ENTERPRISE RISK

irm

THE EVOLVING DISCIPLINE OF PEOPLE RISK MANAGEMENT

Why understanding human behaviour is now central to effective risk management

WWW.ENTERPRISERISKMAG.COM | MAY/JUNE 2026

Symbiant® GRC Software

Recommended

Risk Management Software

“It’s a product I would certainly recommend!”

★★★★★

Innovation Group

symbiant.co.uk

Contents

THIS ISSUE: PEOPLE RISK

ENTERPRISE RISK

Enterprise Risk **is published on behalf of the Institute of Risk Management by Redactive Publishing Ltd**
redactive.co.uk

Sponsorship and advertising
Sales manager
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

Account manager
Aaron Nicholls
+44 (0)20 7880 8547
aaron.nicholls@redactive.co.uk

Editorial/production
Content manager Andrew Demetriou
Lead designer Gary Hill
Picture editor Akin Falope
Group content sub-editor
James Hundleby
Production manager
Aysha Miah-Edwards

Enterprise Risk is the official publication of the Institute of Risk Management (IRM).
ISSN 2397-8848

Institute of Risk Management
1st Floor, 80 Leadenhall Street,
London EC3A 3DH
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

About the IRM
The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

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

A NOTE FROM THE EDITORIAL DESK.

THE EVOLVING DISCIPLINE OF PEOPLE RISK MANAGEMENT

Organisations are discovering that their greatest opportunities, and their most significant vulnerabilities, often lie not in systems, but in people. The human dimension of risk has never been more important. From leadership and decision-making to culture, behaviour, talent and wellbeing, people shape how organisations respond to uncertainty, adapt to change and build resilience.

This issue of *Enterprise Risk* magazine explores the evolving discipline of people risk management and examines why understanding human behaviour is now central to effective risk management. As organisations navigate economic volatility, geopolitical uncertainty, technological disruption and changing workforce expectations, risk professionals are being called upon to look beyond traditional frameworks and engage more deeply with the human factors that influence performance, governance and organisational outcomes.

We are delighted to feature an exclusive interview with Stephen Sidebottom, Chair of the Institute of Risk Management (IRM), to mark the release of his new book, *Fundamentals of People Risk Management*. Stephen shares insights from his extensive experience in risk, leadership and human resources, and explores why people risk deserves a more prominent place in boardroom discussions. His book provides practical frameworks for understanding how behaviour, culture, ethics and decision-making influence organisational success, offering timely guidance for risk professionals seeking to integrate people risk into enterprise-wide risk management.

Throughout this edition, our contributors examine the challenges and opportunities associated with managing people-related risks in today's organisations. From fostering healthy risk cultures and strengthening leadership capability to addressing behavioural biases and enhancing workforce resilience, the articles in this issue demonstrate that effective risk management is ultimately about understanding people as much as it is about understanding processes.

This issue will also be the last collected issue of *Enterprise Risk*. We'll be moving to a more regularly updated news style format on our website with insightful articles, podcasts, interviews and free downloadable resources. We hope you'll check out the new website when it launches this summer. Until then, please enjoy the issue!

Andrew Demetriou
Content Manager | The Institute of Risk Management

Viewpoint

WHY ARE WE SEEING RECORD LEVELS OF MODERN SLAVERY IN THE UK?

When we think of slavery, we often think of the past and the stories we're taught in history classes. We think of film and TV as a form of representation that doesn't mirror modern society, when in actuality, slavery is happening all around us. Forced labour, trafficking and sexual exploitation are all forms of modern slavery, and could become increasingly difficult to detect in the coming years unless urgent action is taken to tackle criminal networks. The independent anti-slavery commissioner (IASC) has warned that the cost-of-living crisis and the rapid development of technology, especially the AI sector, is leading to record levels of modern slavery in the UK. In 2025, 23,000 potential victims of modern slavery were referred to the IASC – a 22% rise from the previous year and the highest figure ever recorded.

Read more here >>

COLLABORATION

IRM announces RIMAS partnership

The Institute of Risk Management (IRM) and the Risk and Insurance Management Association of Singapore (RIMAS) are pleased to announce a new strategic collaboration designed to advance professional development, knowledge sharing and organisational resilience across Singapore.

The collaboration reflects IRM Asia's continued growth and commitment to working with high-quality regional partners to expand access to risk management lifelong learning, thought leadership and professional networks. Through this relationship, IRM and RIMAS will explore practical ways to support members, practitioners and organisations in building stronger risk capability in an increasingly complex operating environment.

Under the framework, IRM and RIMAS intend to collaborate across several areas, including jointly organised events, member engagement activities, promotion of relevant IRM courses and qualifications, joint research and thought leadership, and potential future programmes linked to emerging areas such as AI governance and ISO 42001. The first joint activities are expected to focus on member-facing engagement, including webinars, roundtables and executive briefings, with both organisations bringing together speakers, subject matter experts and practitioners to address current and emerging risk issues.

Victoria Robinson, Head of Partnerships Asia at IRM, said: "We are delighted to be partnering with RIMAS, whose role in Singapore's risk and insurance management community is well established and highly respected. Together, we have an opportunity to deliver practical value for members, support lifelong learning and professional development and contribute to stronger organisational resilience.

PEOPLE RISK IN NUMBERS (FROM IRM RISK TRENDS 2026)

90%
of CEOs expect risk practitioner hires to increase over the next 12 months

71%
of CROs identified staffing and budgets as the biggest challenge in their organisations

50%
of CROs expect talent retention to be one of the hardest people risk issues they will face in 2026

AI RISK

Organisations urged to embrace AI as a governance and risk issue

The Institute of Risk Management (IRM), in partnership with SoftNet Technologies, Britain and New Vision, convened leaders from the Government, finance, technology and governance sectors to discuss the growing opportunities and risks associated with artificial intelligence (AI) in Uganda's institutional landscape. Held under the IRM-East Africa Chapter Executive Risk Engagement Forum, the annual dialogue brought together risk professionals, regulators, senior executives and governance practitioners from across Uganda and the East African region.

Hussein Isingoma, the acting internal auditor general, Ministry of Finance, Planning and Economic Development, emphasised the need for professionals and institutions to develop "fusion skills" that enable people to work effectively with AI instead of competing against it.

"Jobs will mainly be lost by those who fail to upskill and adapt to working with AI, while new opportunities will continue to emerge for those who embrace the technology," Isingoma said, adding: "We need to define AI governance frameworks and be aware of the risks."

He urged organisations to view AI as merely a technological investment and approach it as a business and risk management issue that directly contributes to organisational success and competitive advantage. The discussions come at a time when Uganda is accelerating its digital transformation agenda through the Fourth National Development Plan, the Digital Uganda Vision 2040, all of which promote technology-led transformation of public institutions and service delivery.

But Uganda still lacks AI-specific legislation, and existing governance frameworks were not originally designed to address the complexities and fast-changing nature of AI.

THE MISSING LINK IN CYBERSECURITY AND GOVERNANCE?

As organisations accelerate digital transformation and adopt emerging technologies such as artificial intelligence, cybersecurity and governance challenges are becoming increasingly human-centric. In a recent round-table discussion held together with Chartered Accountants Australia and New Zealand Association, this topic on Human Risk Management (HRM) was attempted to highlight an important shift in thinking: rather than viewing employees merely as vulnerabilities to control, organisations should understand, measure and positively influence human behaviour as a core component of risk management.

Read more here >>

PEOPLE RISK MANAGEMENT

FACE-TO-FACE WITH STEPHEN SIDEBOTTOM

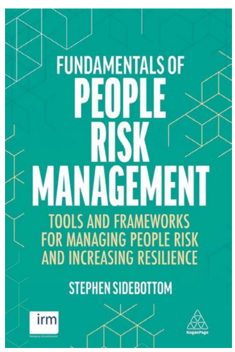
Hear from the IRM Chair about his experience in developing his brand-new book, *Fundamentals of People Risk Management*, available to purchase now at all good book retailers

People risk has become one of the most critical—and often overlooked—areas of organisational resilience. In this interview, we speak with Stephen Sidebottom, Chair of the Institute of Risk Management (IRM), about his new book, *Fundamentals of People Risk Management*. Drawing on his extensive experience in risk leadership, Stephen explores the evolving nature of people risk, why it deserves greater attention from boards and executives, and how organisations can build stronger frameworks to manage the human factors that influence success. We discuss the key themes of the book, the challenges facing practitioners today, and what effective people risk ma nagement looks like in practice.

What inspired you to write Fundamentals of People Risk Management, and why do you believe now is the right time for organisations to focus more seriously on people risk?

The book has grown quite naturally out of the overlap between two parts of my professional working life. I spent many years leading global HR functions and working with leaders on managing the human reality of organisations. I have also become increasingly involved in the world of risk, where there is a strong thinking discipline about uncertainty, exposure, control and long-term resilience.

These two worlds often look at the same organisation and the same event but don't always join the dots to create an holistic interpretation of what is going on. HR can see much of the lived reality of work and understands people management processes. Risk sees the formal architecture of governance and control but often has an underdeveloped view of the connection between the human system and enterprise risk.



The book doesn't argue that organisations have ignored people related risks. On the contrary, they already recognise many of the visible manifestations of these risks. Things like fraud, misconduct, capability gaps, concentration risks, well-being concerns and cultural failures are familiar to us from many examples across sectors.

But in practice it seems to me they are often managed as operational issues through process controls, compliance mechanisms or event responses, or sometimes as abstractions with general statements of intent.

Of course, these responses are often useful. Fraud prevention controls are necessary, as are things like conduct standards, clear incentives and accountability. Well-being requires significant attention to health, safety and workplace design. But the approach to people risk here asks a different question, an upstream question, about the conditions in the human system that make people risk consequences more or less likely.

This is rooted in my belief that a well calibrated human system creates sustainable long-term value for organisations. Financial soundness, commercial relevance and competitive positioning are essential, but they are not sustained in isolation. Sustainable performance also depends on the extent to which the organisation can build and maintain trust, competence, belonging, well-being, and learn and renew itself.

As to "why now?", organisations are operating in conditions where human systems are under increasing pressure.

Images: iStock/Shutterstock

Technology is changing work significantly, trust in institutions is weak, and external demands and pressures are rising. These forces are reshaping what organisations need from the people who work in them. and what those people in turn need from their organisations. Given this context, people risk cannot be treated as a set of HR issues or operational incidents - it has to be understood as part of enterprise risk management in support of long-term resilience.

Drawing on your experience in risk management, what were some of the biggest challenges you faced when translating complex people risk concept into a practical guide for readers?

Human systems are complex open systems, so there was a real challenge in working out how to approach this in a way that was relatively straightforward to navigate and allowed readers to work out what they were going to do. The biggest challenge was perhaps to accept that there is no single answer or formula that can be applied. It's not as straightforward as simply offering a model or checklist.

The book is, however, rooted in a relatively simple argument. People risk starts upstream, in the conditions that shape how people think, decide, and act. It is a property of systems, not individual behaviour. Organisations therefore need to move from events and symptoms to underlying conditions and system design in the way they think about understanding and managing their people risks.

It is also essential to understand organisational context. Every organisation has its own purpose, priorities, history, strategy, pressures and vulnerabilities. So, the practical question rapidly becomes not "what is the universal answer to people risk?", but "how does this organisation create value through its human system and where is that value vulnerable?"

That is why the book offers a framework, or a landscape of issues, rather than a formula. The framework links inputs with outcomes. The inputs are those areas where organisations can act, and the outcomes describe the human conditions that show whether the system is working well. These outcomes are not simply aspirations or sentiment measures but instead markers of long-term organisational health.

Inputs are the areas where leaders, HR professionals, and risk practitioners should intervene. For example, if trust is deteriorating, the answer is not to measure trust more elegantly. The task is to understand what leadership, cultural, work design, or external conditions are causing it to deteriorate in the first place. If there are problems of competence, the question should not be only whether training exists, but whether the organisation's strategy, operating model, and knowledge systems are aligned.

This is where the second line perspective of the book becomes so important - the risk oversight that challenges, monitors, and tests whether risk is being managed effectively. HR owns many people processes, but people risk is broader than HR process effectiveness. The book tries to give HR, risk professionals, and leaders a shared way of seeing how risk exposure is created and transmitted through the human system.

Were there any particular case studies, experiences or conversations that significantly shaped the direction and content of the book?

When I began the project, I expected to spend more time drawing specific lessons from interviews with managers, HR leaders and risk professionals. Those conversations were valuable in shaping the overall

direction, but I realised that the most interesting part was not usually the individual initiative they described, but how they were thinking about their organisation as a system. That shifted the book away from cataloguing good practice and more towards helping readers develop a way of seeing the system in which they are operating. In a complex organisation interventions only make sense in context. Identifying high impact interventions require a real understanding of timing, trust, leadership attention, and readiness for change. The same actions or interventions that can be catalytic in one setting could be performative in another.

Public case studies therefore become important because they allow us to step back and ask different questions. Not "who failed?" but "what did the system make more likely?", "what was being reinforced?", "what was being ignored?". Rather than offering a new diagnosis these case studies offer opportunities to consider how those same issues might play out in other organisations and to recognise that organisations can reach a state where they are no longer able to see and understand the dynamics within their own human system.

The book uses examples such as the Post Office Horizon scandal, Boeing, Wells Fargo and the Metropolitan Police to explore how people risk manifests in different places and over time. These organisations are all very different, but major failures often emerge from familiar patterns such as discounting weak risk indicators, making challenge costly, distorting judgement through incentives and mistaking activity for control.

The IRM people risk survey also shaped book. Respondents recognised people risk as strategically important, but repeatedly described the problem in terms of conditions rather than individual traits. Conditions such as overload, ambiguity, conflicting expectations, hierarchy and blurred ownership. That reinforced in my mind the need for a framework that starts upstream with the conditions that produce behaviour, rather than downstream with the risk event.

How do you see the relationship between organisational culture, leadership and enterprise risk evolving over the next few years?

I think culture will become much more central to enterprise risk, but only if we also become much more precise about what we mean by it and clear about how we manage it.

In the book, culture is not treated as a general organisational atmosphere. Instead, it is defined as what most people do most of the time. From a risk perspective, culture is an essential part of the control environment and should be managed as such. This is because culture either amplifies or dampens weak risk signals, it either accelerates or holds back organisational learning, and it either reinforces or undermines leadership intent. This means culture can become a powerful source of resilience, or a vector of harm. The difference depends on whether leaders see the system clearly and act with discipline to manage it.

In my experience this is where many organisations struggle. They can recognise issues such as conduct risk, ethical risk and cultural risk, but they often try to manage them through values statements, behavioural expectations, or compliance processes. Those things may be a necessary part of the control environment, but they are not enough. Decision discipline, challenge, ethical behaviour and candour cannot simply be mandated, they have to be created instead through the conditions people experience every day.

Leaders collectively shape what the organisation notice and acts on, what it tolerates, and when and how it learns. If leaders say one thing but reward another, the organisation learns from the reward. If challenge is invited but then punished, the organisation learns from the punishment. The formal message may matter, but the lived signal matters more.

Over the next few years, I expect more mature organisations to stop treating culture as a survey topic and start treating it as a living risk control surface. This means understanding how patterns of behaviour affect the organisation's ability to govern itself well, to learn from events and perform in a sustainable way. Organisations that already do this well connect leadership, culture and work design to value creation, reputation and trust outside the organisation. The book describes how this works through the people risk value chain showing the way behaviour inside the organisation translates into value, performance and stakeholder trust outside it.

What are some of the most common mistakes organisations make when trying to manage people related risks, and how can risk professionals begin to address them more effectively?

Organisations don't ignore people related risks. They do however frequently make the mistake of managing the manifestations of this risk in isolation.

Conduct risk is a good example. It is often managed through things like behavioural standards, incentives, customer duty obligations, conflict management and accountability mechanisms. Again, those are all important. But if the organisation only manages conduct at the level of process or individual behaviour, it may miss some of the deeper conditions that shape that conduct in the first place. The risk may lie in those conditions - decision discipline, ethical climate, leadership signals, workload, power, status and whether people can challenge what is happening around them.

The same is true of concerns such as well-being, capability and concentration risk. An organisation can treat each of these as a distinct operational issue, but together they also tell us something about the sustainability of the human system. A stressed system narrows judgement and decision quality. Fragile capability weakens resilience. A concentration of knowledge or authority creates dependency.

The role of risk professionals is to help shift the conversation from incident to system. This means asking not only "what happened?" but "what made this more likely, and where else might the same conditions exist?' They can also help organisations become more deliberate and disciplined about weak signals. The challenge is not simply to collect more data. The task is to understand which signals matter because they connect to the organisation's purpose, strategy and most important sources of value creation. That's where the second line has a particularly important role. It can help test whether people related exposures are being identified, owned, challenged and assured as part of enterprise risk, rather than treated as isolated HR, conduct, or operational matters.

What do you hope readers, particularly risk professionals, board members and business leaders, will take away from the book and apply within their own organisations?

I hope that readers take away the idea that people risk is not just about preventing people from doing

bad things. It's much more importantly about understanding how organisations create value through human systems and where that value is vulnerable.

For risk professionals, I hope the book gives them away into a territory that can sometimes feel difficult to handle. Culture, leadership and behaviour may appear less tangible than financial or operational risks, but they often determine whether controls work at all.

For HR leaders, I hope it offers a stronger connection between their work and enterprise risk and value creation. HR often holds many of the signals that matter, but those signals are too easily reported as activity or sentiment rather than interpreted as evidence about the long-term health of the system.

For boards and business leaders, I hope the book encourages a more disciplined and inquisitive conversation about the organisation they are creating. What is the system they have built teaching people to do? What does it really reward? What does it ignore in practice? Where does it learn quickly, and where does it defend itself against uncomfortable information?

The book frames these questions through the relationship between inputs and outcomes. The inputs are the domains under management influence: leadership, culture, capability, work design and external context. The outcomes are the states that indicate whether the human system is resilient: trust, competence, inclusion and belonging, well-being, and learning and renewal. When one of these outcomes weakens, it is a signal that the underlying input needs attention.

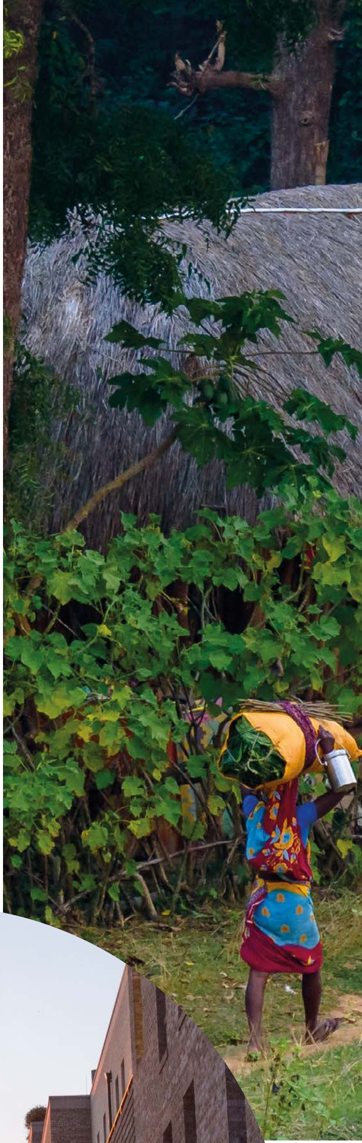
I think this is important for sustainability and preparedness. Organisations rightly spend a lot of time understanding their competitive environment, horizon risks, geopolitical exposure, supply chains and regulatory change. My argument is that the human system is just as fundamental to resilience. It determines the extent to which the organisation can see clearly, decide well, respond quickly and retain the trust it needs to operate.

That, for me, is the heart of people risk management. It's not so much a response to failure or a better way of reporting HR activity. Instead, it's a way of seeing, learning and shaping the human system through which long term business value is created.

Stephen's book is available to purchase now here.

Interviewed by: Andrew Demetriou, IRM Content Manager and ER Magazine Editorial Lead

Image: © Boeing



PEOPLE, SOCIETY AND GOVERNANCE

Anita Punwani, Founder and Chair of the IRM Environmental and Social Governance Group, discusses the ongoing impact of people risk in the ESG space

While organisations do place great emphasis on people in internal policy statements concerning health, safety and welfare, as well as equality, diversity and inclusion, the reality is that the well-being of certain groups of people is at risk due to gender inequality and exclusion factors arising from the way in which society is governed.

Climate change is a man-made crisis which is not affecting people equally - women and girls are at great risk. In the Global South, women constitute many of the poor and, in rural parts, are highly dependent upon local natural resources for their livelihoods. These people in society are at risk from weather events but also gender-based violence, with gender inequality being compounded in the face of the climate crisis as well as ongoing conflicts. In relation to extreme weather events, women and children are fourteen times more likely to die than men, which the United Nations (UN) claims is due in large part to limited access to information, mobility, decision-making and resources - it is estimated that four out of five people displaced by climate change are women and girls.[1]

Inequality and exclusion are placing people at risk in the Global North as well as the Global South. In the UK, certain groups in society were placed at higher risk of death and injury in the Grenfell Tower

disaster because their specific needs were not considered in evacuation planning. An investigation into Grenfell Tower by the Equality & Human Rights Commission concluded that government bodies failed to make reasonable adjustments in planning to help certain groups escape safely, including pregnant women and children; it is estimated that 40% of the building's disabled or vulnerable residents died in the fire.[2] The voices of residents were not valued, either before or after the fire; residents warned about fire safety issues and the dangers of catastrophic failure prior to the event .[3]

> We must ensure that governance oversees the management of risks to all groups in society environmental risk facing mankind today

Grenfell Tower was not an accident – it was a man-made disaster.

As risk professionals, we must ensure that the governance of organisations oversees the management of risks to all groups in society. This requires policies to be underpinned by values which give people from all groups a voice in managing the risks to them, such as the knowledge available from the residents of Grenfell Tower in health, safety and welfare planning, or the gender-sensitive strategies women can develop in handling environmental risks in the Global South. This does not only mean community engagement but inclusion in decision-making and access to resources. The UN encourages the inclusion of women in decision-making, both in mitigating the factors causing climate change, as well as adapting to its impacts. Including women in mitigating the social factors contributing to the crisis may prove to be the best chance of handling the greatest environmental risk facing mankind today.

Anita Punwani CFIRM is Chair of the IRM's Environmental & Social Governance Group which is focusing its thought leadership on 'Women and Children' this year.

References

1 United Nations: 'Why women are key to climate action'

2 International Bar Association: 'Grenfell report: a fire fuelled by a human rights crisis'

3 Fire Protection Association: 'Five years on: A resident's perspective'

Images: iStock/Getty

EMOTIONAL INTELLIGENCE

THE HUMAN SIDE OF RISK MANAGEMENT

Thomas Clare on why emotionally intelligent risk practice would help organisations

What we rarely name in risk: We're supposed to pride ourselves in risk management on objectivity. We have frameworks, controls, appetites, reporting cycles and assurance routines. We discuss uncertainty almost as if it's neutral, but the work itself is not.

Behind every risk manager, team or function, I believe there's a simple truth. Risk work can sometimes be emotionally heavy, which affects people in different ways – particularly when it is done well and close to real decisions.

This often shows up when risk teams are closest to decisions with real human consequences – safety, livelihoods, national capability, or reputational harm – where the work involves repeatedly imagining failure so others don't have to.

Risk professionals hold tension on behalf of a system. We try to anticipate harm, worst cases, challenge uncomfortable truths and decisions that others just want to get through. We're absorbing the anxiety, pressure and expectations of teams, suppliers and leaders, often so that decisions can be made with clearer sight of what matters. Yet our profession can treat emotional neutrality as the expected default, wanting the ideal risk manager to be a machine, not a person.

This becomes difficult to sustain as our profession continues to evolve, operating at a more strategic, decision-focused level. The human side is not a distraction from the technical discipline of our profession – it is a key control that will help its success.

The emotional labour in risk work

We often carry emotional load without the language for it. Over time, this can show up in predictable ways without care:

- **Holding other peoples stress:** absorbing worries from teams, leaders or suppliers
- **Chronic vigilance:** scanning for emerging issues, uncertainties and missed signals
- **Moral tension:** being the person who has to say "this doesn't look right" when everyone wants a yes
- **Identity strain:** balancing challenge without support, objectivity and empathy

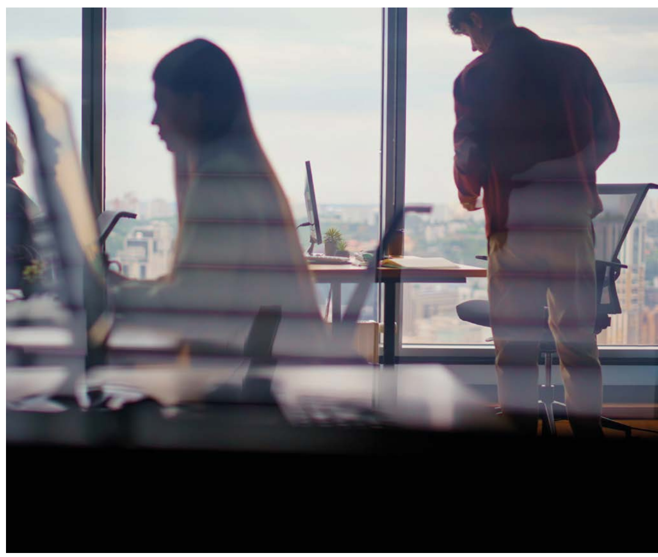
“The human side is not a distraction from the technical discipline of our profession – it is a key control that will help its success”

- **Vicarious stress:** repeatedly sitting with scenarios involving failure, harm, or loss

We'll never see this in a dashboard, but these factors will influence how someone thinks, decides and behaves when under stress. This isn't fragility, but more a sign of professional commitment and care for outcomes across teams and organisations. Without structures that acknowledge this load, people can start carrying it alone, and the early indicators that risk professionals are good at spotting in systems begin to show up closer to home.

The myth of emotional neutrality

Risk culture "done right" can often be described as calm and analytical. There is value here, but emotional neutrality is often mistaken for emotional absence.



Images: iStock

The alternative is not volatility or chaos. It is awareness – knowing what you're carrying and ensuring it doesn't begin to shape your judgement. When neutrality becomes an unexamined expectation, it can create predictable side effects:

- **Burnout masked as resilience:** people look steady long after their sharpness dulls
- **Reduced challenge:** emotional fatigue dampens the courage to speak up
- **Slower escalation:** overloaded teams avoid difficult conversations until they become unavoidable
- **Groupthink:** when feelings are exposed, people mirror the room instead of questioning what they hear.

The role of the risk professional is to model honesty, curiosity and professional dissent. When the load of their work is ignored, those qualities start to quietly recede. A risk team that can no longer challenge with confidence becomes a systemic risk.

Why does this matter now?

Across many organisations, risk conversations are changing. We are moving from compliance to culture, from process to decision quality, from technical expertise to human capability, and from information delivery to influential challenge.

This needs something deeper than frameworks or more elaborate software. It needs risk professionals who can stay reflective, grounded and psychologically safe to challenge with confidence when they need to.

As organisations are asking risk professionals to play a more strategic role, the emotional component of it increases. This will need more than technical excellence. Emotional intelligence, self-awareness and human centred practice are increasingly becoming key differentiators in effective risk leadership.

Emotionally intelligent practice and better decisions

This isn't a wellbeing agenda. It's about strengthening the conditions for better decision making in our organisations.

Some of this sits with individual capability – self-awareness, emotional regulation and personal boundaries. Much of it though is organisational – leadership behaviour, culture, and whether psychological safety genuinely exists.

When the emotional dimension of risk work is

This isn't a wellbeing agenda. It's about strengthening the conditions for better decision making in our organisations

acknowledged and designed for, several effects become visible. Challenge becomes more consistent, rather than personality dependent. Escalation happens earlier, with less filtering of risk signals. Analysis becomes clearer and less distorted by internal pressure. As a result, leaders receive earlier, more direct insight into emerging risk. These are not individual traits, but conditions organisations can deliberately shape.

This is not to make the profession "softer". The world is a complex, rapidly changing place and the risk profession is needed to help understand that uncertainty. If we can remove more of the friction from the system, risk professionals can then help organisations see these threats more clearly and at pace. A risk team that feels safe to think is a team that helps keep the organisation safe.

What helps

We can do this in many ways:

1. **Reflective practice as a standard:** through structured reflection, either individually or as a team, you can help process the emotional load and sharpen judgement. Other high-stakes professions use it regularly, risk could too.
2. **Psychological safety as an indicator:** does the team feel safe to raise concerns, challenge assumptions or signal emerging issues? It's not a "nice to have", it's a significant indicator of organisational risk.
3. **Emotionally aware decision making:** checkpoints with a team benefit from acknowledging what decision is about to be made, or what they need to do. When emotions are surfaced early, it becomes clearer on what needs to happen.
4. **Coaching informed leadership in risk roles:** leaders need the capacity to notice human cues such as avoidance, stress, disengagement, over compliance or bravado. Coaching mindsets

support healthier challenge and better conversations.

5. **Debriefs to address the system and the self:** after major moments, reviews should look at what happened and how it felt. Not as therapy, but to understand how emotional states can influence communication, judgement and escalation.

A new way to think of professional resilience

If resilience often becomes "carry on regardless", when the stresses of the delivery in an organisation strike, there could be a place for something more: "Resilience is the ability to feel the weight of something, understand it, process it and continue with clarity."

This matters because the job requires sustained engagement with ambiguity, failure and difficult truths. Pretending these are emotionally neutral only shifts the burden onto individuals rather than an organisation supporting it. Recognising this openly can help distribute the impact across the system, and benefit all.

Healthy risk teams challenge more effectively, escalate earlier, and ultimately can assist in making organisations safer.

> Leaders need the capacity to notice human cues such as avoidance, stress, disengagement, overcompliance or bravado

The future of risk is human

If the profession continues to want to position itself as one of strategic influence, its greatest asset to look to the future won't be perfect registers, templates and frameworks. They have a place, but they won't be enough.

The real strength will be the human capacity of risk teams. It's awareness, emotional literacy, reflective ability, safety and the authenticity in rooms where decisions are made.

If we want clearer challenge, earlier warnings and stronger organisational outcomes, we must ensure we are designing risk systems that sustain and enable the people tasked with protecting the organisation.

When we look after the humans carrying the risk, the whole system becomes safer and more effective.

Thomas Clare CFIRM

DIGITAL RISK IS ENTERPRISE RISK: THE CASE FOR AI AND DIGITAL COMMITTEES

Where AI adoption is widening and oversight is becoming fragmented, a well-run committee can be difficult to beat

Artificial Intelligence (AI), digital transformation, automation and cloud computing (and other technologies) have quickly become fundamental to modern business strategy. Organisations across nearly every sector are adopting these technologies at pace, pursuing greater efficiency, improved customer experience and lower costs.

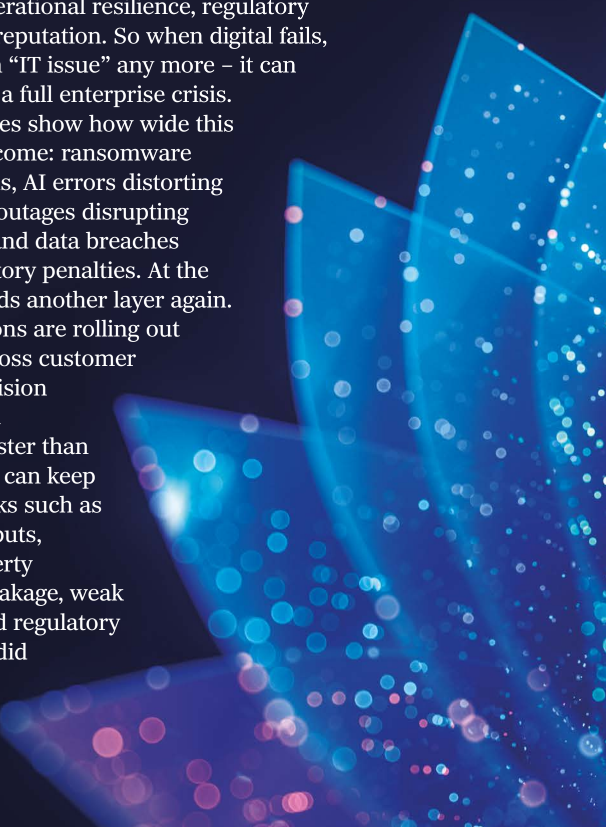
However, one of the challenges of rapid adoption is ensuring sufficient coordination and governance. Without it, organisations can quickly find themselves dealing with fragmented initiatives, strategic misalignment, flawed AI-driven decisions, cyber incidents and poor data governance. Traditional committee structures are not always well positioned to manage this complexity.

The question therefore becomes whether existing governance arrangements are enough. Many organisations continue to oversee AI through existing risk, audit or technology committees, particularly while adoption remains relatively limited. A dedicated committee usually becomes necessary once AI adoption widens, risk exposure increases or oversight starts falling between multiple committees.

Digital risk has become enterprise risk

Digital risk has become enterprise risk. Technology now sits at the centre of strategy, financial performance, operational resilience, regulatory compliance and reputation. So when digital fails, it is rarely just an "IT issue" any more – it can quickly turn into a full enterprise crisis.

Recent examples show how wide this exposure has become: ransomware halting operations, AI errors distorting decisions, cloud outages disrupting critical services and data breaches triggering regulatory penalties. At the same time, AI adds another layer again. Many organisations are rolling out generative AI across customer engagement, decision support and data analysis, often faster than their governance can keep up – bringing risks such as hallucinated outputs, intellectual property exposure, data leakage, weak explainability and regulatory uncertainty that did not exist a few years ago.



That uncertainty is increasingly giving way to expectation. The EU AI Act's requirements for high-risk systems are phasing in, AI-specific regulation is emerging across parts of the United States, and countries such as Saudi Arabia are continuing to formalise their AI frameworks and regulatory expectations. For organisations, the direction of travel is becoming clear. This means organisations need to move towards demonstrating how AI is governed, not simply assert that governance exists.

Digital change has moved faster than many governance arrangements. Oversight tends to be split across committees – cybersecurity here, technology investment there, data privacy and innovation somewhere else again – which can lead to gaps in accountability, duplication of effort and inconsistent decision-making.

However, dedicated AI or Digital Committees are becoming more important. Done well, they bring these responsibilities together, connect technology risk back to strategy, and give boards a clearer way to manage one of the fastest-moving areas of risk they face.

> Technology now sits at the centre of strategy, financial performance, operational resilience, regulatory compliance and reputation

What an AI and Digital Committee is there to do

An AI or Digital Committee isn't there to run technology day-to-day – that remains firmly with management. Its role is to provide oversight, challenge and strategic direction, ensuring digital and AI initiatives align with the organisation's objectives and risk appetite. These committees can operate at either Board or Executive level. Board committees typically focus on strategic oversight, challenge and assurance, while Executive committees are generally more concerned with prioritisation, delivery oversight and escalation.

In practice, the remit is broad. One of the committee's primary responsibilities is ensuring digital and AI investments genuinely support business priorities rather than simply chasing the latest technology trend; maintaining visibility over cybersecurity, data governance, AI controls and third-party dependencies; and overseeing governance and ethical considerations such as transparency, accountability and data privacy as stakeholder and regulatory expectations continue to evolve.

At the same time, technology is often not the real constraint. Whether transformation succeeds usually depends on organisational readiness – leadership, skills and culture – which is every bit as much the committee's responsibility as the technology itself. Ultimately, the committee should monitor whether

Innovation without governance creates exposure. Too much control kills the very transformation it it meant to protect

digital initiatives are delivering their intended outcomes by tracking performance, adoption and control maturity, while ensuring risks remain understood and appropriately managed.

Getting the right voices in the room

Effective committees are multidisciplinary, bringing together business, technology, cybersecurity, risk, legal, compliance, data governance and strategy expertise. This diversity of perspectives helps break down organisational silos, promotes more balanced decision-making and enables the committee to champion responsible AI principles such as accountability, transparency, fairness and appropriate human oversight.

Risk representation is particularly important. Digital and AI initiatives are often driven by innovation and speed – which is entirely appropriate – but without risk involvement from the outset, committees can become overly focused on technology opportunity and insufficiently challenge downside exposure, interconnected risks and whether initiatives remain within the organisation's risk appetite.

In practice, this means maintaining visibility of key technology-related risks, including cyber resilience, AI model risk, data governance, regulatory compliance, third-party dependency and reputational exposure. It also means ensuring AI systems can be properly documented and explained – their purpose, performance and limitations – as regulators and auditors begin to expect this as standard evidence of oversight, not simply good intention.

Why some committees work and others don't

Setting up the committee is the easy part – making it effective is considerably harder and comes down to a few disciplined habits.

It starts with clear terms of reference: scope, authority and interaction with other governance bodies. Reporting should then be concise and decision-focused, covering both value realisation and risk indicators so members can determine whether initiatives are delivering value and operating within appetite, rather than simply creating activity.

One of the practical examples for effective oversight is the AI inventory – a clear, current record of what AI systems are in use, where, and at what level of risk. Without it, committees end up overseeing in the abstract rather than the specific, and this is something regulators are starting to expect organisations to demonstrate, rather than merely describe.

And because this landscape moves quickly, continuous learning is essential. Committee members need to stay current on AI capability, cybersecurity developments and regulatory expectations; otherwise, their oversight risks lagging behind the very technologies they are meant to oversee.

Conclusion

Not every organisation needs a dedicated AI or Digital Committee. However, where AI adoption is widening and oversight is becoming fragmented, a well-run committee can be difficult to substitute for.

One of the biggest misconceptions is that committee effectiveness comes from having more members or the longest terms of reference; they are the ones that can evidence what they oversee – the AI inventory, the risk indicators and how AI systems reach and justify their outputs – rather than simply describe it.

Innovation without governance creates exposure. Too much control kills the very transformation it is meant to protect. Ultimately, the committees that get this right are the ones that can hold both at once.

Alexander Larsen CFIRM, Deputy Chair of the IRM Energy and Renewables Committee and IRM Saudi Arabia Committee member

Images: iStock