

Coffee and tea (critical export crops) are especially sensitive to climate conditions, with implications for farmer incomes and national revenues. Food insecurity is increasingly pressing, with climate shocks reducing production as population growth increases demand. Water scarcity emerges as one of the most critical climate-related risks.

Major water bodies, including Lake Victoria, are experiencing highly variable water levels and more frequent extreme events, driven by changing rainfall patterns and other climate-related factors.

Rivers providing water for drinking, irrigation, and hydroelectric power generation are becoming less reliable in several basins. Energy security is directly threatened, as countries including Kenya, Uganda, and Ethiopia depend heavily on hydroelectric power that becomes unreliable during droughts, forcing expensive reliance on thermal generation and potentially leading to power rationing. The interconnected nature of water, food, and energy security means climate impacts in one area cascade through multiple systems, amplifying vulnerability.

5. Societal Risks: Gender-Based Violence, Inequality, and Social Cohesion

East Africa confronts a gender-based violence epidemic that reached alarming levels in 2024–2025, with rising reported cases and several high-profile femicides and other GBV incidents across Kenya, Uganda, and the broader region. This violence represents profound human tragedy and organizational risk, affecting workforce safety, mental health, productivity, and reputation. The GBV epidemic is symptomatic of deeper challenges including entrenched gender inequality, inadequate legal protections, economic stress, and cultural norms tolerating violence against women. Beyond gender-based violence, East Africa grapples with widening inequality threatening social cohesion. Economic growth has not been equally distributed, with wealth concentrated in urban areas while large segments struggle with poverty and limited opportunities. Youth unemployment is particularly acute, with millions entering the job market annually but finding few formal employment opportunities, creating frustration that can manifest in social unrest, crime, or recruitment into extremist movements. Social cohesion is further strained by ethnic and religious tensions that periodically flare into violence, particularly during politically sensitive periods.

Rapid urbanisation creates new social dynamics as diverse populations come together in rapidly growing cities with inadequate infrastructure.

6. Technological and Cybersecurity Risks: Digital Disruption and Vulnerability

East Africa's rapid digital transformation offers opportunities but creates significant cybersecurity risks. Innovations like M-Pesa demonstrate technology's transformative potential, yet rapid digitalisation has outpaced the development of adequate cybersecurity infrastructure, skills, and governance. Organisations experience increasing cyber threats, including ransomware, data breaches, business email compromise, and fraud resulting in financial losses, operational disruptions, and reputational damage.

The cybersecurity challenge is compounded by significant skills gaps. There is a shortage of qualified cybersecurity professionals, and many organisations lack basic security awareness among general staff who may inadvertently create vulnerabilities. Small and medium enterprises are particularly vulnerable, often operating with minimal cybersecurity measures while increasingly reliant on digital systems. Regulatory frameworks for data protection and cybersecurity are evolving but remain inconsistent across the region. The political dimension of technology risk emerged clearly during recent electoral periods when governments implemented internet shutdowns or social media restrictions, disrupting not only communications but also businesses dependent on digital connectivity.

7.Ethical Risks: Corruption, Fraud, and Integrity Deficits

Corruption remains deeply entrenched across East Africa, undermining economic development, eroding public trust, and distorting markets. Organisations face demands for bribes, encounter procurement processes compromised by favouritism, and navigate environments where personal connections often matter more than merit.

Corruption increases transaction costs, distorts resource allocation, compromises infrastructure projects through inflated costs and substandard materials, and diverts resources from essential public services. The cumulative effect is slower economic growth, reduced foreign investment, and perpetuation of poverty and inequality. For organisations, involvement in corruption creates legal liability under domestic and international anti-corruption laws, reputational damage that can be devastating in an era of social media and stakeholder activism, and internal cultural corrosion undermining ethical standards. The challenge of maintaining ethical standards is compounded by weak enforcement of anti-corruption laws, limited capacity, and sometimes compromised independence of oversight institutions, and cultural factors that can blur lines between acceptable relationship-building and unethical influence.

Opportunities from a Risk Perspective for East Africa in 2026

While East Africa faces formidable challenges, these risks simultaneously create pathways for innovation and sustainable growth. Fiscal constraints are sharpening governance reforms and fostering financial discipline, with countries becoming more frugal and demonstrating better fund management, potentially establishing stronger foundations for self-reliant development. Digital transformation, despite cybersecurity challenges, creates inclusive economic opportunities for the region's young, tech-savvy population. Supporting the digital economy and entrepreneurs represents a significant demographic dividend if properly channelled. Investment in agriculture offers opportunities to enhance food security, create employment, and drive rural development while building climate resilience. Climate challenges are stimulating investments in renewable energy and sustainable agriculture, positioning the region for leadership in green initiatives and access to climate finance. Increasing attention to ESG frameworks and transparent governance attracts responsible investment and promotes stable stakeholder relations.

Fiscal constraints are forcing countries to become more frugal and demonstrate better governance in fund management, a silver lining that could strengthen long-term economic sustainability if properly institutionalised.

– IAN LIVSEY, IRM CEO

The heightened awareness of gender-based violence and social inequalities is prompting more holistic social interventions, integrating human rights into corporate and public policy agendas. Collaborative regional approaches facilitate shared learning and resource optimisation, with the strengthening of the East African Community creating economies of scale and collective bargaining power. Supporting SMEs through accessible risk management tools and financial support can unlock entrepreneurial potential. Enhanced focus on business continuity, data protection, and cybersecurity prepares organisations to minimize impact when risks materialize, turning preparedness into a competitive advantage.

Key Recommendations for 2026

1. Strengthen Fiscal Sustainability and Public Revenue Efficiency

East African countries must build self-reliant, transparent public revenue systems that sustain development without excessive aid dependency. Develop sustainable domestic financing for essential services. Prioritize efficient resource use and invest in high-multiplier sectors like agriculture and the digital economy. Strengthen health infrastructure and social protection systems capable of withstanding external shocks.

2. Enact and Enforce Robust Legislation and Policy Frameworks

Strengthen legal frameworks addressing corruption, gender-based violence, environmental protection, and cybercrime with consistent enforcement by adequately resourced, independent institutions. Harmonize regional legislation to reduce compliance complexity and facilitate cross-border cooperation. Ensure penalties serve as meaningful deterrents. Protect enforcement institutions from political interference while supporting civil society and media oversight roles. Organisations should actively engage in policy development to ensure regulations are practical and implementable.

3. Embed Ethical Governance Across All Sectors (Public and Private)

Make integrity a core organisational value with leadership modelling ethical behaviour. Establish clear codes of conduct, implement ethics training developing ethical reasoning capabilities, and create safe reporting channels with whistleblower protections. Boards must ensure adequate ethics risk management. Extend ethical governance to supply chains through third-party due diligence. Educational systems must cultivate integrity from early education through professional practice, building societal norms of accountability.

4. Invest in Continuous Learning and Capacity Building

Build capabilities in emerging risks (climate change, cybersecurity, ESG integration) through sustained investment in professional development, certifications, and training. Extend risk literacy beyond practitioners to boards, executives, and operational staff. Strengthen university programs, support regional research, and develop professional associations facilitating knowledge exchange. Create communities of practice enabling peer learning and collaboration across the region.

5. Leverage Technology for Risk Detection and Management

Adopt advanced analytics, AI-powered pattern recognition, and real-time dashboards for proactive risk monitoring. Implement automated compliance systems tracking regulatory changes across jurisdictions. Use scenario modelling to test resilience. Accompany technology adoption with robust cybersecurity investments including technical controls and security awareness training. Bridge digital skill gaps through training programs. Governments should support adoption through favourable policies and public-private partnerships.

6. Cultivate Local and Global Collaborative Networks

Sustain and deepen collaborative networks providing platforms for sharing risk intelligence,

exchanging best practices, and coordinating responses to shared challenges. Strengthen collaboration between government, private sector, civil society, and academia within countries. Enhance East African Community institutions to coordinate regional responses to transboundary risks. Develop international partnerships providing access to resources and expertise while ensuring East African perspectives inform global discussions.

7. Build Resilient Systems and Institutions with a Self-Reliance Mindset

Embrace the reality that "nobody's coming to be the saviour." East Africa must build its own resilience. Governments should maintain fiscal prudence, build strategic reserves, invest in climate-resilient infrastructure, and develop adaptive governance structures. Organisations should move beyond efficiency optimisation toward strategic redundancy in supply chains, financial reserves, and backup systems.

Implement comprehensive, regularly tested business continuity plans covering political instability, climate disasters, pandemics, and cyber-attacks. Develop organizational agility enabling rapid adaptation. Strengthen community-level social protection systems and local emergency response capacity.

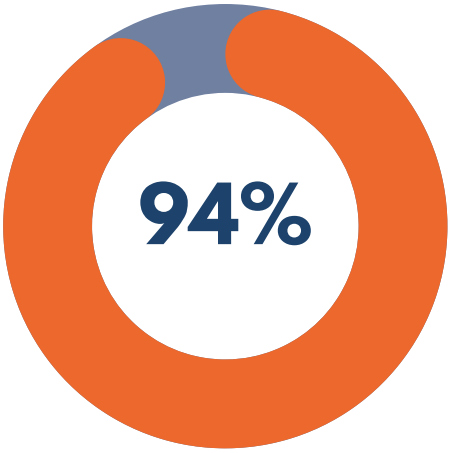
Conclusion

East Africa's 2026 risk landscape poses significant challenges yet embodies promise. Organisations must tighten controls, particularly around business continuity, data protection, and cybersecurity, areas where vulnerabilities could prove costly. Prior experience shows that proactive, transparent risk management coupled with integrity can transform vulnerabilities into growth opportunities.

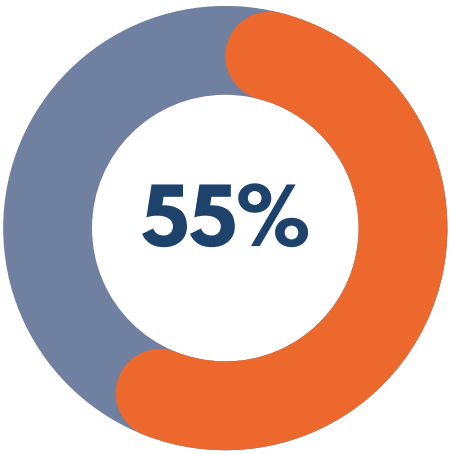
Innovation in the digital economy, environmental consciousness, investment in high-multiplier sectors like agriculture, and demographic potential offer pathways to sustainable development.

Success requires courage to make difficult decisions, collaboration across boundaries, and commitment to sustained effort.

The seven recommendations provide a practical roadmap grounded in regional realities. They are achievable, but only if stakeholders at all levels (from risk managers to boards to government ministers to regional institutions) commit to action. The call is clear: embrace risks with resilience, leverage opportunities with insight, and forge a future anchored in dignity, equity, and prosperity for all East Africans.



of African risk practitioners view the rapid implementation of Artificial Intelligence as the greatest emerging risk in 2026, specifically highlighting concerns around ecological and climate related risks.



of African risk practitioners identified 'S trategic risk leadership and decision-making' as the skill area which will be most critical for developing their organisation's risk management capabilities over the next years.

India Group

The IRM India Regional Group supports the activities pursued by the IRM India Affiliate. IRM in India is focused on empowering students, professionals, and all types of organisations with IRM's globally recognised 5-Level qualifications and industry training in enterprise risk management.

The group aims to expand IRM's global risk community by advancing and generating value for the ERM profession in India. With the highest standards of ethics, education, research, and knowledge that improve outcomes for organisations through our qualified students and members.

This entry has been authored by:

- Rajeev Tanna
- Jyoti Ruparel

Disruption

REGULATORY REALIGNMENTS IN INDIA

The global and Indian business landscape in 2026 is marked by unprecedented complexity and interdependence. Economic cycles, technological disruptions, regulatory realignments, and geopolitical shifts are converging to create an environment that is dynamic, uncertain, and deeply interconnected. For businesses, this means navigating volatility while addressing ambiguity and rapid transformation. Yet, within these challenges lie significant opportunities those who embrace agility, leverage policy incentives, accelerate digital transformation, and diversify supply chains will not only build resilience but also secure a sustainable competitive edge in this dynamic era.

The year 2026 is expected to present a mixed economic landscape globally and for India. Global growth is projected to remain moderate at around 3%, with advanced economies slowing due to tight monetary conditions and trade fragmentation, while emerging markets sustain relatively stronger momentum. Inflation is easing but remains above targets in some regions, and geopolitical tensions continue to weigh on supply chains. Energy markets are likely to stay well-supplied, keeping oil prices stable, though commodity volatility persists.

India, on the other hand, is poised to remain one of the fastest-growing major economies, with GDP growth estimated at 6–6.3%, supported by domestic consumption, infrastructure investments, and manufacturing incentives such as PLI schemes and semiconductor initiatives. Inflation is expected to hover near 4%, assuming normal monsoon and stable commodity prices. However, fiscal consolidation efforts, global trade headwinds, and climate variability introduce significant uncertainties that businesses must factor into their planning.
The broader outlook on India remains positive with India outperforming peers due to its diversified economy, stable government, and ample foreign exchange reserves (~US$700.2 billion as of Sept 2025). India continues to demonstrate remarkable resilience and ambition in its journey toward becoming a developed nation by 2047.

With a projected GDP growth of 6.2% in 2026 and 6.4% in 2027 as per IMF, the country remains the fastest-growing major economy, supported by robust domestic consumption, infrastructure investments, and structural reforms. Currently, India is amongst the Top 5 largest economies in the world GDP ranking 2025 list. The IMF forecasts that by 2028, India will overtake Germany to become the 3rd largest economy worldwide.

Some of the key risks that would have an impact on India during 2026 include:

Impact of Global uncertainty (US-India trade deal)

- Global economic activity remained directionless during 2025, amid tariff uncertainty and supply chain risks. This led businesses to delay or scale back capital expenditure plans.
- U.S. tariffs on Indian goods remain steep at 50%, imposed since late August 2025 as part of a broader strategy to pressure India over its continued imports of Russian oil. These duties are among the highest levied on any major U.S. trading partner and have significantly eroded India's export competitiveness. Despite ongoing negotiations, an India–U.S. trade agreement is yet to materialise, leaving businesses exposed to prolonged uncertainty.
- Other countries may follow suit with tariffs. For example, Mexico has announced a sweeping tariff increase on imports from non-FTA countries, including India, effective January 1, 2026. These tariffs, ranging from 5% to 50%, will sharply raise the cost of Indian automobiles, auto parts, and a wide range of industrial and consumer goods in the Mexican market. This move could disrupt existing trade flows, force exporters to rethink pricing strategies, and potentially reshape supply chains. If similar measures are adopted by other nations, India's export competitiveness could face significant pressure globally.

Geopolitical shocks:

- Persistent geopolitical flashpoints from Middle East tensions that keep oil price volatility alive to ongoing military posturing in the South China Sea and Taiwan Strait pose dual risks of energy cost spikes and shipping route disruptions, amplifying inflationary pressures and supply-chain uncertainty for India's import-intensive sectors.
- Pakistan Escalation: April 2025, Pahalgam terror attack killed dozens of tourists, triggering India's counter operation.
- India's growing reliance on imported semiconductors and foreign-owned cloud infrastructure exposes critical sectors to heightened risks from global disruptions, such as export restrictions, supply chain shocks, or cyber conflicts.
- India's neighbourhood in chaos: India faces heightened regional instability, terrorism, increasing security costs, trade disruptions, and strategic uncertainty across its borders.
- Bangladesh Political Upheaval: Collapse of Sheikh Hasina's government in August 2024 led to an interim Yunus administration. 2025 saw border tensions and trade disruptions, with Dhaka rehabilitating ties with Pakistan and uncertainty ahead of February 2026 elections.
- Nepal Unrest: September 2025: Gen Z protests erupted after social media bans, leading to violent clashes and 19 deaths. PM KP Sharma Oli resigned, political instability raises concerns for India's border security.

Environment-related concerns

- Climate Change: India ranks 9th among the list of countries most affected by extreme weather events between 1995 and 2024, according to the Climate Risk Index 2026. India is affected by recurring and usually intense extreme weather events, which have, over the years, affected both people and the economy. In the last 3 decades, India faced around 430 extreme weather events like floods and landslides, heat waves, cyclones, and droughts, which resulted in inflation-adjusted losses of around $170 billion. More than 80,000 people were reported killed in these events. Focus on sustainability and ESG theme is likely to continue in 2026.

Technology Risks:

- Cyber Attacks/Data Breaches: Cyber incidents are expected to remain high in 2026. In an interconnected world where technology is the way of doing business, India's digital infrastructure could be a frontline target.

- As per Data Security Council of India (DSCI) - Healthcare, hospitality, and BFSI are most impacted sectors, while Telangana, Tamil Nadu and Delhi are classified as top targeted regions.
- AI & Automation Disruption - Rapid adoption could displace low-skill jobs, requiring urgent reskilling and workforce transition strategies

Manpower Risks

- Attraction and retention of talent: Intense competition for skilled professionals, rising employee expectations, diversity and inclusion challenges, and widening skill gaps make it harder to attract and retain top talent.
- Unemployment risk: Persistent youth underemployment, skill mismatches, and low-quality informal jobs could lead to social unrest and political pressure. Rapid automation and AI adoption may further exacerbate these issues.
- India's demographics: With over a billion citizens, the world's largest youth population, and deep digital penetration, India faces amplified vulnerabilities: misinformation can cascade at unprecedented speed, cyber breaches can compromise millions simultaneously, and algorithmic bias in AI-driven welfare or credit systems risks marginalizing entire communities, threatening social equity and trust in governance.
- Impacted Domestic capex - While public capital expenditure has been rising, private investment remains sensitive to global uncertainty, interest-rate cycles, and demand growth. If businesses stay cautious, the hope for a shift to private capex-driven growth may be delayed. That could dampen long-term job creation, outside government-backed infrastructure.

Political Risks:

- Continuation of schemes by government: Government of India has launched various schemes like PLI, Make in India, Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS), National Infrastructure Pipeline etc.

Regulatory and Compliance Risks:

- Four new labour Codes enforced and DPDP act has been notified (Nov 2025) – Implementation and complexities around same may emerge; state level issues may delay the overall implementation.
- Changes in regulations / laws, imposition of new taxes like amendments in corporate tax, Long Term Capital Gain (LTCG) etc. may lead to impact on FPI flows in India or the corporate earnings leading to impact on Capex.

Strategic Imperatives and potential strategies for risk treatment:

India's growth trajectory remains compelling, but the complexity of 2026 demands bold and decisive leadership. The convergence of global trade realignments, geopolitical volatility, technology disruptions, and climate risks requires organisations to move beyond incremental responses and embed resilience at the core of their strategies. This means diversifying supply chains, accelerating digital transformation, and implementing robust risk governance frameworks.

Equally critical is investing in talent and technology, reskilling the workforce to navigate automation, strengthening cyber resilience, and fostering an inclusive culture that attracts top talent. Strategic engagement with policymakers to secure trade advantages, coupled with disciplined execution of ESG commitments, will define competitive differentiation. India's strong fundamentals, a large domestic market, stable governance, structural reforms, and robust foreign exchange reserves, provide a buffer, but resilience does not mean immunity. Geopolitical tensions, regulatory transitions, and climate-related disruptions demand vigilant oversight. 2026 will hinge on anticipating shocks, adapting swiftly, and executing reforms decisively.

For the leadership of the companies, resilience is no longer optional—it is the mandate for sustainable growth and competitive advantage.

Macro Economics

FROM "STABLE" TO "POSITIVE"

In 2026, Nigeria will continue to face a mix of optimism and risks, many of which are economic, structural, and political. In November 2025, S&P Global Ratings revised its outlook on Nigeria from "stable" to "positive", indicating an improved situation. This stems from the recent monetary, economic, and fiscal reforms being implemented, which are expected to yield positive benefits over the medium and long term. The risk landscape also continues to evolve, driven by country-specific dynamics and response strategies therein, and also by regional and global interactions and interconnectedness. Below are details of projections of the most pressing risks and their mitigations, including some upside opportunities.

Macroeconomics and Inflationary Risk

Among the various macroeconomic metrics, inflation will be a risk factor to watch out for in the Nigerian economic landscape in 2026 after receiving so much attention in 2024 and 2025. Per the Nigerian Bureau of Statistics (NBS), inflation continues to decline on both a year-on-year and month-on-month basis in 2025. The average inflation rate has reduced to 16.05% as at October 2025 compared to 33.88% as at October 2024, making attaining the Federal Government's target of 15% achievable (IMF and Africa Development bank predictions were 23% and 21% respectively). Fighting back the persistent food price from 2024 may have gained momentum, but the risk that the central Bank may be unable to significantly cut interest rates (considering other factors) could restrain credit expansion and private sector investment.

Some economic effect on the financial sector for example, could be balanced out by the banking recapitalisation which is underway (with a march 2026 deadline). As 2026 is also a pre-election year, leading up to 2027 general election, increased spending and general focus on the politics and electioneering may challenge the gains already made.

Nigeria Group

The group collaborates with the government and other regulatory bodies in formulating policies pertaining to ERM practices in Africa as appropriate.

This entry has been authored by:

- Adebayo Adebeshin
- Joel Aimuemojie

Security Risk

The Nigerian Government acknowledges the insecurity challenge affecting parts of its northern Nigeria and other West African neighbouring countries. The implication of insecurity could be interconnected and multi-pronged across risk types. Towards the end of 2025, the government realigned its security configuration by making key personnel changes, indicating that 2026 will show renewed vigour to tackle the challenges. Further mitigations include prioritising security spending in the 2026 budget; fast-tracking prosecution; harmonising security operations; encouraging sub-national governments' action; and increasing international security coordination.

Debt Sustainability Risk

Despite successes from the ongoing reforms being implemented by the Nigerian Government, there exist concerns about the growing debt and the burden of servicing this debt over a longer period of time. Significantly relying on domestic borrowing to cover the deficit could have adverse implications on private sector and push up interest rates. Recent (externally driven) stricter monetary policy in developed economies like the USA could increase capital outflows from emerging markets like Nigeria, making it harder to attract stable Foreign Direct Investment (FDI) and putting renewed pressure on the currency. This is not a Nigeria-specific risk.

There are ongoing efforts to ramp up national revenue, leveraging the various tax reforms, and diversifying the economy to hedge global disruption in oil prices, thereby derisking the government's revenue projections, foreign reserves estimates and the exchange rate.

External geopolitical uncertainty impacting African economies

According to the World Economic Forum (WEF) 2025 risk report, geo-economic confrontation has elevated from a ranking of #14 in 2024 to #9 in 2025. This reflects the underlying tension across various economies, with severe implications for African economies, including Nigeria. This is driven by large-scale trade wars and restriction, protectionist measures, tariffs, sanctions, shift in global politics, conflict in regions such as Ukraine, Middle East, Asia. This risk tends to have a ripple effect on other aspects such as global supply chain, financial markets, capital allocation decisions, investment decisions, decline in global stock market, inflation, currency volatility, supply chain and security issues.

Nigeria continues to maintain strategic foreign policy position coupled with required diplomacy to mitigate deterioration in relations with key global players, potentially protecting against higher tariffs which could disrupt its exports and limit access to international markets and financing, which could weigh heavily on growth.

Proactive businesses stay agile by diversifying supply chains, considering regional and local supply options (where feasible), developing deliberate geopolitical risk mitigations at corporate level, and strengthening multi-layered international partnerships.

Technology and Cyber Security Risk

Nigeria continues to develop its digital economy through a combination of private sector innovation and the government's deliberate strategy. This aggregates into an increased reliance on digital infrastructures to power its economy and foster growth across various industries, as seen, for example, in its digital payment platform innovation. Technology and cybersecurity risk will therefore remain applicable to Nigeria in 2026, as it is with the rest of the global community, but exacerbated by Nigeria's own speed of technology adoption and penetration (considering year-on-year self-comparison). Increased technology adoption and global democratisation of technology knowledge.

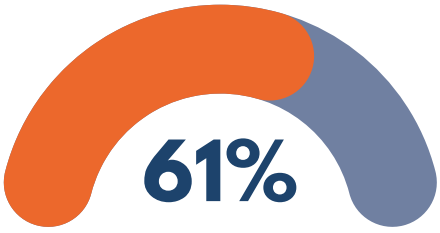
naturally widen the attack surface for actively participating economies. Further to this, Nigeria continues to evolve into a regional technology hub with the new-found attraction to technology competency by its youth-heavy demography, heightened by the availability and penetration of fashionable and trendy advanced technology (such as Artificial Intelligence). These opportunity factors are accompanied by the risk of the international connectedness of cyber criminals enabled by the same advanced tools for automated attacks, seeking to exploit vulnerabilities in digital infrastructure within developing economies. Regulators continue to implement legal frameworks and capacity development measures to address this risk. Relevant authorities are working on notable measures such as the development of a National Artificial Intelligence Strategy (NAIS), ongoing collaboration with global institutions on cybersecurity frameworks to secure critical infrastructure, protect data and build digital trust. The Nigerian technology penetration also presents an upside risk opportunity for individual innovators and corporates that are willing and able to deploy situation-specific technology solutions that can mitigate other risk issues. Examples include agric-technology solutions to boost food sufficiency; start-up innovation capabilities to employ a bustling youth population; and corporate and personal security solutions to build resilience against security incidents.

Recommendations

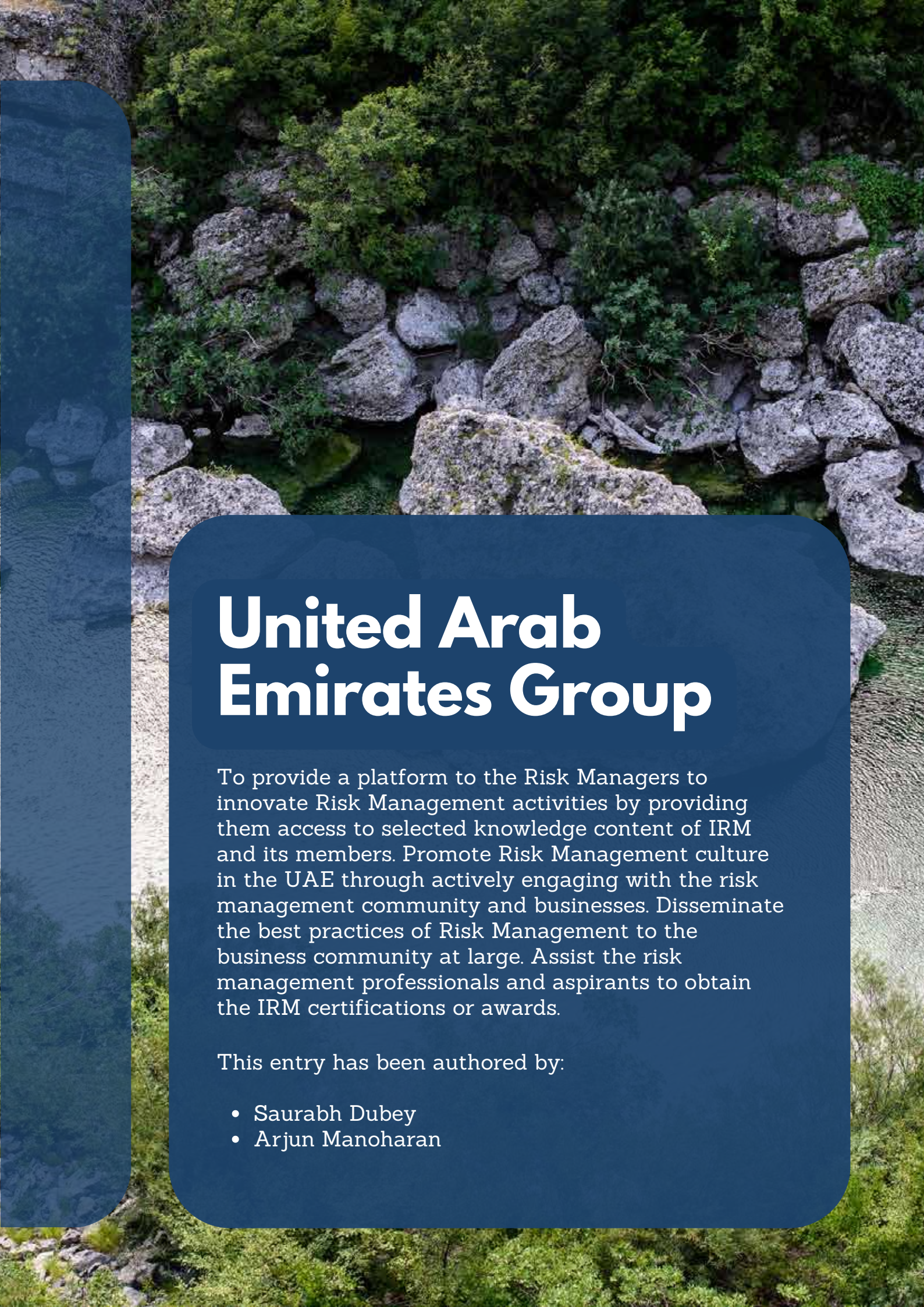
- Consider risk holistically from three perspectives - risk that hinders key objectives; risk emanating from other chosen risk response strategies; and risk that the strategy may not align with the overarching mission and vision.
- Consider risk-reward and upsides by innovating around strength and opportunity areas to create new solutions that can reduce existing risks while enhancing the innovator's commercial value
- Deepen risk resilience capability by moving beyond response and recovery mindset into embedded resilience that reduces actual incidents and guarantees inherent continuity
- Increase public and private sector collaboration in risk mitigation on industry and ecosystem matters
- Deepen stakeholder education and collaboration with regard to key risks and mitigations across the public and private sectors atthe industry and ecosystem levels
- Re-evaluate business models as part of planning processes in view of identified risks, mitigations, opportunities, and outlook.
- Diversify supply chains, consider regional and local supply options (where feasible), develop geopolitical risk mitigations, and strengthen international partnerships

Conclusion

Lessons from the Nigerian risk landscape in 2025 show that intentionally applied risk mitigation strategies consistently applied can produce favourable outcomes, but decisions must proactively consider all possible impact areas beyond those intended. The risk outlook into 2026 highlights a risk-reward trade-off where, in spite of the identified risk and mitigations, certain upside opportunities (for example in technology) remain available to governments and corporate who can provide risk mitigation solutions.



identified cyber risks as requiring the most investment and effort in 2025, with most expecting this increase in 2026.



United Arab Emirates Group

To provide a platform to the Risk Managers to innovate Risk Management activities by providing them access to selected knowledge content of IRM and its members. Promote Risk Management culture in the UAE through actively engaging with the risk management community and businesses. Disseminate the best practices of Risk Management to the business community at large. Assist the risk management professionals and aspirants to obtain the IRM certifications or awards.

This entry has been authored by:

- Saurabh Dubey
- Arjun Manoharan

The New Architecture of Risk

INTEGRATING CYBER, AI, GEOPOLITICS, AND GOVERNANCE IN 2026

For organisations in the UAE, one of the world's most globally connected hubs for trade, finance, energy, logistics, and technology, this complexity is magnified. Openness, speed, and scale drive growth and simultaneously amplify exposure to global shifts in geopolitics, technology, regulation, and economic volatility.

The World Economic Forum's Global Cybersecurity Outlook 2026 highlights a particularly challenging dimension of this environment: the convergence of AI acceleration, geopolitical fragmentation, and cyber-enabled fraud as defining forces reshaping global risk landscapes.

Why the 2026 Risk Environment is Fundamentally Different

Today's risk landscape has three defining characteristics:

1. Acceleration and Amplification: Global forces such as AI innovation and geopolitical tensions are accelerating risk vectors and compounding impacts, making outcomes more volatile and less predictable.
2. Interdependency of Risk Domains: Cyber risk, economic stress, regulatory change, and geopolitical volatility no longer operate in isolation; they interact and cascade, influencing operational resilience, strategic decisions, and stakeholder trust.
3. Blurring of Strategic and Operational Risk: Cyber and technology risks, far from being "IT issues," are now strategic risks that affect national resilience, economic stability, brand trust, and competitive positioning.

For boards, this means shifting from a controls mindset to a resilience and foresight mindset, orienting governance around strategic uncertainty and adaptive capacity.

1. Cyber Risk, AI, and Fraud: Strategic Threats to Trust and Resilience

A New Cyber Reality

The WEF's Global Cybersecurity Outlook 2026 significantly highlighted that cyber-enabled fraud has eclipsed ransomware as the top concern for CEOs, reflecting how pervasive and damaging fraud and social-engineering attacks have become globally. Key global cyber trends include:

- AI as a risk multiplier: 94% of leaders see AI as the most influential force shaping cybersecurity in 2026. AI is both a defensive tool and a mechanism attackers employ to automate and scale attacks.
- Cyber-enabled fraud as a top global threat: CEOs now rate fraud and phishing ahead of ransomware—signaling a shift in how risk is experienced and prioritised.
- Geopolitics embedded in cyber threat strategies: Over 60% of organisations account for geopolitically motivated cyberattacks in their strategies—highlighting a direct link between geopolitical tensions and digital risk posture.

These realities matter especially to UAE boards, given the UAE's rapid digital transformation, high adoption of cloud and AI technologies, strong integration with global supply chains, and its role as a strategic gateway linking East and West.

Board-Level Considerations

- Risk governance beyond IT: Cyber risk must be described in terms of business impact: service continuity, market trust, regulatory exposure, and reputational resilience.
- AI governance and risk frameworks: Boards should ensure that AI deployment, across automation, customer-facing systems, and decision engines, is governed with specific risk metrics and oversight, not assumed safe by default.
- Fraud resilience as a strategic priority: Fraud is not just a compliance risk; it degrades trust, affects customers directly, and can undermine economic stability. Executive leadership must drive fraud-specific prevention and response planning.

2. Economic Volatility and Strategic Stress Testing

Despite strong growth trajectories in many regions, uncertainty remains high. Global projections show growth sustained by concentrated drivers like AI investment, but downside risks related to geopolitical tension, trade barriers, and policy change persist.

For boards, economic volatility should be evaluated not as an external forecast, but as a stress test of strategy, capital allocation, and risk appetite. Key Board Questions:

- Are downside scenarios integrated into strategic planning and capital allocation?
- Are liquidity, cost discipline, and portfolio resilience assessed under stress scenarios?
- Does risk appetite link directly to financial thresholds, investment discipline, and risk capital assessments?

In the UAE context, where sovereign wealth, diversified growth strategies, and international partnerships are core to economic performance, the ability to manage macro volatility is not a theoretical exercise. It is central to sustaining institutional credibility and strategic optionality.

3. Regulatory Complexity and Governance Maturity

The UAE's regulatory environment continues to evolve rapidly across AI governance, data protection, ESG standards, financial crime controls, and corporate governance. Regulatory modernisation, such as adjustments in foreign ownership, shareholder protections, and digital economy laws, offers opportunity and complexity alike.

To govern effectively at this pace, boards must:

- Treat regulatory change as a strategic risk driver, not a compliance backlog.
- Anticipate policy shifts across markets, especially as global regulators increasingly focus on AI, cyber resilience, and fraud.
- Ensure governance models incorporate risk foresight capabilities tied directly to strategy execution.

Regulatory clarity in the UAE enhances investor confidence but only if governance and risk frameworks are agile, forward-looking, and anticipatory.

4. Geopolitical Risk: Strategic Exposures and Opportunity Costs

Geopolitical fragmentation is a top global risk driver in 2026, not just for macroeconomic projections, but for cybersecurity, supply chains, and cross-border cooperation. According to the WEF's risk insights, geopolitical volatility now directly shapes cybersecurity approaches and readiness.

For boards:

- Geopolitical scenarios must be part of strategy, not considered "externalities."
- Supply chains should be evaluated not just for cost and efficiency, but for fragility and geopolitical exposure.
- Technologies and operations should be stress tested for geopolitical shock scenarios, including sanctions, trade disputes, and hybrid digital threats.

The UAE's position at the crossroads of global trade and diplomacy means exposure is inevitable, but so too are opportunities to lead in multilateral risk governance, standards coordination, and systemic resilience initiatives.

5. Operational Resilience: Beyond Continuity to Strategic Stability

Operational resilience expectations are rising globally. Regulators and stakeholders now expect organisations to demonstrate that critical business services can continue within agreed tolerances even during severe disruption. Key elements of resilience include:

- Clear identification and prioritisation of critical services
- Impact tolerances mapped to business outcomes and customer expectations
- Assigned executive accountability and scenario-tested recovery plans

Boards must ensure that resilience is integrated into strategy, not siloed within operations.

What 2026 Demands of Leadership

Risk is now inseparable from strategy. In 2026, risk management must:

- Embed cyber resilience, AI governance, and fraud preparedness into strategic planning
- Treat geopolitical volatility as a core strategic consideration
- Align economic scenarios with governance and risk appetite
- Drive cross-stakeholder collaboration internally and across sectors

For the UAE, these dimensions intersect with national priorities, digital leadership, economic diversification, and global connectivity.

In this environment, boards and executive teams must evolve from risk responders to strategic risk stewards, not just preserving value, but actively shaping organisational resilience, trust, and long-term competitive advantage.

Resilience

MOVING BEYOND CONTINGENCY PLANNING

Introduction

The Charity Special Interest Group, drawing on member insights and sector research, has identified five key risks, against the backdrop of geopolitical change, shaping the charity sector's landscape. For the charitable sector, the changes in the global landscape are not distant headlines, they are the drivers of key risks: financial volatility and public financial concerns, supply chain risks, and cyber security threats. Charities are moving beyond contingency planning to organisational resilience assessment. The risk landscape facing charities in 2026 is characterised by increasingly interconnected and compounding pressures, where financial, technological, workforce and regulatory risks interact to create systemic challenges that cannot be managed in isolation.

Financial volatility and decline in public giving

The UK's economic landscape remains turbulent. Households are still grappling with high energy bills and grocery bills. These pressures have significantly impacted the public's ability to donate to charitable causes. According to the Charities Aid Foundation's UK Giving Report 2025, only 50% of the UK population donated to charity in 2024, the lowest level recorded since this metric was tracked. The report highlights a particularly pronounced decline among younger adults, with participation among 16-24 years olds falling by one third since 2017. contributing, a drop of one-third since 2017. [UK Giving Report 2025 | CAF]

Charities are contending with rising operational costs, driven in part by increases in the National Living Wage. These pressures are forcing difficult strategic and operational conversations, including decisions about strategic delivery, service reduction or closure, and the maintenance of staff and volunteer morale amid ongoing uncertainty.

In response, charities are developing mitigation strategies, including financial scenario analysis and stress testing, prioritisation of core services and streamlined delivery models, and the diversification of income through corporate partnerships and social enterprise approaches.

Risk practitioners can support financial decision-making and organisational resilience by embedding risk-based approaches within budgeting, forecasting and strategic planning processes.

Charities Group

The IRM Charities Special Interest Group was established to provide practical guidance about managing risk and opportunities by sharing knowledge, tips and best practice amongst sector professionals.

Our aim is to increase the sector's knowledge of risk management best practice, to explore practical solutions for managing sector challenges (such as new regulation requirements), and provide opportunities for risk professionals to learn from one another and share up to date risk management practice.

This entry has been authored by:

- Kathryn Jackson

Technology Gaps and the AI adoption

Rapid technological advancement, particularly in artificial intelligence (AI), is reshaping how charities operate. The 2025 Charity Digital Skills Report indicates that 76% of charities are now using AI tools in some capacity, up from 57% the previous year. However, only 25% report using AI strategically, highlighting a potential gap between experimentation and organisational focus. [Charity-Digital-Skills-Report-2025.pdf]

For charities, AI adoption presents both significant opportunities and risks. Structural constraints such as ageing digital infrastructure, limited IT budgets and a lack of in-house technical expertise, mean many organisations may struggle to realise the full benefits of new technologies. At the same time, AI and automation offer clear potential to improve operational efficiency, generate better insights and enhance service delivery. Charities that underinvest in, or delay, AI adoption risk losing effectiveness and missing opportunities for innovation. This may lead to inequalities across the charitable sector, with larger charities being able to progress more rapidly, while smaller organisations fall behind due to funding and capability constraints.

AI adoption must also be accompanied by appropriate investment in cyber and information security maturity. Without this, increased digitalisation may heighten exposure to cyber incidents, including data breaches. Developing an effective security culture requires robust technical controls, such as multi-factor authentication as well as a developed workforce understanding of data risks. This involves training staff and volunteers to recognise phishing and other social-engineering attacks.

With one in three charities experiencing a cyber incident in the past year, cyber risk and reporting should be an item on every charity's risk register. To strengthen digital resilience, charities may also draw on external expertise, through volunteer IT specialists on boards particularly where in-house capability is limited.

A single high-profile cyber incident has the potential to cause lasting reputational damage and impose substantial recovery and remediation costs, underlining the importance of proactive risk management in this area.

Challenges with recruitment and retention

Charities rely on people, staff and volunteers to achieve their mission. Risk professionals believe that 2026 will continue to see recruitment and retention challenges, especially for roles requiring specialised skills such as technology. Recruitment and retention in the charitable sector have become increasingly difficult due to competition from the private sector, where salaries are often more attractive. A combination of workforce burnout, competition from other sectors, and limited training investment has created a capability gap that threatens charitable delivery.

Candidates with specialist skills may have a connection to cause, but higher private sector salaries may prevent them from working with charities. Combined with financial challenges, charity training budgets may suffer. The NCVO reports a "serious skills shortage, compounded by reduced investment in training" across the sector. [The Road Ahead 2025: NCVO pg 19 ncvo_theroadahead_a4_5jd_3.pdf]

If charities are not able to hire specialists skilled workers, it will impact the delivery of key objectives as innovation slows down. It may also result in a reactive or firefighting culture which impacts staff morale and leads to burnout.

To close this gap, charities must treat talent and skills management and recruitment as a strategic priority. Charities may not be able to compete with private sector salaries, but they are able to prioritise other benefits such as flexible working, enhanced leave options as well as strengthening the connection to cause. To close training gaps, charities can invest in professional development opportunities such as mentoring, coaching, and secondments as well as looking at developing skills based opportunities for greater flexibility.

Clear progression pathways and opportunities to develop skills can satisfy growth needs. Charities can also build positive, inclusive work cultures to significantly improve retention; employees who feel valued are more likely to stay if they have a voice in decisions that affect their work.

Risk managers should ensure that people and skills related risks are integrated into organisational risk registers and addressed through strategic workforce planning.

Volunteer Workforce: Demographic shifts and engagement challenges

Workforce and volunteer risks are interconnected. Recruitment and retention challenges within the paid workforce are driving a reliance on volunteers, while a decreasing volunteer figure is intensifying pressure on staff, increasing the risk of burnout, service disruption and reduced organisational resilience. Volunteers remain integral to the charity sector, providing essential capacity across a wide range of activities, from frontline service delivery in charity retail to fundraising and community engagement. However, many charities are experiencing both a decline in volunteer numbers and a shift in who is volunteering, creating risks to delivery models that depend heavily on voluntary support.

These changes are being driven by several factors: an ageing volunteer base, with many older volunteers not returning following the pandemic, ongoing economic pressures that limit the time and resources individuals can commit to volunteering, and evolving expectations among younger volunteers, who increasingly seek flexible, or virtual opportunities. The impact of this change is felt through the reduced service delivery, where activities may need to be scaled back or given to paid staff which leads to an increase staff workload and costs. Another risk is reduced community involvement. Volunteers are key links to the community and a reduction in volunteers can result in charities becoming disconnected to the community and charitable purpose.

As a response to these changes, charities are creatively innovating their volunteer engagement strategies, providing flexible or micro volunteering and remote volunteering to fit into changing schedules, or allowing taster sessions, that let people explore volunteering before committing.

Regulatory change and compliance requirements

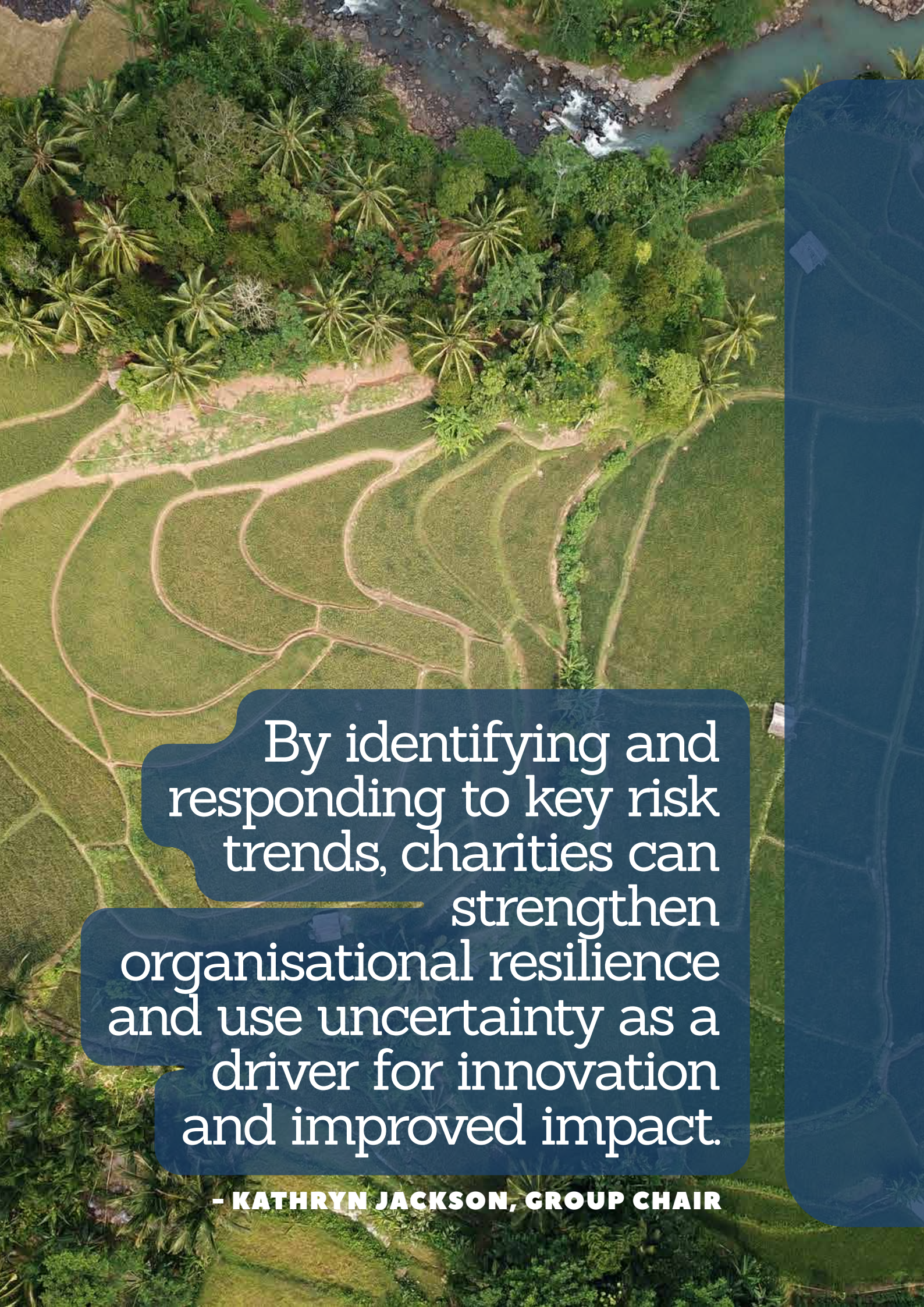
The regulatory environment for charities is becoming increasingly complex.

New requirements around data protection, safeguarding, fundraising practices, financial and sustainability reporting are placing additional demands on already stretched resources. Recent updates to the Fundraising Regulator's Code of Fundraising Practice, and changes to the Charities Act, the Statement of Recommended Practice (SORP), have all contributed to a heightened compliance burden. While these changes aim to improve transparency and public trust, they also require significant time, training, and investment to implement. The key risks to noncompliance are regulatory sanctions and reputational damage leading to funding loss. Regulatory changes increase administrative work, especially for smaller charities.

Supporting mitigations to these changes can be provided through proactive engagement with regulatory and sector bodies, external auditors, legal advisors and other professional group to horizon scan and prepare for changes in legislation and policy. Charities can also create cross team or cross sector working groups where clear ownership is assigned throughout the charity. Regulatory compliance should be a standing item on operational risk registers. Risk professionals should work closely with governance and legal teams to ensure that compliance is embedded into operational processes and that risks are proactively identified and managed.

Conclusion

By identifying and responding to key risk trends, charities can strengthen organisational resilience and use uncertainty as a driver for innovation and improved impact. Central to this is the role of risk professionals working closely with strategy colleagues to align risk, strategy and performance, embedding risk-informed decision-making across governance, planning and delivery. The IRM Charity Special Interest Group will continue to support risk professionals and charities by providing insight, professional guidance and a platform for sharing practical experience and best practice across the sector. Through collaboration and shared conversations, charities can navigate complex risk and continue to deliver against their objectives.



By identifying and responding to key risk trends, charities can strengthen organisational resilience and use uncertainty as a driver for innovation and improved impact.

– KATHRYN JACKSON, GROUP CHAIR

Temperature Check

CLIMATE RISK PREDICTIONS

Introduction

In 2025, the Climate Change Group reintroduced its Climate Change Matters (CCM) newsletter. The main objective is to provide a valuable resource for members in providing insights and updates from the world of climate change risk management.

The latest update outlined an event we held in London that is particularly relevant to managing and mitigating emerging risks, the design of a robust stress and scenario testing framework to cover the whole breadth of physical, transition, and liability risks. Many regulate such as the Bank of England, provide guidance on the developing climate scenario analysis, and a whole chapter is set out in the new Supervisory Statement SS5/25 that was recently published in December 2025.

The World Economic Forum (WEF) has just issued its 2026 global risk report, the 21st edition of this annual report, which marks the second half of a turbulent decade. The report analyses global risks through three timeframes to support decision-makers in balancing current crises and longer-term priorities.

Although environmental risks have decreased in importance in the short-term with a reprioritization towards geoeconomic and societal shocks, in the next 10 years, environmental risks have retained their ranking as the most severe risks, with extreme weather events identified as the top risk and half of the top 10 risks being environmental in nature.

The report states that “the downward reprioritization of environmental risks is unfolding in a geopolitical landscape shaped by growing multipolarity and protectionism”. They state that “while 2024 marked a record $2.1 trillion in low-carbon transition investments, growth in clean energy funding slowed compared to previous years”.

This is linked to the growing divergence between rising demand for energy on one hand, and climate change and associated social realities on the other, which could come to a head in the coming years.

Climate Change Group

The group focuses on identifying and sharing best practices in climate change risk management. It brings together cross-sector expertise to support IRM's strategic objectives, including membership growth and member education, through monthly committee meetings and three to four events each year.

This entry has been authored by:

- Martin Massey, Group Chair

Contributions from:

- Bogdan Pletea
- Jerry Flechais
- AbuJahed Ahad
- Luke Watts
- Christine Page
- Bob Tyley
- Rose Chemutai

Climate Risk Predictions

Organisations continue to take positive steps to meet regulatory and business requirements and embed climate change into their enterprise risk management frameworks and business processes.

The Group committee has set out six main macro risk themes that risk managers should focus on in 2026, in the context of managing and mitigating risks in their business. Some of the major climate risk trends included in the seminars we conducted in 2025, which we expand on in this year's risk trends report. It is important to note that there are a number of ongoing emerging climate risks that we have covered in previous years' reports, including an increase in flash floods and failure to meet climate emissions targets.

Physical Risks

There is a range of new and evolving climate-related physical risks for organisations to manage and mitigate, and we set out three key areas of focus for 2026. For example, in 2025, there was a major prolonged heatwave across Europe as well as across India and Pakistan, where temperatures reached 48 °C. Many of the emerging risks are interconnected, which is why climate change physical risk assessment is so complex.

1. Physical Risks – Increasing insurance protection gaps
2. Heatwaves as an escalating risk to health
3. Nature neglect is an emerging climate risk multiplier

Physical Risks – Increasing Insurance Protection Gaps

Introduction/ Definition

The insurance protection gap generally refers to the difference between insured and uninsured losses. The insurance protection gap for climate change-related (especially natural catastrophe) losses has been increasing and is expected to grow.

A greater protection gap lowers the financial ability of economies to bounce back from disasters, as a lack of insurance makes recovery harder for businesses and people.

Understanding Insurance Projection Gap as a Risk

In Swiss Re's report in 2025 entitled "How big is the protection gap from natural catastrophes where you are?", they state that in 2024, according to their latest Sigma report, that 43 %, or USD 137 billion, of global economic losses of USD 318 billion were insured.

Some of the most uninsured climate-related perils include floods with increasing flash floods; wildfires, often labelled a secondary peril and severe convention hurricanes, tropical cyclones, drought, and heatwaves. For example, according to Munich R it is estimated that 50 % of wildfires in Europe are uninsured, and as total economic losses are rising, that means the protection gap is rising.

One of the best recent reports written on the subject last year was from Howden's climate risk and resilience unit entitled "The insurability imperative". They state that "For many, the risk of becoming uninsurable looms larger and more immediately than physical climate threats themselves.".
From an insurer's perspective, increasing volatility and variability of climate change make it more difficult to model future weather patterns and price risks appropriately.

This leads to an increase in conservative pricing or changes in the coverage and growing exclusions in coverage being provided, or both. In more vulnerable places or the more complex risks, these may become prohibitive for consumers and corporates. Some locations already struggle to afford flood insurance cover, such as US Gulf states and South Florida. On a positive note, the insurance industry is developing innovative alternative risk transfer solutions including:

- Public-private reinsurance and pooled schemes such as Flood Re;
- Catastrophe bonds (Cat bonds) and insurance-linked securities;
- Parametric insurance and
- Microinsurance.

New types of parametric insurance for example, can also cover losses from non-damage physical risks that are often associated with climate change events, such as droughts and heat stress, which can support increased financial resilience to organisations, for example, credit defaults or increased cost of working.

Relevance for Risk Managers
Risk managers must consider the increasing likelihood of physical climate-related events across their risk profile and integrate them within their risk planning, focusing on infrastructure upgrades, disaster preparedness, and comprehensive insurance solutions.

It is important to map climate-related risks and review existing insurance coverage within their policies. One of the best and most advanced risk management techniques is called "Strategic insurance risk gap analysis," in which organisations need to build out physical climate scenarios and undertake a mapping exercise against existing and alternate insurance coverage availability.

Heatwaves as an escalating risk to health

Introduction/Definition
Climate change is materially increasing the frequency, severity, and duration of heatwaves, while simultaneously elevating drought and wildfire risk that increase the risk of infrastructure degradation.

Heatwaves have primary and secondary modes of impact on human health:

- Primary: heat stroke and dehydration, leading to increase in accidents, cardio-vascular and respiratory diseases;
- Secondary: exposure to UV radiation and air pollution leading to increase in cancer risk; increase; increase in vector-borne diseases (malaria, dengue, Lyme)

Understanding Heat Stress to Health as a Risk
Intense heatwaves can laed to thousands of excess deaths. For example, the heatwave in 2003 in France led to 15,000 excessive deaths with risks increasing for those in top-floor, non-air-conditioned apartments. The most vulnerable populations, especially those over 65, are at the highest risk for severe health issues or death.

Climate change intensified Europe's summer heat in 2025 and drove an estimated 16,500 additional deaths across 854 cities, according to a recent study led by researchers from the London School of Hygiene & Tropical Medicine (LSHTM) and Imperial College London.

Dr Garyfallos Konstantinoudis, Lecturer at the Grantham Institute – Climate Change and the Environment, Imperial College London and study co-author, said: "Heatwaves are silent killers. The vast majority of heat deaths happen in homes and hospitals, where people with existing health conditions are pushed to their limit, but heat is rarely mentioned on death certificates."

Health systems experience surge demand at the same time as staff shortages, power instability and degraded facility performance. These dynamics increase operational risk, particularly for organisations reliant on frontline workers, just-in-time staffing models or climate-exposed labour forces. For employers and service providers, extreme heat presents a material workforce continuity risk, increasing absenteeism, reducing productivity, limiting outdoor and manual work, and heightening occupational health and safety liabilities.

Relevance for Risk Managers

In respect to risk assessment and modelling of exposures it is difficult to make accurate predictions. However, it is important to consider future climate scenarios to use as a basis to stress test the potential impacts that are important to certain sectors such as life insurers to assess the possible impacts to help build future resilience, to changes both mortality and mobility.

Risk management plans should be developed in conjunction with OSH colleagues and centered on frontline workers. Heat plans should be primarily focussed on acclimatisation based on an understanding exposure. Cool environments and access to water are crucial, as are breaks and access to sanitation, especially for female workers.

Nature neglect is an emerging climate risk multiplier

Definition

The growing urgency of biodiversity loss and ecosystem degradation presents a critical risk for organisations and their risk managers. Nature-related issues are not only environmental concerns but also create significant physical and transition risks for asset portfolios. The transition to a lower-carbon, nature-focused economy can expose organisations to operational, financial, and reputational risks if nature is overlooked in climate strategies.

Understanding overlooked Nature risks and their Financial Implications

Biodiversity loss remains an urgent crisis. As of 2025, over 55 % of global GDP (≈$58 trillion) is moderately or highly dependent on nature, with nature-positive transitions offering up to $10 trillion in annual business value and 395 million jobs by 2030 (PwC, WEF 2025).

Nearly 75 % of terrestrial and 66 % of marine environments are degraded by human activity (WEF 2025).

The 2024 WWF Living Planet Report found a 73 % decline in monitored wildlife populations since 1970, with freshwater populations down 85 %.

Over 48,600 species (28 % of those assessed) are threatened with extinction (IUCN 2025). These trends have direct financial implications for organisations, increasing exposure to regulatory penalties, litigation, and stakeholder scrutiny.

Regulatory and Legal Pressures

Recent regulatory developments, particularly in Europe, are reshaping the risk environment. The EU's Corporate Sustainability Reporting Directive (CSRD) was updated in 2025, delaying some requirements but maintaining strict disclosure on nature-related risks. Typical nature categorisation includes"

- Biodiversity and Land use
- Water Stress
- Raw material sourcing
- Toxic emissions and waste

In parallel, the Taskforce on Nature-related Financial Disclosures (TNFD) has emerged as a leading global framework for assessing and reporting nature-related risks and opportunities. Its recommendations are increasingly referenced by regulators and integrated into sustainability standards, including alignment with the ISSB and EU reporting requirements.

These frameworks mean that risk managers must now integrate nature-related risks into their assessments and ensure compliance with evolving legal standards. From including strategic risks that can have reputational/brand damage from for example negative publicity and consumer boycotts. Asset owners and organisations face reputational risks if they fail to align with robust biodiversity safeguards. Nature loss can disrupt supply chains, increase operational costs, and trigger insurance claims.

Climate Change Risk Management in numbers

30% indicated that the integration of climate risk management across different departments/functions was the biggest challenge in 2025.

67% identified the increased use of AI as the greatest emerging risk in 2025.

80% said the development of new data centres to power AI software will be the biggest risk over the next 5 years

12% said 'Climate and sustainability risk expertise' will be critical for developing their organisation's risk management capabilities over the next 5 years

Which aspect of climate change or environmental transition poses the most significant risk to your organisation?

Physical risks (e.g., extreme weather, natural disasters)
25%

Transition risks (e.g., regulatory or policy changes)
19%

Increased operational costs from sustainability requirements
12%

Supply chain disruptions linked to environmental events
9%

Reputational risk due to environmental performance
9%

Shifting customer or market expectations around ESG performance
6%

Inadequate internal capacity for climate risk assessment
4%

Uncertainty in carbon pricing and disclosure requirements
2%

Investor or stakeholder pressure for decarbonisation
2%

Relevance and actions for Risk Managers

As with any other types of risk it is important to develop a robust risk identification and assessment process that is often supplemented through the design of qualitative scenarios to build out a nature capital across the risk profile of the organsation. Risk managers should specifically seek to assess dependencies on natural capital and develop contingency plans for ecosystem-related disruptions

To address these challenges, several key actions are recommended for risk managers:

- Education: Build understanding of biodiversity and natural capital.
- Engagement: Actively engage with stakeholders and service providers.
- Monitoring: Track regulatory developments and nature-related risks.
- Strategy: Integrate nature protection into core risk management frameworks and investment strategies.
- Asset ownership: Both capital allocation and stewardship are necessary to make meaningful progress on nature and biodiversity.

Transition Risks

There are a range of new and evolving climate-related transition risk for organisation to manage and mitigate and we set out three key areas of focus for 2026. The global landscape of climate and sustainability is increasingly defined by a profound tension between advancing regulatory mandates and shifting political priorities that is a key emerging transition risk that we cover as part of our update.

1. Maladaptation Risk in Climate Response
2. Divergence between global regulatory and political sustainability requirements
3. Positive ways AI reduces the impact of climate change and how this can be applied in the workplace

Maladaptation Risk in Climate Response

Introduction/Definition

Maladaptation refers to an action or adjustment intended to respond to climate change or environmental stress that unintentionally increases vulnerability, exposure, or risk over the medium to long term rather than reducing it. In risk management terms, maladaptation represents a failure mode of otherwise well-intentioned controls, where short-term risk reduction is achieved at the expense of long-term resilience.

Understanding Maladaptation as a Risk

Climate adaptation is often framed as a technical or environmental challenge. In practice, maladaptation is a governance and decision-quality risk. It emerges when adaptation measures are designed to address immediate hazards, regulatory pressure, or public expectations without sufficient consideration of system behaviour over time.

The result is a solution that can performs well under current conditions but can degrade as climate stress intensifies or as assumptions embedded in the original decision no longer hold. There are many examples including for example retrofitting for higher temperatures using materials or designs that fail future energy – efficient or emissions standards. In rapidly urbanising regions with arid climates, climate response strategies often focus on improving liveability and resource security in the face of extreme heat and water scarcity. Large-scale urban greening programmes and expanded water supply infrastructure are common responses. However, maladaptation risk emerges when such responses create long-term dependency on resource-intensive systems. From a risk perspective, maladaptation typically arises from three patterns. First, climate hazards are treated as static rather than dynamic, leading to controls that lack flexibility. Second, decisions are optimised at the project or asset level rather than across interconnected systems such as water, energy, land use, and population growth.

Third, performance is measured in near-term outputs rather than lifecycle outcomes, masking the accumulation of future exposure. Maladaptation risks are particularly difficult to manage because they often sit beyond conventional risk horizons and organisational boundaries. They may not trigger immediate incidents or non-compliance, yet they steadily increase residual risk, operating cost, and dependency on continued intervention. In this sense, maladaptation is not a failure of execution but a failure of foresight.

Relevance for Risk Managers

For risk managers, maladaptation challenges traditional notions of mitigation effectiveness. Controls cannot be assessed solely on whether they reduce risk today; they must be tested against how they influence future exposure, optionality, and resilience. This requires adaptation decisions to be evaluated as risk trade-offs rather than definitive solutions. Effective management of maladaptation risk relies on several disciplines. These include lifecycle risk assessment, climate scenario testing, and explicit consideration of second- and third-order impacts. Risk managers must also play a governance role by ensuring that adaptation measures are revisited as conditions evolve, rather than treated as permanent fixes. Without this, organisations risk locking themselves into pathways that become increasingly costly, fragile, or politically difficult to reverse.

Divergence between global regulatory and political sustainability requirements

Definition

The global landscape of climate and sustainability is increasingly defined by a profound tension between advancing regulatory mandates and shifting political priorities. A primary driver of this divergence is jurisdictional fragmentation, where a "tug-of-war" persists between different levels of government. In the United States, for instance, a significant split has emerged between federal rollbacks and ambitious state-level actions, such as California's landmark disclosure laws. Similarly, the European Union is experiencing internal revisions, where political pressure to maintain industrial competitiveness has led to "Omnibus Packages" that simplify or reduce the scope of key directives like the CSRD and CSDDD, potentially exempting a vast majority of previously targeted companies. It is important to recognise that scaling back reporting requirements changes the compliance effort, not the underlying risk exposure.

Understanding the divergence as a Risk

Ongoing regulatory uncertainty is further exacerbated by a growing "green lash" or political backlash against environmental policies. In many regions, sustainability measures are being reframed as threats to energy affordability and national sovereignty, leading to the dilution of long-term climate goals.

This shift is accompanied by a move toward protectionism, where instruments like the Carbon Border Adjustment Mechanism (CBAM) are increasingly viewed through the lens of national security and trade friction rather than purely environmental cooperation. Consequently, many organizations are adopting a strategy of "green hushing"—deliberately downplaying their sustainability progress to avoid litigation or political targeting from both pro-climate and anti-ESG factions.

Relevance for Risk Managers

The management of risks arising from the divergence between global regulatory and political sustainability requirements requires a strategic approach that addresses jurisdictional fragmentation. Some of the regulatory changes that for example reduction in reporting requirements in effect sets a higher bar for boards and CROs as simplification reduces the checklist but increases accountability for how risks are actually managed.

A key mitigation involves establishing a multi-jurisdictional compliance matrix to track and map the most stringent requirements, such as California's disclosure laws and the EU's CSRD, against regional variations. By adopting a "highest common denominator" approach, organizations can maintain core operational standards while ensuring flexibility. Furthermore, decoupling operational strategies from volatile political cycles by aligning long-term investments with stable market forces, such as the declining cost of renewable energy, provides a safeguard against fluctuating national policies.

To address the increasing threat of litigation and "lawfare," organizations should implement robust internal controls focused on data integrity and strategic disclosure. This includes mandatory third-party assurance and rigorous internal audits of all sustainability-related data to defend against claims of greenwashing or breaches of fiduciary duty.

Moreover, shifting the governance of sustainability reporting from marketing departments to legal and compliance teams ensures that all public-facing climate commitments are thoroughly vetted. This legal-centric approach helps mitigate the risks associated with both aggressive transparency and the defensive "green hushing" trend. The specific risk dimensions analysed—regulatory, legal, operational, and strategic—demand distinct management actions. In terms of regulatory compliance, the primary control is the adoption of a "highest standard" global policy to avoid the costs of fragmented reporting. For legal and litigation risks, the focus is on rigorous data auditing and legal vetting of all disclosures. Operational and trade risks are best managed through advanced carbon accounting and increased supply chain transparency to mitigate the impact of protectionist policies. Finally, strategic and political risks should be addressed through regional diversification and the inclusion of scenario-based "political shift" clauses in long-term contracts to allow for renegotiation in the event of sudden regulatory rollbacks."

Positive ways AI reduces the impact of climate change and how this can be applied in the workplace

Introduction/Definition

Artificial Intelligence (AI) is reshaping how organizations understand, mitigate, and adapt to climate risks, while simultaneously introducing new environmental burdens through the energy and resource demands of digital infrastructure. Although there is a lot of negative media focus recently about the impact of AI data centres due to their fact that they are extremely energy intensive and use up a lot of water AI technological innovation can also lower emissions and climate risk by improving forecasting, optimizing systems, and enabling better decisions. This is a risk that has both threats and opportunities in the context of climate and we will focus our update this year in the positive ways AI can be used to the workplace.

Understanding the divergence as a Risk
Below is a list of positive ways in which organisation are using to reduce emissions:

Buildings and Facilities

- Smart HVAC optimization: Use AI-driven control (model predictive control or reinforcement learning) to adjust heating/cooling based on occupancy, weather forecasts, and tariff/carbon signals.
- Occupancy-aware lighting/ventilation: Computer vision or sensor fusion to automate lights and ventilation where and when needed.
- Predictive maintenance for energy equipment: Detect inefficiencies in chillers, boilers, air handlers, and motors before failures.

Energy Procurement and Demand Management

- Renewable forecasting and dispatch: Improve forecasts for on-site solar/wind to maximize self-consumption.

Logistics, Supply Chain, and Travel

- Route and load optimization: AI to minimize miles, idling, and empty runs for deliveries or internal logistics.
- Inventory and procurement optimization: Reduce overproduction, rush shipments, and waste via demand forecasting and supplier selection with embedded emissions criteria.
- Travel minimization and virtual collaboration quality: Use AI scheduling and meeting analytics to replace travel with high-quality virtual alternatives when impact is large and in-person value is limited.

Manufacturing and Operations

- Process control and energy optimization: AI models tune setpoints for ovens, kilns, reactors, and compressors to minimize energy while maintaining quality.
- Waste and yield improvement: Computer vision detects defects early, reducing rework and scrap.
- Leak detection (methane, refrigerants): Deploy vision/acoustic/spectral analytics to spot leaks early.
- Materials and lifecycle optimization: AI-supported design to select lower-carbon materials and extend product life.

Facilities Resilience and Risk

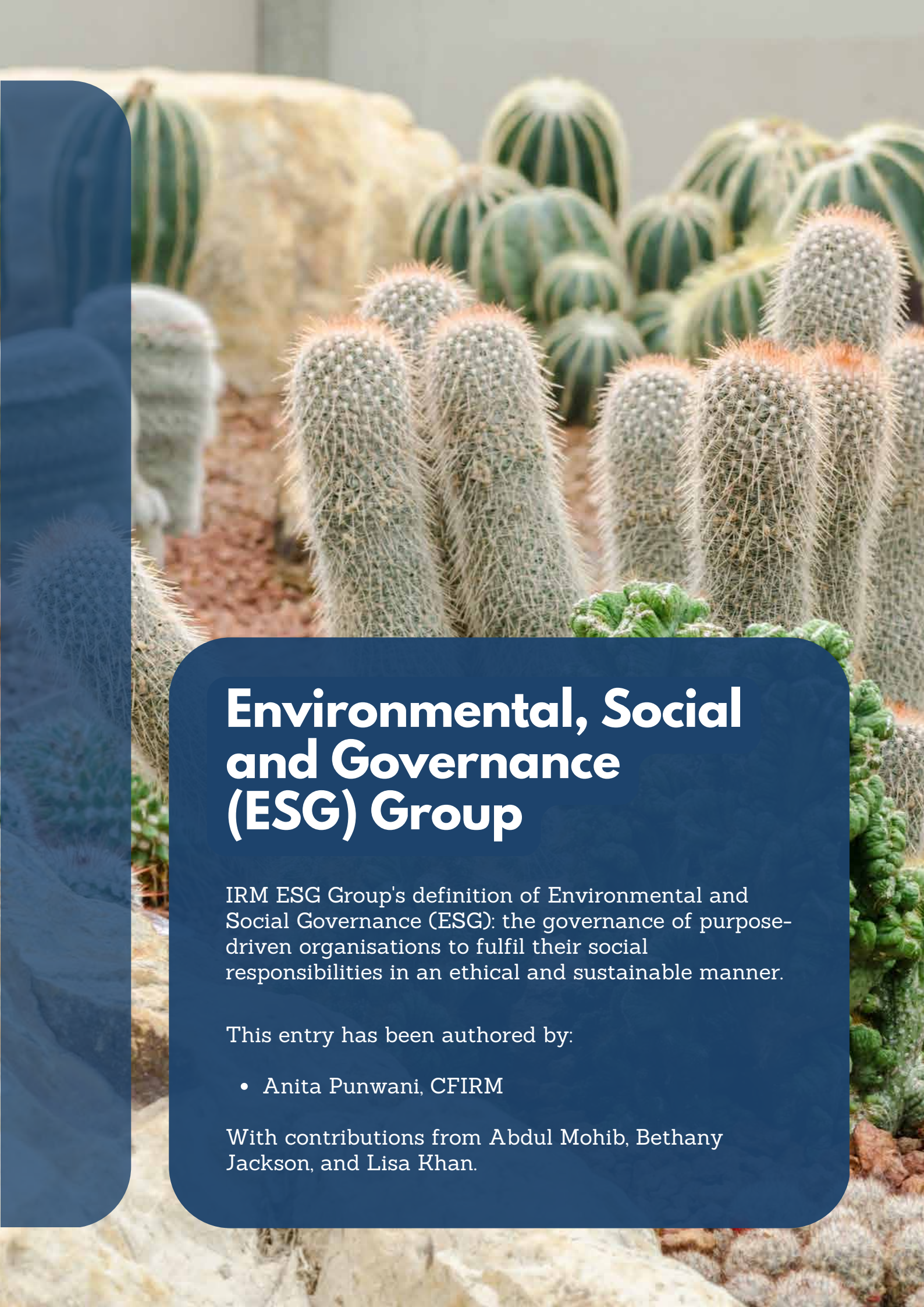
- Climate risk forecasting for continuity: Downscaled weather and flood/fire risk predictions to schedule operations, protect assets, and avoid high-emission emergency generation.

Product and Service Design

- Materials and lifecycle optimization: AI-supported design to select lower-carbon materials and extend product life.
- Application: Lifecycle assessment models in the design workflow; optimize for durability and repairability.
- Impact metrics: Embodied carbon per unit, service life extension, end-of-life recovery rate.

Relevance for Risk Managers
Risk managers should position AI as a key risk control and embed within their ERM Frameworks and align it with their carbon emissions management framework. From a governance perspective it will be increasing import to integrate AI into operational and IT risk frameworks. In terms of initial practical steps:

- Use AI when the use is justified and effective
- Train staff: In the efficient and correct use.
- Pilot, then scale: Test and fail fast.
- Keep within legal parameters



Environmental, Social and Governance (ESG) Group

IRM ESG Group's definition of Environmental and Social Governance (ESG): the governance of purpose-driven organisations to fulfil their social responsibilities in an ethical and sustainable manner.

This entry has been authored by:

- Anita Punwani, CFIRM

With contributions from Abdul Mohib, Bethany Jackson, and Lisa Khan.

Instability

ESG BLIND SPOTS

The instability of the last few years will continue to pose many risks to organisations in 2026; the risk professional will need to consider the full range of risks the organisation might face to support it in successfully managing risks as well as opportunities. The pressure for greater transparency and accountability to a range of stakeholders will continue in 2026, into 2027, and beyond, including in relation to managing risks to the environment and society, notably systemically excluded groups.

In 2026, ESG – or rather the letters 'E', 'S,' and 'G' – will continue to be a topic of much discussion; however, there is a widespread tendency to focus on E, S, and G separately instead of understanding the interconnected nature of environmental and social governance. In the commentary provided by StrategicRISK magazine when communicating the findings of its 'Global ESG Risk Survey', it was revealed that there are 'S' and 'G' 'Blind Spots' and it was stated that 'risk managers are currently more concerned with 'E' risks like physical climate risk than with 'S' and 'G' risks, despite the interconnected nature of all three'.

I contributed thought leadership in Environmental and Social Governance to support StrategicRISK communicate to risk professionals the need for intention to turn into action in relation to ESG and Enterprise Risk Management, including conveying that our focus on human rights, modern slavery and child labour in global supply chains did not rank high enough on board agenda; these issues remain relevant ones for the risk professional in 2026 and more details of my contribution to the full survey and article can be found here.

Modern slavery is a case in point; eradicating this global issue requires management of the risks that support this unethical, and often criminal, practice. In 2025, the IRM Environmental & Social Governance Group committee - together with Andrew Wallis OBE, Unseen, and Dr Bethany Jacks, Rights Lab, University of Nottingham - published thought leadership which set out why the conventional view of 'E', 'S' and 'G' is too simplistic a way of understanding the risks that organisations now face in relation to risk professionals addressing modern slavery in global supply chains, notably in the face of handling the climate crisis.

Risk professionals need to understand risks as varied as those arising from extreme weather events, withdrawal of funding, shifting immigration policies and fluctuating economic costs, notably insurance costs. Environmental issues will continue to present risks to many sectors. Social issues will continue to present risks to the workings of sectors highly dependent upon workers; therefore, risk professionals need to understand risks arising from inequality, lack of social inclusion, as well as anti-migrant sentiment in nations witnessing hostile political discourse in these respects.

The repercussions on nations in the Global South following the sudden withdrawal of international aid and assistance on the part of several powerful nations in the Global North will continue to have adverse social and economic effects and on the some of the most systemically excluded groups in the world - including on local programmes in Africa, at least in the short to medium term until these governments are able address the challenges through diplomatic and funding means; IRM's Environmental & Social Governance Group is leading the work of the institute in managing the risks posed to 'Women and Children' in 2026.

Technological progress will continue to generate opportunities in green and renewable technology and infrastructure, but at the same time, greater use of Artificial Intelligence presents risks to the environment for reasons related to energy usage, as well as in relation to job losses, notably with respect to lower socio-economic communities, all at a time of economic instability and a cost-of-living crisis. In an organisational context, the use of AI tools in supporting risks to be managed needs guidance with respect to the legitimate use of such technology. The pressure upon organisations to demonstrate greater transparency and accountability to a range of stakeholders will continue in 2026, not only in relation to managing risks related to the climate but also modern-day slavery, child labour and safeguarding, DEI, as well as a range of environmental risks.

Greater scrutiny in terms of ESG reporting is still characterised by a lack of standardisation, presenting a need for organisations to resource teams to comply with diverging global ESG standards. In this context, it is still apparent where organisations are excessively focused on compliance and reporting in 'E', 'S', and 'G'.

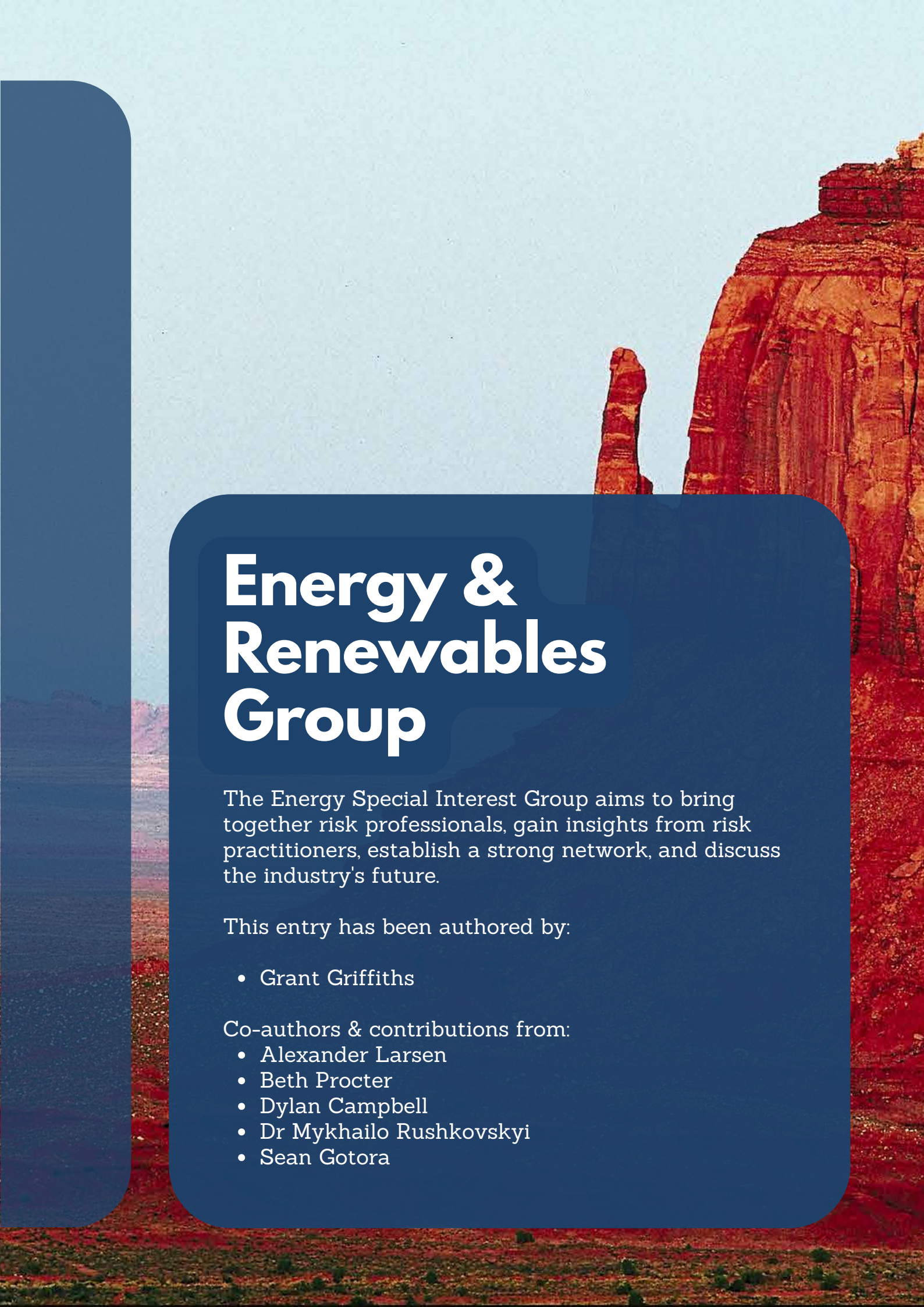
Although organisations have been making progress in their reporting, in part, driven by a desire to meet ever more pressing stakeholder requirements, the risk professional will need to support the organisation to ensure it has made the shift in thinking from a traditional mindset to one that reflects the needs of meeting the challenges and requirements of a wider range of stakeholders and society.

In this regard, risk professionals need to support organisations to be fully transparent and accountable in relation to their decision-making. In 2026, many boards will again be faced with competing priorities when considering and managing short-term versus long-term risks. Boards will face short-term pressures, including financial ones, and there is a danger that decisions might be made to address short-term pressures at the expense of proactively identifying, assessing, and addressing long-term threats and opportunities. The greatest challenges for organisations seeking to handle such risks lie in gaining deep and reliable visibility of supply chains, and also in relation to ICT in making difficult trade-off decisions, notably in relation to understanding the risks to systematically excluded groups.

The Environmental & Social Governance Group is focusing on 'Women and Children' in 2026 and collaborating with IRM's East Africa Group on the topic of the risks posed to children in sharing our respective knowledge and experience with the aim of raising awareness across the international risk community that child rights must be protected.

Risk professionals need to support organisations to be fully transparent and accountable in relation to their decision-making.

– ANITA PUNWANI, CFIRM



Energy & Renewables Group

The Energy Special Interest Group aims to bring together risk professionals, gain insights from risk practitioners, establish a strong network, and discuss the industry's future.

This entry has been authored by:

- Grant Griffiths

Co-authors & contributions from:

- Alexander Larsen
- Beth Procter
- Dylan Campbell
- Dr Mykhailo Rushkovskyi
- Sean Gotora

Power On

ENERGY RISK INSIGHTS

While 2025 was a year of re-assessment, adjustment and adapting to the ever-changing global risk landscape, we see 2026 as being an opportunity to consolidate – or at least it should be; the reality is likely to be different.

In many ways, 2025 was a year of missed opportunities for regulators and political leaders to step-up and provide strategic clarity and support on the current and future challenges facing the global community, and 2026 is unlikely to be much different.

The main drivers of energy risks in 2026 are:

- Geopolitics,
- Energy infrastructure challenges,
- NetZero / decarbonisation,
- Regulatory ambiguity,

and will contribute individually and collectively to the risk landscape.

- Geopolitics will continue to drive strategic alliances – and will also remain a top 3 concern. Ongoing conflicts such as the Russia–Ukraine War, renewed unrest in China-Taiwan, and new conflicts in The East Mediterranean and the USA-Venezuela situation reflect the deepening fragmentation of the geopolitical order and with it, continuing fractures of international relationships and established global energy frameworks.
- Oil prices – supply remains buoyant, providing a hedge against ongoing geopolitical and supply chain concerns.
- Grid infrastructure investment – advanced economies will need to commit to longer-term plans amid inflationary pressures on economic growth and long-term prosperity.
- Cyber and digital – concerns about both security and performance/resilience, especially in a world of realigning political alliances and rapid technological advancement.

Political pragmatism and regulatory clarity are needed to maintain balance and to build confidence among stakeholders. A severe dislocation event or events in financial markets have the potential to shake investor confidence, in turn creating greater and potentially more complex long-term risks for energy markets.

The IRM Energy & Renewables Special Interest Group will be continuing our thought leadership throughout 2026, with our ongoing series of Energy Risk Clinics, our topical publications and our global Energy Risk Leaders' Survey.

As we did throughout 2025 we will regular review and monitor these forecasts and provide regular feedback and commentary on the energy sector and events as they unfold.

Here are the 10 Risk Trends to watch in the Energy Sector for 2026

Trend 1: Deepening fragmentation of the geopolitical order

As we predicted in previous years, geopolitics will continue to influence policy and investment, driving risks for global energy.

Rival blocs and shifting alliances will continue fracturing international relationships and established global energy frameworks, with significant ramifications for both commodity prices and critical infrastructure costs. With concentrated supply chains (critical minerals, semiconductors, skilled labour) local conflicts or export curbs carry the potential for cascading globally through oil, gas, petrochemical and grid projects. For example, upheaval in the Gulf or a sanctions shock on rare earths, could interrupt refinery feedstock or power-plant schedules worldwide. Such polycrises also undermine coordinated climate action. Energy risk managers should consider embedding this fragmentation into scenario plans and dual-sourcing strategies, ensuring resilience across multiple governance regimes.

Trend 2: Muted Oil prices

Ongoing suppressed oil prices are likely to be the normal throughout 2026, while other commodities show resilience to adverse price movements. OPEC+ is projected to manage supply through cautious adjustments, while US policies are likely to dictate pricing, with an eye on inflation. Global oil inventories are anticipated to grow with the market expected to remain volatile. Some forecasts indicate prices could fall well below the levels oil companies expect; however, the risk of a serious geopolitical event such as a loss of Venezuelan oil production in case of a U.S. military intervention, could materially impact global benchmark prices, although as a counter to this scenario Venezuela's production capacity is not significant enough on its own to have amajor impact on prices. Expanding geopolitical risks will have to be balanced against persistently weak fundamentals.

Trend 3: Energy Shaping the U.S. – EU Relationship

July's landmark trade deal between the U.S. and EU to cut tariffs and boost economic ties included a major expansion of EU energy imports from the U.S. which are projected to reach $750 billion by 2028. The agreement promises strategic alignment and energy security but is non-binding and vulnerable to market forces; success of this landmark deal depends on commodity prices, investment, and political stability, with no enforcement provision if targets are not met. While continued cooperation is likely, risks remain: policy shifts, market disruptions, or accelerated EU decarbonisation could stall progress, eroding trust and exposing both sides to renewed trade tensions and energy vulnerabilities.

Trend 4: Electrification and the strain on aging grid infrastructure

Europe's growing population and rapid electrification driven by EVs, heat pumps, and industry demand are straining aging grids which have suffered from under-investment and a lack of consistent policy direction. Legacy systems lack the flexibility for decentralised generation, risking congestion and reliability issues in Transmission and Distribution networks.

Without timely upgrades, operational risks and outages will rise. Countries like the UK, Germany, and Ireland must align grid reform with electrification policy to avoid delays and systemic failures. Net-zero goals and retiring traditional generation add pressure, increasing the likelihood of prolonged outages. Strategic investment, clear infrastructure policy, and demand management are critical to ensure reliable power delivery.
Risks posed by both inflation and supply chain factors will further impact current projects and economics, presenting additional complexity for utilities investors, operators and regulators in their efforts to expand and enhance infrastructure.

Trend 5: Supply chain impacts on climate and energy transition

The global pivot to renewables faces headwinds from uneven technology readiness and divergent national policies. Some major economies are already resisting decarbonisation, aligning on fossil-fuel countermeasures and slowing transition commitments. Supply-chain chokepoints (such as lithium or polysilicon) could derail renewable projects, delaying decarbonisation and driving up costs. With climate diplomacy strained, energy risk managers must track COP outcomes, carbon tariffs and incentives closely. Shifting climate policies and trade rules may reshape the viability of projects and investment across the energy industry.

Trend 6: Regulatory & Geopolitical factors impacting the energy transition

The global shift to renewables faces hurdles from uneven technology readiness and policy divergence. Strains in climate diplomacy, often driven by domestic political imperatives, adds uncertainty to the equation requiring close monitoring of COP outcomes, carbon tariffs, and incentives. With several significant green investments in Africa moving to Final Investment Decision between 2026 and 2028 - and requiring competitive support from EU and Asian partners - risks such as resource-source dynamics and geopolitical weaponisation of critical minerals present significant downside risks to the progress towards meeting energy transition goals.

Trend 7: Technology-driven vulnerabilities and cyber risks

The energy sector's surge in digitalisation, from AI-driven grids to high-performance data centres, expands the attack surface for cyber warfare. A single software vulnerability or state-sponsored hack could cascade across generation assets, transmission & distribution networks, or oil & gas operations. For instance, a breach of an AI-driven pipeline control system or an outage at a hyperscale data centre could shut down refineries or grid segments overnight, highlighting the systemic vulnerability to such events. Additional vigilance and monitoring of the ever-changing and increasingly sophisticated digital space should remain a priority for all energy enterprises.

Trend 8: High Performance Computing (HPC) & Energy Grids

HPC data centres have presented both risks and opportunities to energy grids globally HPC demand is accelerating as AI data centres and Bitcoin-mining facilities expand, increasing grid pressure and energy intensity. Bitcoin mining consumes 173–240 TWh annually, while AI data centres are projected to consume 20% of global electricity by 2030, with usage surging through 2025.However, Bitcoin mining has been demonstrated to act as a "shock absorber" for energy grids. Miners can ramp up during energy surplus and shut down during peak demand, helping balance supply and demand. This flexibility allows utilities to integrate more HPC data centres have presented both risks and opportunities to energy grids globally. HPC demand is accelerating as AI data centres and Bitcoin-mining facilities expand, increasing grid pressure and energy intensity.Bitcoin mining consumes 173–240 TWh annually, while AI data centres are

projected to consume 20% of global electricity by 2030, with usage surging through 2025. However, Bitcoin mining has been demonstrated to act as a "shock absorber" for energy grids. Miners can ramp up during energy surplus and shut down during peak demand, helping balance supply and demand. This flexibility allows utilities to integrate more renewable energy without needing costly infrastructure upgrades. HPC operations are increasingly located near hydropower and solar sources, using energy that would otherwise go to waste. In regions like Malawi, Ethopia, Bhutan and the Columbia River Basin, Bitcoin mining has helped fund local development and support renewable energy projects.

HPC companies are becoming acutely aware of the risks they pose to grids and the need for them to be good environmental stewards, and we expect that they will trend toward managing these risks while continuing to leverage the opportunities.

One growing area of risk for HPC companies is a shortage of available energy capacity to meet growing demand for their services. To help address this, we expect these companies to vertically integrate energy generation into their businesses, clamour for power supply agreements with power utilities, and invest in research in micro-scale powerplants, for example, small modular nuclear reactors (SMRs).

Trend 9: UK Policy and Regulatory challenges to grid connections

In 2025, as part of the UK's Clean Power Action plan, a new energy grid gate-based "first-ready, first-connected" regulatory change was implemented to address a connections queue backlog of over 738 GW of capacity - far exceeding the 200 to 225 GW of clean generation capacity required by 2030. This grid reform is aimed at fast-tracking build-ready developments with speculative applications that would otherwise hold up more mature projects being sent to the back of the queue.

Compared to Germany's reactive congestion zones and Ireland's auction-linked access, the UK's grid reform directly targets the massive connection backlog through its structured prioritisation system.

However, all three countries face similar risks. Without coordinated upgrades to Transmission and Distribution networks and ongoing regulatory changes to support the implementation of these changes, progress may be slow. In addition, while the UK may seek to improve efficiency and grid stability, the stricter criteria could disadvantage smaller developers, stifle innovation and hinder investment, in turn becoming a systemic risk in meeting the government's own mandates.

Trend 10: Water-scarcity driven generation shortfall

Africa's power infrastructure faces critical climate risk due to heavy water dependence. Thermal plants need vast cooling water, while hydropower relies on steady flows. Heatwaves and droughts raise water temperatures, crippling thermal efficiency and forcing shutdowns, while reservoirs evaporate, slashing hydropower output. This "scissors effect" cuts supply as cooling demand spikes, triggering blackouts. Financial impacts may be severe; failure of one large plant can cost millions daily.

Utilities and investors must stress-test assets against climate models and evaluate a more resilient energy mix, potentially favouring water-independent energy technologies and sources such as solar and wind, supported by storage, as a means of reducing vulnerability and ensuring grid stability.

2025 was a year of missed opportunities for regulators and political leaders to step-up and provide strategic clarity and support on the current and future challenges facing the global community, and 2026 is unlikely to be much different.

– GRANT GRIFFITHS

Infrastructure Group

The Infrastructure Risk Special Interest Group is intended for individuals interested in all aspects of infrastructure risk as it relates to design, construction, management, funding, insurance, technology advances, and resilience.

This entry has been authored by:

- Yukitaka Matsuda, Chair, IRM Infrastructure Special Interest Group
- Wesley Cadby
- Dr Robert Chapman
- Cameron Burton

Four Outlooks

INFRASTRUCTURE IN THE UK

The Infrastructure SIG committee has identified emerging risk trends for 2026, with a primary focus on the UK infrastructure sector. This report draws on recent UK Government announcements and is structured into four sections: UK Infrastructure Outlook, UK Infrastructure Supply Chain Resilience and Capability Risks, Resilience of the UK's critical national infrastructure, and UK Rail Infrastructure Trends.

UK Infrastructure Outlook
by Yukitaka Matsuda

The UK Government has introduced the Planning and Infrastructure Bill 2025 to accelerate infrastructure delivery and stimulate economic growth. A pro-growth package, announced on 14 October, is designed to unlock the full potential of this landmark legislation—a key driver for reducing planning delays that have long constrained the UK economy. [1] [2] [3]

Budget 2025 reinforced this strategy with £120bn infrastructure investment, major transport upgrades, and an upgraded growth forecast to 1.5 %, positioning the UK as the second-fastest growing G7 economy.[4] At the time of writing this article, once enacted, this transformative Bill will amend several existing statutes, reshaping regulations across planning, housing, transport, energy, and environmental policy. It also introduces opportunities for the defence sector, with spending set to rise from 2.3 % of GDP to 3.5 % by 2035, aligning with NATO security commitments. The following paragraphs outline the key reforms and their implications.

Key Legislative Amendments

Planning Act 2008 (NSIP Regime)

Streamlines the consenting process for Nationally Significant Infrastructure Projects (NSIPs) by reducing pre-application requirements and limiting judicial review grounds. This accelerates delivery of critical infrastructure, energy grids, roads, water systems - supporting the Clean Power 2030 agenda.

Electricity Act 1989

Modernises grid connection processes and introduces community benefit schemes for areas hosting new transmission infrastructure. These changes aim to boost renewable energy deployment, enhance energy security, and advance decarbonisation targets. Budget 2025 complements this with investment in nuclear projects, including Small Modular Reactors (SMRs) and Sizewell C, to strengthen clean energy capacity.

Highways Act 1980 & Transport and Works Act 1992

Simplifies approval processes for road and rail projects and permits temporary land possession to support construction. Guidance will define possession limits and compensation terms, enabling faster delivery of transport networks, including EV infrastructure. Additional funding for local roads and city-region transport projects announced in Budget 2025 will accelerate these improvements.

Compulsory Purchase Act 1965

Removes "hope value" from compensation calculations, expediting land assembly for housing and infrastructure projects. This reform promotes predictability and supports regeneration and affordable housing delivery. Budget 2025 reinforces housing delivery with plans for 1.5 million homes and new towns.

New Towns Act 1981

Expands development corporations' powers to deliver new towns, urban extensions, and regeneration schemes, enabling large-scale housing and mixed-use development through strategic planning, infrastructure provision, and sustainability requirements.[5]

Senior Courts Act 1981

Replace the paper permission stage with oral hearings and limit appeals where permission is refused as "totally without merit." These changes aim to reduce litigation delays and provide greater certainty for developers.[6]

Nature Restoration Fund

Through a levy system, developers contribute to a central fund instead of site-specific mitigation. Natural England will use these funds for Environmental Delivery Plans (EDPs), starting with nutrient pollution. This coordinated approach streamlines development while delivering landscape-scale biodiversity recovery and broader environmental benefits.

The legislation creates significant opportunities for the UK infrastructure sector.

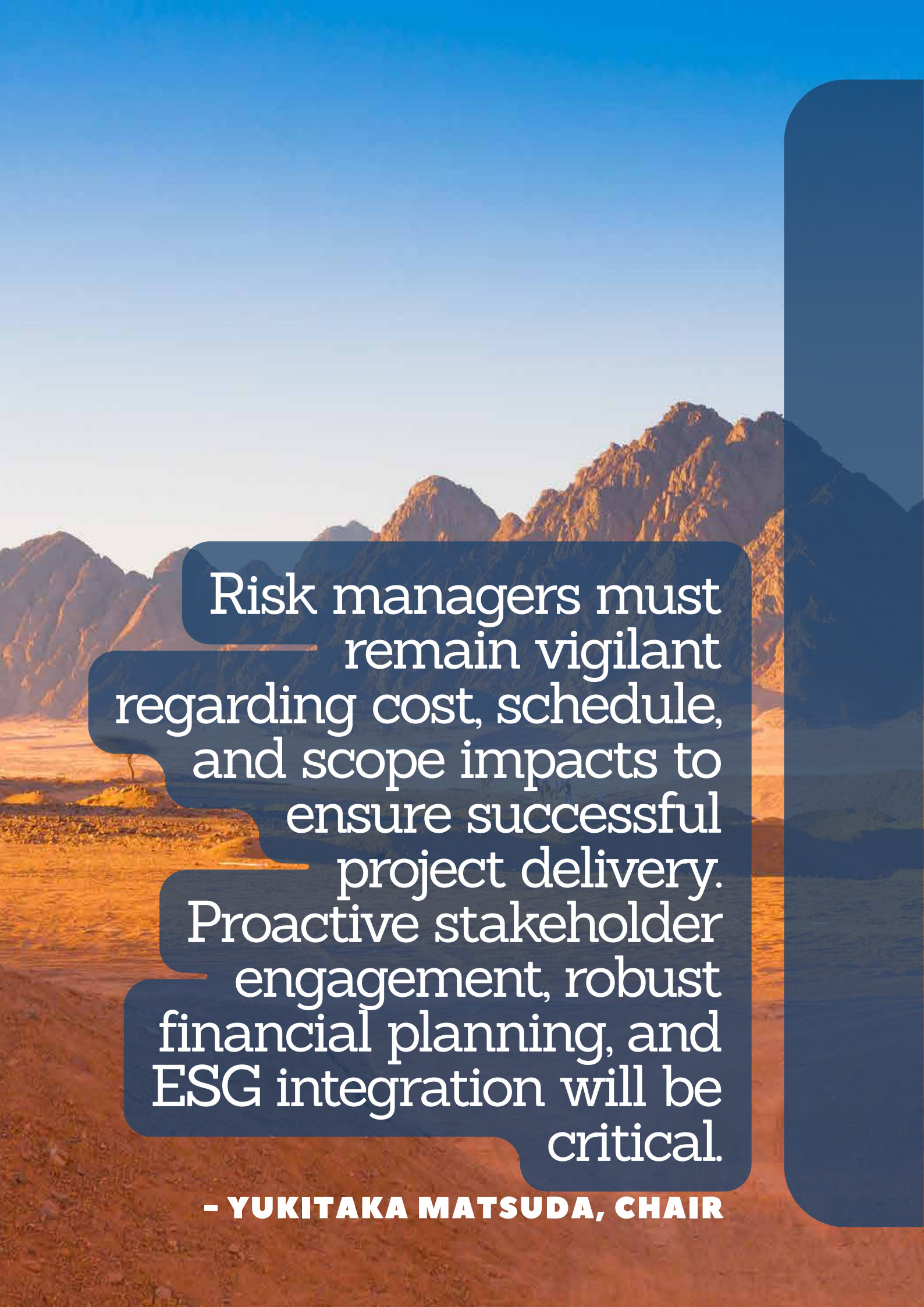
Combined with Budget 2025's record investment, accelerated delivery through streamlined approvals and reduced judicial delays would improve schedule certainty and mitigate time-related risks.

Access to capital is another major advantage, as increased public and private investment in energy grids, transport, and housing opens the door for innovative funding models and robust financial risk strategies. Furthermore, sustainability integration is strengthened by ESG-aligned measures such as the Nature Restoration Fund and prioritisation of clean energy, enabling risk managers to address environmental risks effectively while enhancing reputational value. Although the framework accelerates delivery, it may introduce risks that must be managed carefully. Regulatory and legal complexity remains a concern, as reduced appeal rights could trigger stakeholder backlash and reputational damage if challenges arise later in the process.

Cost escalation is another significant threat, with large-scale projects exposed to inflationary pressures and high upfront costs, increasing the likelihood of budget overruns and financial instability. Additionally, community and environmental pushback may intensify, as reduced local input and concerns over visual and ecological impacts could lead to objections and delays, particularly for energy and transport projects. Risk managers must remain vigilant regarding cost, schedule, and scope impacts to ensure successful project delivery. Proactive stakeholder engagement, robust financial planning, and ESG integration will be critical.

References:

[1] Planning and Infrastructure Bill - Bill 328 2024-26 (Lords Amendments)
[2] Guide to the Planning and Infrastructure Bill
[3] Pro-growth package unshackling Britain to get building
[4] Policy paper Budget 2025
[5] Planning and Infrastructure Bill concludes Lords report stage
[6] Lord Hunt of Kings Heath's amendment, After Clause 51



Risk managers must remain vigilant regarding cost, schedule, and scope impacts to ensure successful project delivery. Proactive stakeholder engagement, robust financial planning, and ESG integration will be critical.

– YUKITAKA MATSUDA, CHAIR

36% identified infrastructure risk as requiring the most investment when plugging skills gaps in their organisation.

UK Infrastructure: Supply Chain Resilience and Capability Risks

By Wes Cadby CFIRM

Introduction

The UK's infrastructure ambitions for 2026 are bold, but the reality is challenging. Supply chain fragility and uneven capability across delivery partners threaten to derail timelines and inflate costs. Global material shortages, price volatility, and skills gaps, particularly in engineering and project management, are no longer abstract risks; they are already impacting projects like HS2 and the EV charging rollout. Budget 2025 reinforces these ambitions with record capital investment and targeted skills programmes, but success will hinge on embedding resilience into supply chains and strengthening technical competencies at every tier.

The government's 10-Year Infrastructure Strategy and the Planning and Infrastructure Act signal a renewed commitment to fixing systemic delivery issues. Together, they pledge billions in funding and introduce reforms aimed at accelerating critical projects. Budget 2025 complements these measures with £120bn infrastructure investment and initiatives to boost workforce capability. Yet, these ambitions collide with a harsh reality: a supply chain under pressure from resource scarcity, rising costs, and fragmented capability. For risk managers, the question is clear, how do we turn these vulnerabilities into resilience before they compromise delivery?

Policy Context

- 10-Year Infrastructure Strategy (2025–2035): Annual investment of £9–10 billion for health, education, and justice estates; emphasis on clean energy, digital connectivity, and regional growth; drive to attract private investment and strengthen UK-based supply chains.
- Planning and Infrastructure Act (Oct 2025): Streamlined planning for major projects and clean energy infrastructure; mandatory training for planning committees and faster consenting processes; supports Clean Power 2030 and accelerates EV charging infrastructure rollout.
- Budget 2025 (Nov 2025): Introduces £120bn capital investment for transport, energy, and housing, plus targeted skills programmes to address engineering and project management shortages.

The Competency Challenge

Infrastructure delivery is no longer just about concrete and steel, it's about digital engineering, AI-driven asset management, and low-carbon construction. Yet, the sector faces:

- Shortages of skilled labour in sustainability and advanced technologies.
- Critical gaps in engineering and project management expertise create bottlenecks in planning and execution.
- Uneven capability across subcontractors, creating weak links in complex delivery chains.
- Pressure to meet net-zero targets, amplifying demand for "green skills."

59% see infrastructure risk in their organisation as a driver of performance and long-term value.

Supply Chain Fragility

Recent disruptions have exposed the vulnerability of UK infrastructure projects:

- Material scarcity, steel and aggregates remain volatile, with renewable components often sourced from overseas.
- Price inflation, global shocks and energy costs are driving up procurement budgets.
- Single-point dependencies, specialist equipment often relies on limited suppliers, increasing exposure to geopolitical risk.

Emerging Risk Drivers

- Digitalisation Risks: Cyber vulnerabilities in IoT-enabled infrastructure.
- Regulatory Complexity: ESG reporting and sustainability disclosure requirements.
- Climate Resilience: Extreme weather is disrupting logistics and construction schedules.

Mitigation Strategies

- Invest in Capability Building: Develop training pipelines for engineering, project management, and sustainability skills; partner with universities and industry bodies.
- Diversify Supply Chains: Reduce reliance on single-source suppliers; explore regional manufacturing hubs.
- Embed Risk Intelligence: Use predictive analytics and scenario planning to anticipate disruptions.

Mitigation Strategies (continued...)

- Strengthen Governance: Implement robust ESG compliance and cyber resilience frameworks across all tiers.
- Leverage Budget 2025 initiatives: Utilise funding for skills development, regional supply chain hubs, and workforce training programmes to strengthen resilience and reduce reliance on overseas suppliers.

What Risk Managers Should Do

- Conduct comprehensive supply chain risk assessments, focusing on material scarcity and capability gaps.
- Establish contingency plans for critical projects, including alternative sourcing strategies.
- Engage suppliers to verify ESG compliance and cyber resilience measures.
- Invest in supplier development programmes to build technical competencies in engineering and project management.
- Use scenario planning to stress-test infrastructure delivery under disruption conditions.

Resilience of the UK's critical national infrastructure

by Dr Robert Chapman CFIRM

The UK's Critical National Infrastructure (CNI) affects every man, woman and child in the country, from safe drinking water, to food on supermarket shelves to the energy that heats our homes. Significant international developments over the last 12 months have made the UK more concerned about the protection of its CNI. Geopolitical tensions, state and criminal cyber campaigns, global supply chain fragility and extreme weather are all having a direct impact on CNI resilience and our way of life. For clarity, the UK government has defined CNI as being composed of 13 elements:

There is a clear consensus that the UK's CNI plays a vital role in the UK's economy by ensuring the smooth functioning of essential services and supporting economic growth. Here are some key contributions:

1. Economic Stability: The CNI sectors, such as water, energy, transport, and finance, are crucial for maintaining economic stability. They provide the backbone for our daily lives and business activities up and down the country.
2. Investment and Growth: Significant investments are made in infrastructure projects, which drive economic growth. For example, the current government recognises substantial investment in infrastructure is required, (jointly by the government and private enterprise), to support economic recovery and long-term growth.
3. Job Creation: Infrastructure projects create numerous job opportunities across various sectors, including construction, engineering, digital technology and space. This not only boosts employment but also enhances skill development and innovation for long term prosperity.
4. Regional Development: Investments in infrastructure help in regional development by improving connectivity, reducing disparities, and supporting local economies. Projects like the previous government's £36billion Network North aimed to unlock significant transport benefits for towns, cities, and rural areas.
5. Resilience and Security: The CNI ensures the resilience and security of essential services, which is critical for national security and public safety as well as the economy. Protecting these infrastructures from cyber threats and other risks is a priority for the government.

The UK government's latest response to protecting CNI is the introduction of the Cyber Security and Resilience Bill (November 2025), alongside the wider UK Government Resilience Action Plan (July 2025).

These measures aim to strengthen cyber defences, broaden regulation, and embed resilience across essential services. The Cyber Security and Resilience Bill (2025) was introduced to Parliament on 12 November 2025 as the most significant update to UK cyber legislation since 2018. Its purpose is to reform and expand the Network and Information Systems (NIS) Regulations 2018 to increase UK's defences against cyberattacks. Its key provisions include taking steps to strengthen vulnerabilities in the supply chains for operators of essential services (OESs) and relevant digital service providers (RDSPs). Specifically tougher security obligations for a wider set of technology service providers (including data centres and managed service providers), a stronger regulatory landscape for reporting cyber incidents, national security powers allowing ministers to direct preventive action against threats and measures to address risks linked to artificial intelligence misuse.

The backdrop to this Bill, according to Infosecurity Magazine, is that the National Cyber Security Centre (NCSC) reported a 130% increase in nationally significant cyber incidents in 2025 compared to 2024. Within their 2025 Annual Review 2025, the NCSC advise the Cyber threat to the UK CNI remains high. Cyber remains a discreet, low-cost, high-impact vector through which threat actors target the UK's CNI for espionage, ransomware and disruptive purposes. Ransomware conducted by financially motivated criminals continues to be the most immediate, disruptive threat to CNI sectors. The high-profile cyberattacks by the DragonForce ransomware group left customers unable to make payments and saw the data of all 6.5 million Co-op members stolen.

CNI providers must 'step up to the plate' and ensure that their operations are resilient to external threats, regardless of their source or nature. One approach is to ensure 'secure by design' to ensure that the lifecycle of CNI projects incorporates resilience within the design from inception through all design stages, to supply and finally operations.

Uk Rail Infrastructure Trend

By Cameron Burton

The UK Government's Spending Review 2025 (SR25) provided the rail sector with multi-year capital certainty, offering stable investment for long-term planning on major rail infrastructure programmes. [1]

The capital funding settlement strengthens the pipeline of major projects and enhancements across the UK by supporting key national and regional schemes. Budget 2025 reinforced this commitment with over £120 billion in additional capital investment for roads, rail, and energy, including £15.6 billion for city-region transport projects. [2] While SR25 has enabled regional enhancements through additional capital investment, uncertainty remains over whether operational funding will be sufficient to meet the needs of ageing assets and the condition of existing infrastructure, an issue that will place greater emphasis on strong and effective risk oversight across the sector.

Major projects, including High Speed 2, the Transpennine Route Upgrade, East–West Rail, and other regional enhancements, will benefit from this multi-year funding.

Budget 2025 also announced a one-year freeze on regulated train fares, easing cost pressures for passengers while supporting demand recovery. These investments can modernise infrastructure, improve connectivity, and deliver long-term value for passengers and operators. These investments create potential opportunities for project risk managers across the UK, provided that risk management is embedded in project culture and reinforced by the demands of sponsoring government departments.

Delivering the ambitions enabled by SR25 presents challenges in project risk management capacity and capability across the UK.

A shortage of experienced risk managers on rail projects could limit effective controls and slow decision-making. Budget 2025 includes measures to strengthen workforce capability through targeted skills programmes, supporting delivery of major infrastructure projects. As major programmes continue to accelerate, the industry must address the regional skills gap, provide targeted training and deploy experienced rail risk professionals strategically to critical projects.

While SR25 secures capital funding, operational funding presents a contrasting picture. The Office of Rail and Road forecasts real-term reductions in operational expenditure. [3]

Reduced operational budgets increase reliance on maintenance rather than full asset renewals, placing pressure on an ageing network. This reduced flexibility heightens the likelihood of infrastructure failures, unplanned interventions and service disruptions. These pressures affect passengers, operators and supply chains, while reactive work typically carries higher financial, schedule and performance risks. Project risk managers must be vigilant in identifying emerging risks early and mitigating them promptly, enabling informed decision making and safeguarding a resilient, operational railway.

SR25 provides capital certainty to the rail industry, creating significant opportunities to better connect Britain. However, without commensurate operational funding, disruption risks remain high - despite Budget 2025's capital boost. Project risk managers must anticipate and mitigate these pressures so that long-term rail investment delivers value while avoiding preventable cost growth and programme delays.

References:
[1] Policy paper Spending Review 2025
[2] Policy paper Budget 2025
[3] ORR: Network Rail is delivering efficiently, but cost pressures remain and the industry must keep focus on safety throughout rail reform

As major programmes continue to accelerate, the industry must address the regional skills gap, provide targeted training and deploy experienced rail risk professionals strategically to critical projects.

- CAMERON BURTON

Innovation Group

The Innovation Special Interest Group is a forum for discussion and development of new ideas in the field of risk management. The Group is specifically interested in concepts that create value for the enterprise and which focus on “upside” or opportunity risk.

This entry has been authored by:

- Rodrigo Silva de Souza
- Sarah Gordon
- Katalin Horvarth

Interdependence

INNOVATION INSIGHTS

Emerging Risk Trends to 2026: Insights from the IRM Innovation SIG

On 27th November, the IRM Innovation Special Interest Group (SIG) met to explore emerging risks, using an interactive Mural board exercise, aiming to identify major global shifts, threats, and opportunities on the horizon of risk practitioners, representing a gender, age, jurisdictional and sectorial diverse group.

Over the past year, these practitioners have had a broad set of issues on their risk radar: developments in AI and quantum computing, cyber threats, climate change and extreme weather events, economic downturns, geopolitical tensions and armed conflicts, political polarisation and misinformation, the impacts of US politics, rising inequality and unemployment, ageing populations, and the availability of critical minerals. Looking ahead to 2026, they highlighted a set of interconnected threats and opportunities that risk professionals should pay particular attention to.

Climate and Environmental Risks

Climate risks are becoming a constant feature on the risk landscape. Extreme weather events are more frequent and severe, including droughts, floods and natural disasters. Participants shared a growing recognition of the need to build climate resilience. Increasing climate-related disclosures and regulatory requirements are driving greater transparency, but also the risk of non-compliance and greenwashing, especially, due to fictitious sustainability targets and figures.

Climate change is also a source of great opportunities. Governments, corporations and individuals are pushing for circularity and regenerative business models, supported by better data and focused on strengthening climate actions. Moreover, advances in renewable energy and nuclear fusion hold great potential to innovative solutions away from the overreliance on fossil fuels. Thus, climate risk management can increasingly be reframed as an enabler of long-term value creation and preservation, not only a threat.

AI, Technology and Cyber Security

AI emerged strongly in the discussion also representing both sides of the risk coin. Although singularity may not be immediate, participants recognised its largely unknown consequences. Furthermore, AI is already reshaping our lives and risk management practices in several ways, such as:
·Amplifying misinformation and fake news, increasing polarisation and mistrust;
·Enabling integrated, data-driven solutions to improve decision-making, analytics and efficiency;
·Increasing the attack surface for cyber threats, while also offering powerful tools to detect, prevent and respond to cyber incidents.

In this mix of threats and opportunities, quantum computing has been identified as another transformative technology that will influence how we deal with both encryption and cyber security, potentially triggering a new phase of technological change.

A consistent concern across the group was also the skills gap as organisations are still working out how to acquire, develop and retain the capabilities needed to operate in an 'AI-enabled' world. Yet, open questions exist regarding how AI will truly support social needs and inclusion, for example in healthcare, and what it will mean for national security and geopolitics, whether as a critical asset and potential weapon.

Geopolitics, Inequality and Society

Geopolitical instability and rising tensions due to armed conflicts (e.g., in the Ukraine, Gaza and Africa) and the wider impacts of political changes (e.g., in the United States) are expected to remain central to the risk landscape in 2026. These dynamics affect energy security, supply chains, critical infrastructure and international relationships.

Access to technology has the potential to exacerbate global inequalities. In the Global North, earlier adopters and broader access to advanced technologies, has the potential to reinforce disparities. In the Global South, technological developments may trigger radical changes, challenging oppressive regimes, organising social movements and questioning long-established institutions (e.g., Nepal's recent upheaval). While these forces are sources of great uncertainty, they may be used to erode trust in traditional structures.

Demographic trends add further complexity as a relatively young and growing Global South contrasts with ageing societies in the Global North. Declining birth rates, generational gaps in the workforce and forced migration create pressures and opportunities for labour markets, social systems and political stability. There are also important social and psychological dimensions to technological change.

Participants noted potential impacts on social isolation, mental health, productivity and workforce availability. As new ways of work practices emerge, organisations will need to focus more on multi-stakeholder engagement, diversity, equity and inclusion, and on ensuring that new models remain humane and sustainable.

Regulation, Infrastructure and Operational Resilience

Participants emphasised the growing importance of operational resilience, particularly in light of systemic risks, new financial services regulations and expanding requirements for disclosures. These developments are occurring against a backdrop of ageing infrastructure, especially in the Global North, and increasing interdependence across systems.

Interconnectedness and interdependence mean that local disruptions can propagate quickly along supply chains and across sectors. This requires a more collaborative, integrated and systemic risk management perspective, to understand not only own vulnerabilities but also those of critical suppliers, partners and wider ecosystems.

Implications for Risk Management

Across these themes, several implications for risk management to 2026 emerged:

- From threat-focused to opportunity-aware: There is a need to build a more positive risk culture that recognises opportunities alongside threats and learns from successful cases of new (and more sustainable) business models, decentralised technological developments, ecosystemic resilience and innovation.

- Managing multiple dimensions of values: Risk professionals must consider multiple dimensions and values at risk, not only financial impacts, and think beyond a simple 'threat versus opportunity' framing.

- Systemic and long-term thinking: Interconnected, long-horizon risks such as climate, technology and demographic change require integrated, cross-functional approaches and a willingness to think beyond short-term planning cycles.

- Capabilities and collaboration: Addressing emerging risks will require both robust risk management and critical, innovative thinking. Organisations will need new skills in areas such as data analytics, scenario planning, technology, stakeholder engagement and systems thinking.

Ultimately, the discussion pointed towards the need to integrate business strategy and risk management into three dimensions: individual, organisational and broader multistakeholder community, such as farther tiers of supply chain. In other words, we need to start to consider risks by 'thinking with our whole brain', 'operating as a whole body' and to collaborating across functions, organisations and sectors as a 'family of families' within a broader society.

By doing so, we can co-create new opportunities and build a more resilient future for organisations and society, not only to 2026 but beyond.

Use of imagery in this report:

The imagery in this document has been specifically chosen to reflect the emerging risk of water scarcity due to the proliferation of new AI data centres around the world. AI uses massive amounts of water, primarily for cooling data centres, with a single large facility using up to 5 million gallons daily. Consumption is projected to reach up to 6.6 billion cubic meters annually by 2027.

As with the world, this report's visual language gets increasingly drier, amplifying the narrative of the research presented.

Acknowledgements

Thank you to all the IRM members who took the time to complete our survey and help us shape the data in this report. And an enormous thank you to the IRM staff members who helped to put this report together.

Most importantly, we'd like to thank all the members of the IRM Special Interest and Regional Groups for their invaluable contributions. Their insights and expertise are the reason we're able to put together reports like these, and we're incredibly grateful to work alongside them.

Design and Project Management:
Andrew Demetriou, IRM Content Manager

Research and Development:
Danial Ibrahim, IRM Senior Marketing Manager

Proofreading:
Gemma Bowles, IRM Marketing Manager
Pearse Walsh, IRM Marketing Manager
Nick Webber, IRM Digital Marketing Coordinator