crf
CORPORATE RESEARCH FORUM

THE HR FUNCTION AND RISK MANAGEMENT:

Navigating Complexity with Resilience.

ABOUT CRF:

Corporate Research Forum (CRF) is a research-led learning network dedicated to building the capability of HR leaders and their teams to drive organisational performance.

Through more than 30 years of research and practical expertise, we have developed a deep understanding of the ways HR can contribute to business outcomes – what works, what doesn't and in what circumstances. We support our network of over 275 organisations through an evolving programme of evidence-based insights: delivering expert-led events, facilitated peer exchange, personalised and timely answers through our AI research tool and impactful

CORPORATE RESEARCH FORUM

technology-enabled learning – all informed by research and shaped by practice.

Our focus enables HR to become a more strategic, future-ready function delivering consistent and measurable value tailored to the needs of your organisation.

For more information on how CRF can support you and your organisation, please contact **Richard Hargreaves, Managing Director,** at **richard@crforum.co.uk**

Please visit our website »

RHR COMMENTARY

Navigating the High-Wire Leadership Succession as a Strategic Risk Exercise

By RHR Senior Partner, Head of International, Region Lead—Europe, Orla Leonard

Leadership succession is often treated as a static governance exercise—a list of names reviewed annually and filed away. But recent data and behavioural research suggest that succession is one of the most volatile strategic risks organisations face. In 2024, CEO departures reached record highs, with more than 2,200 exits globally, a 16 percent year-over-year increase. By 2025, the projected annual succession rate for large-cap companies climbed to 13 percent.

The financial consequences are severe. Replacing a senior executive can cost more than 200 percent of annual compensation, while a failed CEO appointment can erase an average of $1.4 billion in shareholder value. Yet many boards and HR teams still approach succession as a probability exercise—focused on preventing failure—rather than as a plausibility exercise that prepares leaders for disruption. The shift from "controlling probability" to "managing plausibility" is now critical*.

The Failure of the "Autopilot" Model

Traditional succession frameworks often fail because they rely on retrospective data and linear assumptions about the future. This creates an illusion of control and leaves organisations exposed when reality deviates from plan.

Three patterns show up repeatedly:

- **The "Crown Prince" Syndrome:** Over-reliance on a single anointed successor concentrates risk. Research suggests that up to 70 percent of successions fail when transitions disrupt momentum or undermine trust.
- **The Operator Trap:** Many organisations over-prioritise operational excellence, producing leaders optimised for efficiency rather than transformation. As business models and stakeholder expectations evolve, this bias leaves companies short of strategic, adaptive leaders.
- **External Dependence:** By 2025, external CEO hires in the S&P 500 had risen to 33 percent—an eight-year high. This signals not opportunity, but a breakdown in internal bench strength.

These patterns reflect a deeper issue: succession systems designed to minimise visible risk often weaken an organisation's ability to absorb real risk.

Building "Risk Muscle" for Leadership Transitions

Succession should be treated as a dynamic capability, not a one-time event. A useful metaphor is jazz: structure matters, but success depends on improvisation when conditions change.

- **Distributed sensing.** Early warning signs of leadership strain—cultural drift, decision bottlenecks, loss of confidence—are often detected first by those closest to the work. HR's role is to enable distributed sensing, ensuring weak signals travel upward before they become crises.
- **Risk as a perishable skill.** Behavioral research shows that risk tolerance functions like a muscle: if it is never exercised, it deteriorates. When leaders are protected from small, contained risks, their stress response remains elevated, increasing the likelihood of paralysis in a true crisis. HR can counter this by designing "safe discomfort" through simulations, scenario planning, and leadership wargaming that normalise uncertainty.

The Psychology of the Successor

Modern succession decisions rely too heavily on résumé and past roles, and not enough on how leaders are psychologically wired to respond under pressure.

- **Experience weighting:** Leaders differ in how strongly they weight past losses versus gains. Those who are hypersensitive to loss may become overly cautious when stakes are highest.

- **Emotional modulators:** Emotions shape risk behavior. Fear tends to reduce perceived control and drive avoidance, while anger—counterintuitively—often increases confidence and risk tolerance. Understanding these patterns helps predict how a future CEO or CFO will act when conditions deteriorate.

These psychological factors are not character flaws; they are predictable human responses that can be assessed and developed when surfaced early.

HR's Role as Strategic Advisor

To play a central role in governance, HR directors must challenge inherited assumptions and recalibrate how boards think about talent risk.

- **Encourage small-stakes neutrality.** For initiatives involving 5–10% of budget or scope, optimise for learning rather than failure avoidance.

- **Apply temporal distancing.** Asking, "How will we feel about this appointment in ten years?" helps shift decision-making from emotional reaction to long-term judgment.

- **Audit the risk portfolio.** Leadership pipelines should be balanced portfolios, combining reliable operators with higher-variance visionaries. Individual failures are data points; systemic imbalance is the real risk.

The Imperative

In a volatile 2026 environment, succession planning can no longer be about preserving stability at all costs. Organisations that build true leadership resilience treat succession as an ongoing risk discipline—one that prepares leaders to improvise, learn, and act decisively when the unexpected arrives.

Three Takeaways for HR Directors

- **Succession is a risk system, not a list.** Static plans create false confidence; dynamic preparation builds resilience.

- **Risk tolerance must be practised.** Leaders who never face small risks are least prepared for large ones.

- **Psychology predicts performance.** How leaders respond emotionally to uncertainty is as important as what they've done before.
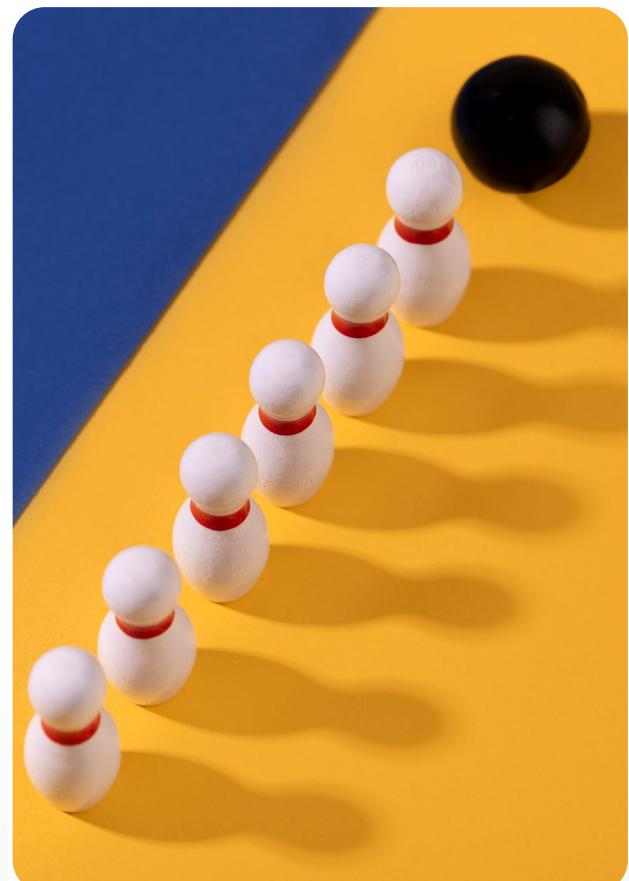
BIRD & BIRD COMMENTARY
The Role of HR in Mitigating Legal Risk
By Bird & Bird Senior Partner, Furat Ashraf

The convergence of technological advancement, geopolitical turbulence, and evolving employee expectations has created a challenging legal landscape for employers to navigate in recent times. HR functions are no longer simply managing people—they are navigating complex legal minefields that demand proactive, strategic responses. We look below at some of the key people-related legal risks facing businesses today and why HR leaders need to be at the forefront of tactical risk mitigation.

Cross-border compliance: handling international divergence

For organisations operating across jurisdictions, the regulatory divergence between the UK, EU and the US presents particular challenges. To take just one example, the EU Pay Transparency Directive (to be implemented by members states by June 2026) contrasts sharply, in both substance and in form, with pay transparency rules in the US and gender pay reporting in the UK. Similarly, areas such as monitoring working time, employee engagement in AI adoption and HR data collection and monitoring all require employers to operationalise compliance with a multi-jurisdictional lens.

A "one-size-fits-all" approach is increasingly harder to maintain and HR functions must now develop expertise in monitoring legal developments closely as they emerge and ensuring their employment practices and policies comply with differing legal standards. This has led to the development of more sophisticated and cross-functional compliance infrastructures, with dedicated resources for HR centres of excellence (to encompass payroll, people operations, reward and finance) that lead on change management exercises arising from key legal developments. Often the cost of getting it wrong—both financially and reputationally—can be significant and HR acts as a critical point of coordination across the business.

Data security in an age of remote working

The shift to hybrid and remote working has increased the vulnerability of employers to data breaches and cyber security threats. Confidential information now flows across home networks, personal devices, and unsecured connections, creating significant information security risks that can often be viewed as business critical. HR teams are central to effective risk mitigation, implementing robust data protection training programmes, enforcing stricter device management policies, designing effective offboarding procedures and collaborating closely with IT departments to ensure employees understand their role as the first line of defence. The challenge is not merely technical but behavioural - cultivating a culture where data protection is embedded in daily working practices rather than viewed as an inconvenient compliance exercise.

HR functions may also be first responders in case of deliberate data breaches by disgruntled employees and tasked with coordinating a response to swiftly recover confidential material, liaise with the DPO in respect of any disclosure obligations and implementing remedial employment procedures.

HR teams will often have a dual responsibility in both developing robust preventative measures to reduce the occurrence of such data breaches, alongside developing a clear response strategy for dealing with any breaches that occur.

Bird & Bird

Employee activism and geopolitics: reactive or proactive?

Employee activism around social and political issues has now emerged as a permanent feature of the employment relationship. Whether concerning climate change, diversity and inclusion or geopolitical conflicts, employees increasingly expect their employers to take a stand on such matters. Many workplaces have now become a forum for partisan debate which, alongside the use of social media platforms, can often result in a perfect storm for senior management.

Early responses were largely reactive and often inconsistent, increasing the legal risk of unfair dismissal and discrimination claims. Forward-thinking HR functions are now adopting proactive approaches, developing clear frameworks for an organisational voice, thinking carefully about establishing channels for employee dialogue, and intentionally shaping cultures and policies that can accommodate diverse viewpoints whilst maintaining tolerance and cohesion. This requires strategic management of employer values and culture together with a willingness to self-educate and engage with uncomfortable conversations.

Managing employee relations in a litigious environment

The substantial rise in employment tribunal claims and litigation has fundamentally changed the risk calculus for people management in recent years. The upcoming legal changes under the Employment Rights Act 2025 are likely to encourage more employees towards litigation, especially in light of potentially uncapped compensation for unfair dismissal and the shorter qualifying period of six months. Employees are generally more aware of their rights, better resourced through the advent of AI tools such as ChatGPT, and increasingly willing to pursue grievances and legal claims where they feel they have been treated unfairly or been discriminated against.

Proactive employee relations, both at an individual and collective level, has become a critical part of managing this legal risk.

HR functions are investing heavily in robust employee relations frameworks, improved performance management practices, and more sophisticated redundancy and change management processes, all with a view to managing employee expectations and investing in fair, documented and transparent procedures. This has a knock-on effect of making people management more time-intensive, but it is essential for mitigating legal risk and financial exposure for the business. The era of informal, relationship-based HR is giving way to one where the legality of the employer's actions is paramount since mistakes can be costly.

The advent of AI

The rapid advancement of AI technologies presents both opportunity and legal uncertainty. Questions surrounding AI-assisted decision-making in recruitment, performance management, and redundancy are largely unresolved, yet organisations cannot afford to wait for legal clarity before moving with their competitors. HR functions have a key role to play in contributing to AI governance frameworks, developing employee training and policies that regulate AI use, ensuring human oversight of automated talent and people management processes, and investing in upskilling programmes to maintain business continuity as roles continue to evolve. The challenge is to harness AI's potential whilst managing the impact of this on the future of the workforce.

crf
CORPORATE RESEARCH FORUM

THE HR FUNCTION AND RISK MANAGEMENT: NAVIGATING COMPLEXITY WITH RESILIENCE.

KEY TAKEAWAYS

- **Risk oversight needs to reflect how organisations actually create value today.** Much of that value now comes from people, knowledge and relationships — so it no longer makes sense to treat "people issues" and "risk issues" as separate.

- **Simply predicting risks in advance isn't enough anymore.** Because risks are more complex and uncertain, success depends just as much on how well organisations respond in real time as on spotting risks early.

- **Boards now expect HR to turn people data into clear risk insight.** Instead of just reviewing workforce metrics, boards want to understand how people dynamics affect risk exposure and organisational readiness.

- **HR leaders play different roles in risk management depending on the situation.** Their impact comes from knowing when to be directly involved in decisions, and when to shape the environment in which decisions are made. Our research sets out four roles HR leaders typically play. As **Subject Matter Expert**, HR provides data and insight into people-related risk exposure. As **Facilitator**, HR facilitates discussions on people risks, testing assumptions and linking to business strategy. As **Full Contributor**, HR contributes to enterprise risk strategy on an equal footing with other executives. As **Implementer**, HR translates business risks into practical people interventions. HR leaders can use our framework to consider what contribution they can make to risk and how they might take on that role.

- **Employee relations can serve as an early warning system for bigger risks.** How concerns are raised, listened to and acted on determines whether problems are dealt with early or spiral into major issues, placing HR at the heart of good decision-making and risk control.

- **Cyber risk isn't just a technology problem; it's a people and judgement problem.** When cyber incidents happen, outcomes depend on everyday behaviours, how quickly issues are escalated, and how decisions are made when standard controls fail.

- **Talent risk is a long-term business risk.** As skills needs change quickly and labour markets tighten, an organisation's ability to adapt its workforce shapes its future growth options.

- **Even though risks are harder to predict, organisations can still improve preparedness.** Preparedness means not just relying on forecasts and risk registers, but developing scenarios, experimenting with different solutions, building the ability to make decisions under pressure and being alert to early people signals.

- **The Conditions, Signals and Actions framework provides a practical lens through which HR leaders can answer three questions:** Where is risk building? How might it escalate? What actions should be taken?

- **When crises hit, success depends on practices that are built in advance.** HR helps by ensuring leaders know who needs to act, what really matters, and what boundaries to work within before disruption happens.

crf
CORPORATE RESEARCH FORUM

RETHINKING ENTERPRISE RISK MANAGEMENT

Many organisations operate under a paradox: enterprise value is increasingly shaped by human judgement and behaviour, yet enterprise risk management and HR functions have historically evolved along largely parallel trajectories.

This separation between people governance and enterprise risk oversight is becoming progressively difficult to justify in conditions of uncertainty and rapid change, representing a structural weakness in organisational resilience that HR is well placed to contribute to addressing.

Rather than being positioned as the owner of enterprise risk management, HR is better understood as the function responsible for helping to shape the organisational conditions through which contemporary risk is identified and managed.

This paper brings together research conducted by CRF and insights from our event in London on 22 January 2026.

View our webinar on The HR Function and Risk Management here »

> *If you asked me what my job is, I would say I'm a risk manager. That's what HR really does.*
>
> **Alison O'Connor, Chief People Officer, Arriva**

WHERE ENTERPRISE VALUE HAS SHIFTED AND WHY RISK OVERSIGHT MUST FOLLOW

The distinction between the governance of risk and the governance of people is increasingly difficult to sustain in an environment where corporate value is predominantly created through intangible and human-mediated assets.

Intangible assets describe the part of a company's value that comes from how it operates and what it knows, rather than from the physical or financial assets it owns. Examples include:

- Brand (customer trust and reputation)
- Intellectual property (patents and trade secrets)
- Technology and software (software code and algorithms)
- Customer relationships (long term contracts and switching costs)
- Data (proprietary datasets and analytical insight)

Ocean Tomo's *Intangible Asset Market Value* (2020) offers longitudinal analysis of the S&P 500 and shows a fundamental change in the composition of market value. In 1975, intangible assets accounted for approximately 17 percent of total market value. By 1995, this figure had increased to approximately 68 percent and by 2020, intangible assets accounted for approximately 90 percent of total market value.
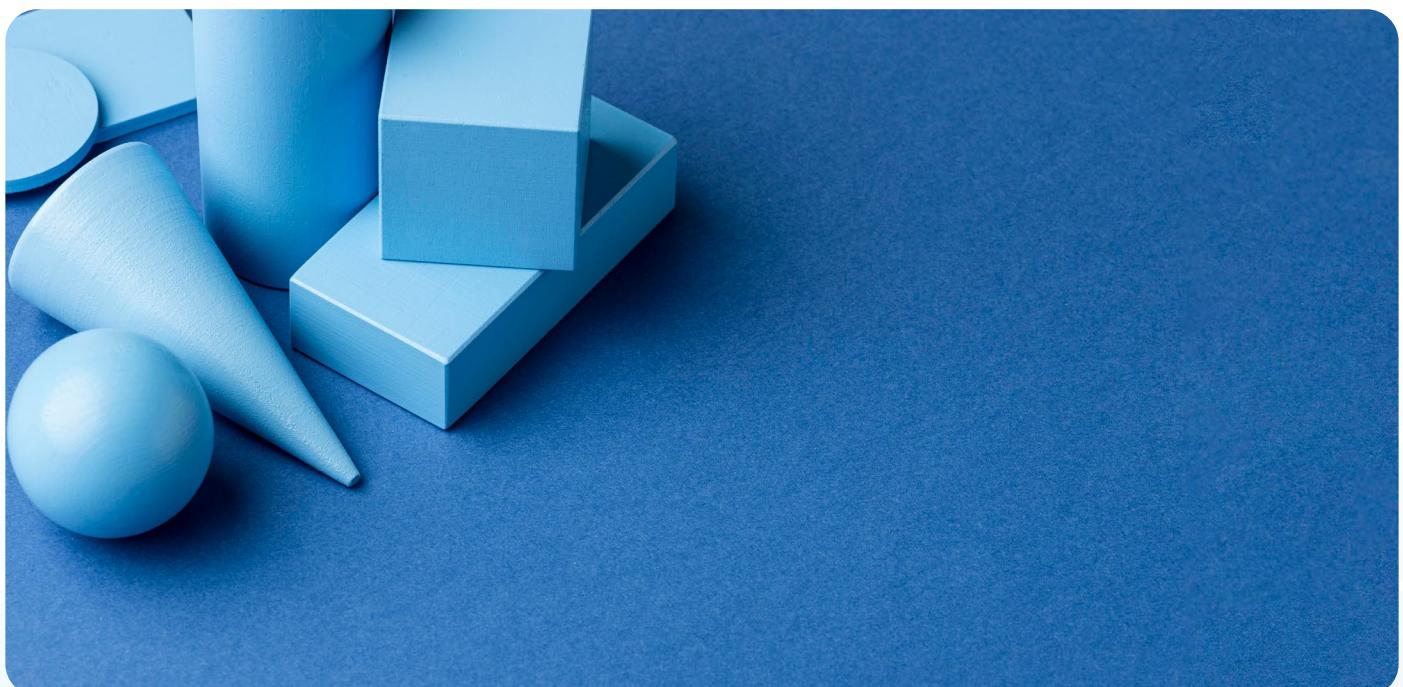
COMPONENTS *of* S&P 500 MARKET VALUE

	1975	1985	1995	2005	2015	2020
Tangible Assets	83%	68%	32%	20%	16%	10%
Intangible Assets	17%	32%	68%	80%	84%	90%

Tangible Assets — Intangible Assets
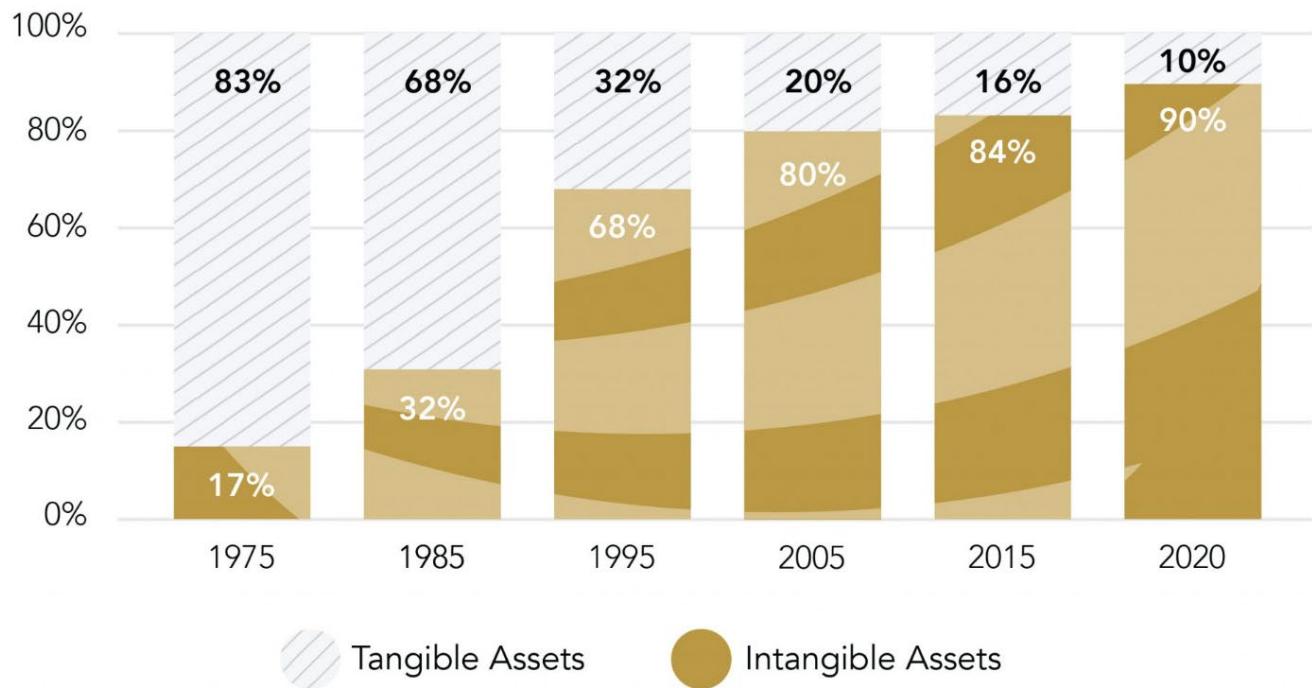
SOURCE: OCEAN TOMO, A PART OF J.S. HELD, INTANGIBLE ASSET MARKET VALUE STUDY, 2020

"The economy is inverting from one where value was measured by 'touch' to one where value is driven by thought." – Ocean Tomo, Intangible Asset Market Value Study (2020)

The significance of this shift lies not only in the scale of intangible asset dominance but in its persistence. The proportion of intangible value has remained consistently high across economic cycles, including periods of severe market disruption, indicating a structural rather than cyclical change in the composition of enterprise value.

As intangible assets are created and sustained through human judgement and organisational capability, their impairment is inherently linked to how decisions are made and knowledge is applied over time. This creates a growing misalignment between risk oversight models primarily designed to protect tangible assets and the primary sources of value and vulnerability in modern organisations.

THE CHANGING DYNAMICS OF ENTERPRISE RISK AND THE LIMITS OF PREDICTION

> *Much of what organisations are trying to manage is not only unpredictable but largely intangible and difficult to understand. As the risk environment becomes more complicated and more connected, HR sits at the centre through its role in people risk.*
>
> **Julia Graham, CEO, Airmic**

As enterprise risk becomes increasingly interconnected and uncertain, its impact is determined less by the accuracy of prediction than by the quality of organisational judgement exercised under pressure, making the governance of decision-making conditions central to effective risk oversight.

Risk no longer presents as a series of isolated events, but as interconnected pressures that interact and amplify across the organisation.

For example, the rapid shift to remote and hybrid working, initially treated as a discrete operational response to the COVID-19 pandemic, has generated sustained knock-on effects across workforce capability, organisational culture, leadership effectiveness, technology and employee wellbeing in ways that could not have been fully anticipated at the outset.

The pace and novelty of technological change increasingly outstrip the ability of organisations to fully understand or model risk in advance.

As organisations adopt new technologies to maintain competitive relevance, they are often required to make decisions under conditions of limited precedent and incomplete understanding, with consequences for how work is performed and information is handled shaped less by prior modelling and more by the quality of judgement exercised as impacts unfold.

Emerging risks reflect structural uncertainty rather than short-term volatility.

Aon's 2025 *Global Risk Management Survey* shows that geopolitical volatility has entered the top ten global risks for the first time. Increasing competition, ranked fifth and projected to rise to third by 2028, is driven by factors such as talent scarcity, technological disruption, changes in trade relationships and supply chain fragility. As organisations operate in conditions where risk drivers evolve faster than they can be stabilised, sustaining competitive relevance increasingly depends on adaptive approaches to decision-making.

At our London event, Professor Elmar Kutsch shared practical frameworks for scenario planning in contexts where prediction falls short.

To view our summary guide, please click here »

Preparedness gaps highlight limits of prediction.

McKinsey's *The State of Organisations* (2023) report found that only 50% of business leaders believe that their organisation is prepared to react to future shocks and disruptions. The same report found that over two-thirds of their organisations are overly complex and inefficient. This reframes risk as not failing just because it is unidentified, but because organisations cannot respond effectively once change occurs.

> "
> *The classic way of managing risk at the moment is very process driven… people use charts, talk about them once a year and tick it off. Moving forward that will change. People will start to think about the reality of more catastrophic eventualities becoming things they might have to deal with*
>
> **Nick Dalton, Former EVP HR, Unilever**
> "

FROM PREDICTIVE RISK MANAGEMENT TO ORGANISATIONAL RISK CAPABILITY

Taken together, the misalignment between asset-based risk oversight and the growing limits of prediction points to a shift in how enterprise risk capability must be developed.

In conditions where risk is embedded in judgement and unfolds through human systems, effective risk oversight depends less on centralised frameworks and more on the organisational conditions that shape how decisions are made in practice.

With visibility across the workforce, organisational design and leadership capability, HR occupies a structurally distinctive position in relation to enterprise risk. If risk now turns on judgement under pressure, boards need a clearer line of sight into the people conditions that shape that judgement.

> " *Organisations will have to develop a risk muscle, rather than a standalone risk strategy. HR can help teams and leaders develop that.*
>
> **Orla Leonard, Senior Partner, RHR** "
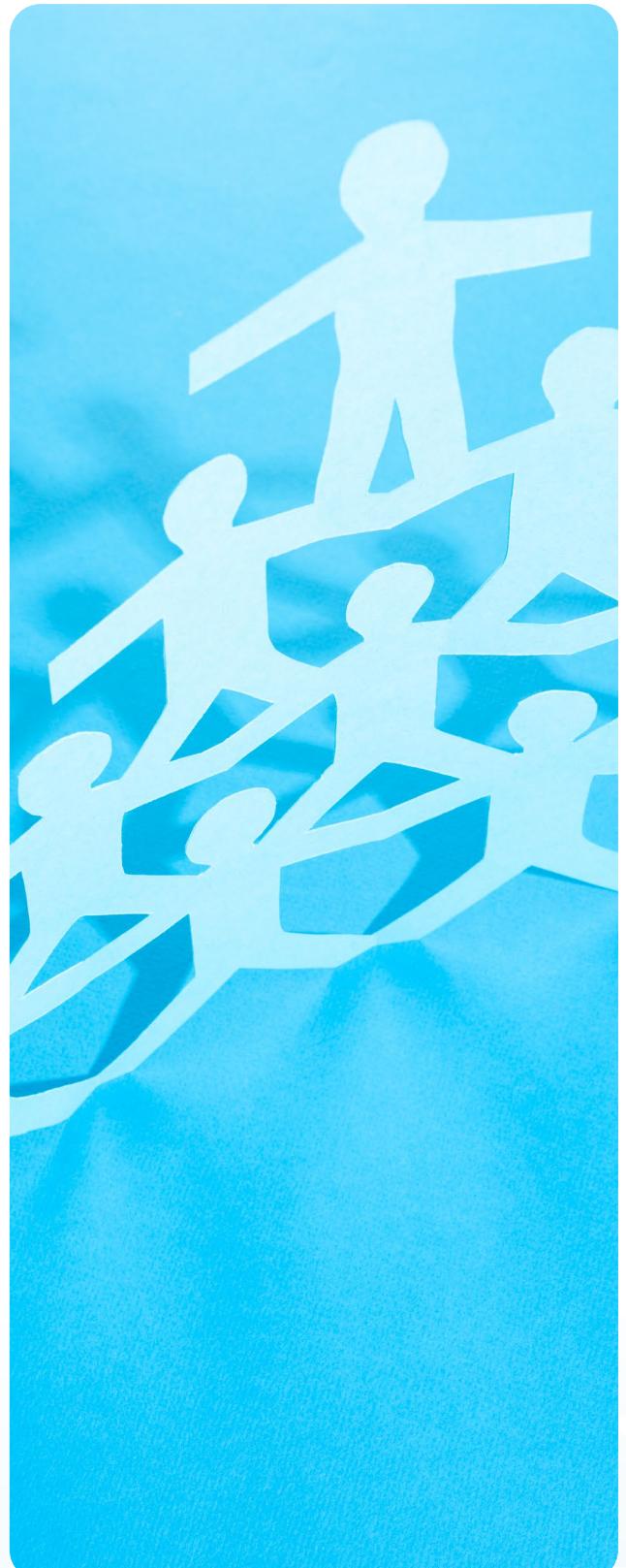
THE ROLE OF THE BOARD

> " *When making the case to boards for investing in HR, the risk argument matters as much as the benefits. Leaders need to understand what it costs when people decisions go wrong, and the role HR plays in protecting value.* "
>
> **Nick Dalton, Former EVP HR, Unilever**

Boards are taking greater ownership of people risk, but are still building the capability to interpret it, creating growing demand for HR to translate workforce insight into enterprise-level judgement.

Boards are no longer treating people issues as an operational or delegated concern.

They increasingly recognise workforce and capability decisions as material to enterprise value, resilience and risk. Research published by Forbes in 2024 found that higher-performing boards are taking a more active role in shaping and monitoring people strategy, recognising its importance to long-term value. This is reflected in governance structures, with WTW reporting in 2024 that more than 90 percent of S&P 100 companies have expanded the remit of their compensation committees to include broader workforce oversight.

At the same time, many boards still lack the capability to interpret people-related risk with confidence.

Research from CIPD in 2023 found that only 2 percent of organisations have HR representation at executive board level, and that fewer than a

third of FTSE 350 boards include HR expertise in either executive or non-executive roles.

There are signs that this is beginning to change.

Research from the Conference Board, reported via the Harvard Law School Forum on Corporate Governance in 2025, shows that CHROs are becoming more directly engaged with boards and are contributing more actively to strategic and enterprise risk discussions. The appointment of former CHROs to US public company boards has almost doubled in recent years, and expectations of deeper engagement are rising, with a majority of corporate secretaries anticipating that HR leaders will become more involved in board-level oversight over the next three years.

Together, this points to a shift in what boards expect from HR: not only more reporting, but clearer interpretation of how people dynamics translate into enterprise risk and strategic choice.

> " *The emphasis should be on insight rather than raw data. Without a strong risk culture, HR functions tend to produce data without addressing the 'so what'. The critical step is translating data into insight and demonstrating that senior leaders have actively discussed and engaged with those implications.* "
>
> **Jane Storm, CPO, Insurance, Wealth & Retirement, Aviva**

THE ROLE OF THE HR LEADER

Our research offers four ways HR leaders may engage with enterprise risk in practice. These can be understood through a two-by-two matrix that reflects both the depth of risk insight HR contributes and the extent to which it shapes how risk strategy is formed. Which an HR leader adopts depends on factors, such as:

- Individual capability
- Organisation expectations
- The needs and cycle time of the organisation
- Relationships with the CEO and executive team

In practice, HR leaders may move between roles over time rather than occupy a single position on the matrix. Some roles also create inherent tension. For example, acting as a 'full contributor' involves shaping the substance of decisions, while the 'facilitator' role focuses on shaping the process through which those decisions are developed. Where HR is expected to act as a 'full contributor' and no dedicated 'facilitator' exists, another executive or function may need to take on that role, allowing the executive team to focus fully on decision content.

CONTENT (vertical axis label)

PROCESS (horizontal axis label)

SUBJECT MATTER EXPERT:

- HR provides data on employees, demographics and markets to inform strategic decisions through a people-risk lens.

- HR provides expert insight into people-related exposure embedded in business strategy, for example succession vulnerability in critical roles under AI-driven skills disruption, or employee relations risk arising from inconsistent local practice across jurisdictions.

FACILITATOR:

- HR convenes and structures discussions on people-related risk, ensuring that these considerations shape the development of risk strategy from the outset.

- HR adopts a deliberate challenge role, testing executive assumptions by examining how strategic initiatives are likely to play out across the workforce in practice.

IMPLEMENTER:

- HR translates business and risk strategy into practical people interventions, creating a clear line of sight between strategic priorities and day-to-day activity.

- HR embeds people-risk considerations into roles, processes and incentives, ensuring that risk mitigation is built into how work is carried out rather than managed retrospectively.

FULL CONTRIBUTOR:

- HR contributes to enterprise risk strategy on an equal footing with other executives, shaping decisions rather than responding to them.

- HR originates strategic perspectives on risk by translating insight about the workforce, operating model and market context into enterprise-level exposure and opportunity.

Case Notes: The Four Roles

The examples that follow illustrate how HR leaders perform the four roles described in practice. Each case reflects a specific organisational context and moment in time, and the role adopted may shift as circumstances and risk exposure change.

Subject Matter Expert: Bank of England

- The Bank operates a three-lines-of-defence model for enterprise risk.

- Each quarter, every directorate, including HR, completes a Risk Control Self-Assessment, providing a largely 'bottom-up' view of risk that combines quantitative people metrics with qualitative judgement.

- The central risk function aggregates these assessments into an enterprise view, which is reviewed at Executive Risk Committee, with HR leaders sense-checking the people-risk commentary and contributing to discussion and deeper dives where required.

Implementer: Arriva

- Arriva operates under a unified "Zero Harm" principle that acts as a single organising logic for how risk is understood and acted on across the business.

- Zero Harm does not assume accidents can never happen, but rejects the idea that harm is inevitable.

- HR supports this by running a culture survey across 35,000 employees to understand lived safety conditions and by designing bespoke, practice-based leadership programmes to embed the mindset across the workforce.

- The approach is treated as ongoing and iterative, with the logic refined as organisational context and risk exposure change.

Facilitator: Hostinger

- HR facilitates cross-functional AI and automation guilds and squads, bringing together specialists from across departments and applying L&D expertise to design effective collaboration and learning formats that enable rapid experimentation and surface people and capability implications.

- The guild provides a forum where tensions between leadership pressure for speed and cybersecurity controls are worked through openly, recognising that both perspectives are valid.

- Rather than resolving these trade-offs within HR, the approach enables shared dialogue about how to balance innovation and risk in practice.

Full Contributor: Telecommunications organisation

- During post-acquisition integration, a payroll system failure days before the first payday meant thousands of employees were at risk of not being paid.

- Because payroll sat closest to HR's functional responsibility, the HR Director became the executive lead for the crisis, underwriting decisions about impact and response.

- HR owned supplier relationships and led judgements on continuity measures, working closely with technology and communications rather than deferring to them.

At our London event, Vincent Hodder, Chief Executive Officer of Leeds Bradford Airport, offered insight into the role HR leaders can play in supporting CEOs on enterprise risk.

Here are the key takeaways:

When assessing people risk in the context of business strategy, HR should evaluate decisions in terms of organisational resilience and future opportunity, not only immediate risk reduction. This requires comparing the consequences of action versus inaction, rather than attempting to eliminate risk altogether. In some cases, a difficult exit or legal process may carry less overall risk to the organisation than allowing sustained underperformance or a continued erosion of trust.

Enterprise risk decisions are more effective when HR establishes a trusted, non-subordinate relationship with the CEO. By operating as a partner rather than an executor, HR can speak honestly about implications, challenge thinking and provide a trusted space for CEOs to work through sensitive people issues that directly affect risk and performance. As noted by Hodder, *"The partnership between an HRD, CPO and the CEO is one of the critical relationships for the chief executive."*

These roles describe how HR leaders engage with enterprise risk. The following sections show where that engagement matters most in practice, focusing on three domains where people judgement now plays a decisive role in shaping enterprise risk outcomes.

EMPLOYEE RELATIONS

Employee relations is often treated as a reactive or compliance-focused activity. In practice, it is one of the earliest points at which emerging enterprise risk becomes visible. The way concerns are raised and responded to reflects underlying organisational conditions and shapes how risk is likely to escalate when pressure increases.

What's Changing?

Employee relations is being reshaped by forces that can lead to issues escalating at a pace and scale that would not have occurred in the past.

A more litigious and rights-driven workforce.

Workplace issues now escalate with less tolerance for ambiguity, making judgement and consistency more critical than procedural correctness alone. In the UK, the Employment Rights Act is likely to reinforce this dynamic by raising the legal baseline of employment practice and strengthening both collective rights and enforcement.

Loss of organisational containment through social and digital platforms.

Employee relations issues can move beyond the organisation quickly, reducing the time available to understand, resolve and contain them before wider consequences emerge.

> "
> *The impact social media is having on the workplace is to change stable networks into random networks.*
>
> **Nick Dalton, Former EVP HR, Unilever**
> "

AI-enabled escalation of disputes.

Easier formalisation and escalation of concerns is driving more adversarial disputes and weakening organisational capacity and decision quality. A 2025 survey by Irwin Mitchell found that 60 percent of HR professionals reported dealing with grievances they suspected were generated by AI, and 52 percent said these were more difficult to resolve, often because they used formal or legalistic language and lacked personal context.

Fragmentation of shared organisational context.

Differences in how decisions are experienced across the organisation mean that perceived inconsistency is increasingly a source of risk in its own right, rather than a by-product of policy failure. What one group experiences as moral leadership, another may experience as exclusion or bias, creating contested terrain in which neutrality is often interpreted as a stance.

How Are Organisations Responding?

In response, organisations are shifting from reactive case handling towards approaches that bring risk forward and improve the quality and defensibility of decisions.

Recognising managers as the primary risk control point.

Serious employee relations issues are typically preceded by earlier concerns that are not addressed consistently or in time. This places managerial judgement at the front line of containment, with HR processes operating as a backstop rather than the primary control. In practice, HR focuses on equipping managers to identify, address and record concerns early, using everyday judgement to prevent escalation into formal cases.

At our London event, Nick Dalton, former EVP HR at Unilever discussed the changing employee relations landscape. Two key takeaways were:

Workforce power is shifting from formal hierarchy to networks. Employees now have greater collective influence. As a result, employee-related risk increasingly arises from unmanaged networks rather than individual conduct alone, requiring HR to consider collective behaviour when assessing emerging enterprise risk.

The employment relationship is shifting from security to development. If organisations are increasingly unable to promise long-term job security, committing to the development of skills and capabilities provides employees with greater meaning and agency.

Using labour and union insights.

As collective bargaining strengthens, union relationships are increasingly being used to shape decisions earlier, rather than to discuss issues after conflict arises. Some organisations are appointing roles such as Head of Labour Relations to engage works councils and employee representatives before decisions are made, particularly where obligations such as pay transparency are still emerging.

Balancing psychological safety with decision accountability.

Psychological safety reduces risk when it helps surface issues that may be missed by formal processes and enables concerns to be raised early. However, it only supports risk reduction when anchored in disciplined problem-solving and clear decisions. As Orla Leonard, Senior Partner, RHR, cautions, openness must be paired with clarity about outcomes and rationale: "If there is an issue, step back, get the data, look at the pros and cons, and allow people to contribute openly, but be very clear and transparent about the conclusion and the rationale behind it."

Using systems and data to determine whether risk is visible or hidden.

Research from AdviserPlus finds that less than 40 percent of large organisations report full availability of employee relations metrics providing insight into trends, root causes and consistency across cases. Weak systems turn employee relations into a blind spot rather than an early warning function. Data supports judgement when it allows organisations to demonstrate decision consistency and evidence compliance at scale, enabling leaders to act with confidence rather than defensiveness under scrutiny.

> "
> *The instinct is to talk about trade unions and the issues they are going to cause that we will have to react to, as opposed to the opportunities of leveraging the collective productivity growth*
>
> **Nick Dalton, Former EVP HR, Unilever**
> "

> "
> *HR carries responsibility for team dynamics and effectiveness. That links directly to psychological safety and trust, which shape how open, creative, and honest risk conversations can be. The stronger those conditions, the more likely it is that teams surface the unusual or uncomfortable risks that would otherwise be missed in a tick-box process.*
>
> **Jonathan Kohn, Chief People Officer, Bibby Line Group**
> "

> *Compliance is twofold: it is not only about the legal interpretation of legislation across jurisdictions, but also about whether the organisation has the technological infrastructure to effect compliance at scale.*
>
> **Furat Ashraf, Partner, Bird & Bird**

Case Study: Hostinger — Employee relations as early risk detection

- Hostinger operates a leader-led approach to employee relations, positioning line managers as the primary mechanism for surfacing and containing issues before they escalate into formal risk.

- HR focuses on educating and equipping managers to address employee relations concerns while individuals are still in role, rather than relying on reactive case handling once positions harden.

- This approach is underpinned by clear cultural expectations and quality-assurance mechanisms, ensuring that early judgement is applied consistently rather than informally.

- A transparent peer-feedback system enables HR to scan for emerging employee relations signals across teams, recognising that, as Head of People Gabrielė Zakaitienė notes, "these problems usually start very small."

- Exit interviews are treated as a formal risk control, used to identify patterns that may indicate future employee relations exposure rather than isolated dissatisfaction.

CYBER AND TECHNOLOGY

Cyber and technology risk has extended beyond a purely technical issue owned by specialists and managed through controls. As advanced technologies become more widely accessible and less predictable, risk is increasingly shaped by everyday behaviour and judgement, determining whether incidents are contained or escalate into enterprise-level crises.

> *What's being exploited by cyber criminals isn't principally technology, it's human beings exploiting human behaviour.*
>
> **Marcus Willett, Senior Advisor for Cyber,**
> **International Institute for Strategic Studies**

What's Changing?

Cyber risk is no longer defined by isolated breaches or technical failure, but mirrors the characteristics of modern risk: persistent, uncertain, widely distributed and shaped by everyday human judgement.

Cyber risk is increasingly treated as inevitable rather than avoidable.

It is shifting from something organisations seek to prevent entirely to something they must be prepared to absorb and recover from.

Cyber risk is increasingly unknown, unpredictable and unbounded.

When incidents occur, organisations rarely have immediate clarity on what has been compromised, how far impacts extend or how long recovery will take. The 2025 cyber-attack on Marks & Spencer, for example, only confirmed customer personal data loss weeks after initial operational disruption. Such issues are multi-domain, influencing areas like regulation and reputation simultaneously.

Significant cyber incidents often involve criminal activity and legal scrutiny, with impact extending beyond organisational boundaries as third parties and supply chains shape both exposure and recovery. These wider dimensions mean that cyber risk unfolds in public and human terms as well as technical ones, highlighting the importance of ethical decision-making as incidents evolve.

At our London event, Marcus Willett, Senior Adviser for Cyber at the International Institute for Strategic Studies, shared practical insights on how organisations can strengthen cyber resilience. Key takeaways included:

Cyber attacks frequently focus on senior executives because they hold high-value information and access. This means leaders must not only demand strong cyber discipline from others but also model higher standards than the rest of the workforce.

Cyber exposure through international travel and remote connectivity is often under-appreciated. While organisations may restrict laptops, smartphones are often overlooked despite providing access to sensitive systems or data. HR plays a key role in translating this risk into clear and practical safeguards, such as mandated VPN use or defined expectations for employees when travelling or working remotely.

Organisations should seek guidance from the National Cyber Security Centre and other trusted external sources. Cyber security is a team effort within organisations and across wider society, and resilience is strengthened by drawing on existing expertise or third-party support rather than managing cyber risk in isolation.

"

What makes cyber incidents so hard is the uncertainty. You do not know what you are dealing with, how long it will last, how much damage has been done, or how long recovery will take.

Maria Antoniou, Chief Human Resources Officer, Morgan Advanced Materials

"

The cyber-attack surface is now distributed across the workforce.

Access to powerful technologies and data is no longer confined to specialist teams. Risk is created wherever discretion and autonomy sit, often through tools and practices that fall outside formal oversight, including unofficial use of AI and digital workarounds. As a result, organisations are exposed to risks they may not fully see or control centrally.

AI has lowered the threshold for misuse and error.

It has reduced the skill required to create convincing phishing or automate mistakes, while also increasing the risk of unintentional data misuse. The result is a higher volume and pace of incidents, alongside greater difficulty distinguishing malicious intent from error or experimentation.

How Are Organisations Responding?

Organisations are increasingly shifting from cyber security models focused on breach prevention towards cyber resilience approaches that assume disruption and prioritise sustaining operations and decision-making when controls fail.

Defining cyber resilience through data that reveals how people behave under real conditions, not what they have been trained to know.

Organisations are moving beyond awareness-based training towards observing behaviour in practice. Unannounced phishing simulations and live incident-response exercises are increasingly used to surface how people actually respond under pressure. HR teams are using behavioural data, such as repeated credential failures, reporting delays and escalation speed, to assess genuine organisational readiness rather than assumed competence.

> "
> *You might be able to implement new technology systems, but if you do not have the skills in your organisation to be able to operate them you're going to come across and introduce new risks.*
>
> **Mark Hughes, Chief Security Officer, The National Lottery**
> "

> *You can do all the IT system monitoring in the world, but it does not matter unless you cultivate a culture where, if someone clicks on something by mistake, they feel able to report it immediately. The worst response is for someone to close their laptop and hope the problem goes away.*

Maria Antoniou, Chief Human Resources Officer at Morgan Advanced Materials

> *Quite often you find that, come the crisis, you'll get a CISO coming in who completely baffles the board with technical gobbledygook and is in return baffled by 'board-ese'. There's nobody there to translate between technical detail and board-level risk and decision-making. It needs someone in the middle. At the very least, the board should exercise its recovery process so that a real crisis is not the first time such translation is needed'.*

Marcus Willett, Senior Adviser for Cyber, International Institute for Strategic Studies

Treating silence as a greater risk than error.

Cyber risk escalates when people fail to speak up, not only when mistakes occur. When individuals hesitate to report incidents out of fear of blame, issues that could be contained quickly can escalate into enterprise-level crises. Containment depends on the deliberate cultivation of a 'speak-up' culture in which incident reporting is treated as a normal and supported part of how work is done.

Preparing leadership communication in advance for when controls fail.

Because cyber incidents unfold under uncertainty, organisations are increasingly preparing communication playbooks before incidents occur. Pre-agreed holding statements and escalation routes allow leaders to communicate clearly even when information is incomplete. Ongoing internal communication reduces the secondary risk created when employees are left to interpret events for themselves.

Positioning HR as a translator between technical risk and enterprise decision-making.

As cyber risk becomes a board-level concern, organisations increasingly need technical signals to be interpreted in ways leaders can act on. HR plays a critical role in aligning judgement and behaviour across the organisation when incidents unfold under pressure. In practice, this involves helping leaders understand what technical updates mean for people and operations, enabling coordinated action in conditions of uncertainty.

crf
CORPORATE RESEARCH FORUM

TALENT

Talent is no longer primarily a workforce planning challenge, but a source of structural enterprise risk shaped by long-term shifts in labour supply and the pace of technological change.

In this context, talent risk is not limited to shortages or capability gaps. It also includes the risk of missed opportunity when organisations lack the skills, experience or organisational capability required to enter new markets, develop new products or sustain innovation over time. In such cases, the cost of talent failure is not only operational strain, but the loss of future growth options and strategic relevance.

> *People are one of an organisation's most significant assets, and their management needs to be led — or at least jointly managed — by risk and HR.*
>
> **Julia Graham, CEO, Airmic**

What's Changing?

The talent landscape is being reshaped by constraints that restrict labour supply and reduce organisations' ability to adapt, increasing reliance on skills that are difficult to replace.

A shrinking and ageing workforce.

Demographic shifts are reducing overall labour supply while intensifying competition for experienced talent, making workforce availability a structural risk rather than a cyclical challenge. *The OECD Employment Outlook 2025* reports that the old-age dependency ratio across OECD countries has risen from 19 percent in 1980 to 31 percent in 2023, and is projected to reach 52 percent by 2060, exceeding 70 percent in several countries.

> *Too many experienced professionals have left the industry. Organisations are now struggling to find seniors who can sense-check outputs from AI systems and challenge errors or hallucinations.*
>
> **Julia Graham, CEO, Airmic**

Misalignment between education systems and employer needs.

Formal education and training pathways are not keeping pace with the skills organisations require, increasing reliance on in-house development and raising the cost and time required to build workforce readiness. The World Economic Forum's *Future of Jobs Report 2025* finds that, on average, 39 percent of workers' existing skill sets are expected to be transformed or become outdated.

Persistent shortages in critical skill areas.

Capabilities in digital, cyber, data and advanced technical domains remain scarce, concentrating risk within small populations and creating single points of failure inside organisations. The *UK Employer Skills Survey 2024* reports that 27 percent of vacancies were skill-short vacancies, while 12 percent of employers had at least one member of staff who was not fully proficient in their role.

The destabilising impact of AI on jobs and careers.

AI has the potential to reshape roles faster than organisations can redefine skills, career paths and workforce models, creating uncertainty about what capabilities are needed and how they should be developed. This uncertainty complicates workforce planning and increases risk exposure when capability gaps emerge faster than organisations can respond.

> "
> *To what extent are we recruiting for a job versus recruiting for a job and the potential to do future jobs?*
>
> **Jonathan Kohn, CPO, Bibby Line Group**
> "

> "
> *A major risk facing organisations is AI adoption and the associated skills gap, and the role of HR actively managing that is critical. Organisations are progressing at different speeds on this front, but HR's role is to stay one step ahead by equipping the workforce for what is coming.*
>
> **Furat Ashraf, Senior Partner, Bird & Bird**
> "

How Are Organisations Responding?

Organisations are responding to uncertainty by building resilience into how talent is planned, deployed and developed. The focus is shifting from prediction to preparedness, recognising that flexibility is now the primary defence against talent risk.

CRF has developed a framework for dynamic talent planning that helps organisations identify emerging talent risks and maintain multiple response options rather than relying on a single fixed plan.
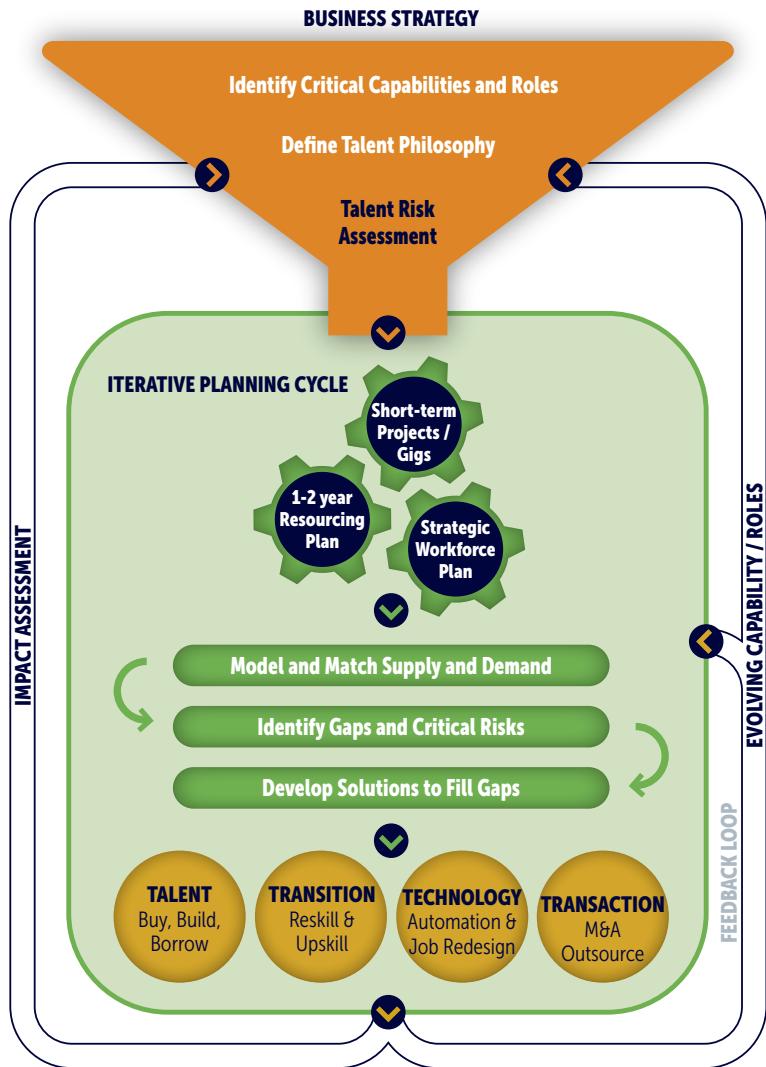
The framework has three elements:

- **First, alignment between business strategy and talent strategy.** This requires HR to be involved early in strategic discussions and to translate strategic choices into an understanding of the talent risks they create.

- **Second, an iterative approach to planning and action.** Talent planning is treated as an ongoing business conversation rather than an annual exercise. This allows organisations to test approaches, learn quickly and respond to risks as they emerge.

- **Third, a data-informed feedback loop.** This has two components. One focuses on impact assessment, using performance data and stakeholder input to understand what is working and adapt accordingly. The other focuses on bottom-up insight into how work is changing as AI tools are used in daily roles, and what this means for job design, capability requirements and people risk.

For further detail on the report and how to prepare your talent strategy for future risk, please click here »

Hostinger: Rethinking talent to protect future enterprise resilience

- Hostinger is committing to reinvest in early-career talent despite limited short-term operational need, acknowledging that AI and automation have materially reduced entry-level hiring need in recent years, and recognising the erosion of learning pathways as a long-term enterprise risk.

- Early-career hiring has been elevated to a company-level priority, with OKRs to recruit a small number of high-potential junior hires even where automation has reduced immediate demand.

- Selection has shifted away from task-based assessment toward learning agility, reflecting the speed at which roles and skill requirements are changing.

- The organisation uses the HERO framework (Hope, Efficacy, Resilience, Optimism) in hiring and L&D practices to assess whether individuals can sustain learning and judgement under uncertainty rather than demonstrate current task mastery.

- The emphasis is forward-looking, prioritising situational judgement capacity over proficiency in today's roles.

- The same logic applies to existing talent. Recognising that fears about AI can drive role protection, Hostinger encourages reinvention rather than preservation. Gabrielė Zakaitienė, Head of People, explains the paradox: "If you show proactivity in automating your role, you are more likely to have a future in our organisation."

> " *One of the risks we are spending more time on is the risk of 'silent quitting' in the context of fatigue. We're looking at change and individual burnout in the context of the resilience of the organisational resilience.* "
>
> **– Nicki Auret, CPO, ISBC, Standard Bank**

Bank of England: Building early insight into people-related risk

- The Bank of England has introduced a new HR capability called People Strategy and Insights.

- As Jane Cathrall, Executive Director for People, explains, "the focus of the team is on developing our people strategy using insights that we get internally and externally to put ourselves on the forefront of risks and opportunities that might be presenting themselves."

- The team prioritises surfacing concerns through direct conversations with teams before they appear in formal reporting.

- These qualitative insights will be combined with structured data, including engagement results, workforce composition and recorded incidents, in dashboards shared with HR and senior leaders.

- The aim is to build an early, forward-looking view of people-related risk that supports better judgement rather than retrospective reporting.

THE CONDITIONS, SIGNALS, ACTIONS FRAMEWORK

Although enterprise risk in modern organisations is increasingly unpredictable, it often follows a broadly consistent pattern. Risk tends to accumulate through organisational conditions, surface through early human signals and escalate or stabilise depending on the actions exercised under pressure.

This framework provides a practical lens through which HR leaders can engage with people-mediated risk, directing attention upstream of formal risk metrics while remaining aligned with established risk governance.

At its core, the framework helps HR leaders answer three questions:

- Where is risk building?
- How might it escalate?
- What actions should be taken?

Conditions

Conditions refer to the relatively enduring features of an organisation that shape how people operate and make decisions. They do not indicate that risk has materialised, nor do they describe decision-making in a crisis. Instead, they define the environment in which risk may accumulate over time.

Examples of relevant conditions include:

- **Decision architecture.** How authority for key decisions is formally allocated, including whether accountability is clearly defined when decisions cut across functions or levels.

- **Operating model and organisational design.** How work is structured across the organisation, including whether complexity or interdependence makes coordination difficult in day-to-day operations.

- **Resourcing and capacity assumptions.** The underlying expectations placed on teams in relation to workload and pace, independent of short-term performance pressures.

- **Incentive and performance frameworks.** The formal objectives and reward mechanisms that signal what the organisation prioritises in practice.

- **Governance and oversight arrangements.** How risk and performance are reviewed, including the regularity and depth of oversight.

Signals

Signals are the early indicators that suggest organisational conditions are beginning to strain. They do not identify root causes or prescribe responses. Instead, they provide evidence that risk may be accumulating and that closer attention is warranted. In practice, effective signals draw on both qualitative insight and quantitative data, brought together in a structured and consistent way.

Examples of relevant signals include:

- **Shifts in employee voice.** Changes in how concerns surface across the organisation, including patterns observed in tone and listening or survey insight.

- **Escalation patterns.** Evidence that issues are emerging later than expected or bypassing established routes, visible in case data and executive intervention logs.

- **Capacity pressure indicators.** Sustained increases in absence, turnover or overtime within specific roles, combined with qualitative reports of workload strain.

- **Reliance on key individuals.** Growing dependency on particular people to resolve issues or maintain continuity, visible through succession data and leadership feedback.

- **Employee relations activity.** Movement in grievance or dispute volumes, supported by qualitative insight into recurring themes or points of tension.
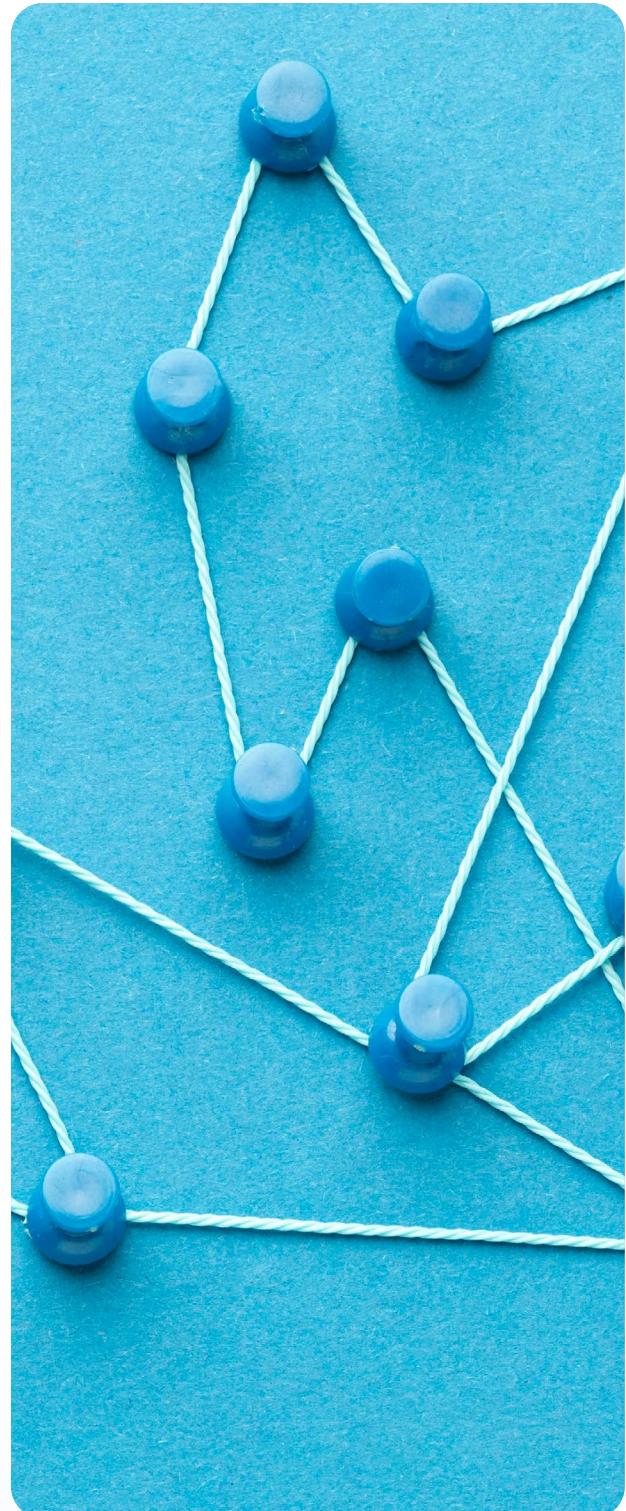
Action

Action refers to what decisions are made once risk begins to escalate. It is revealed through the choices organisations make under pressure

Examples of relevant actions include:

- **Speed and direction of escalation.** Whether issues are addressed promptly at the appropriate level or delayed while responsibility is debated.

- **Trade-offs made under pressure.** How leaders balance delivery, cost or speed against longer-term exposure when constraints tighten.

- **Use of authority in uncertain situations.** Whether decision-makers act within their mandate or defer decisions upward when consequences are unclear.

- **Response to challenge.** How dissenting views or uncomfortable information are treated when time or reputational pressure is high.

- **Consistency of decisions across similar situations.** Whether comparable risks are handled in similar ways or resolved differently depending on who is involved.

In some situations, escalation is immediate and organisations cannot afford the time to interpret conditions or assess early signals before acting.

In these moments, the quality of response depends more on what has already been clarified and agreed in advance.

HR's role in crisis readiness: a CSO perspective

At our London event, Mark Hughes, Chief Security Officer at The National Lottery, outlined how HR can help organisations prepare for crises by ensuring a small number of critical questions are answered in advance:

- What are the organisation's mission-critical activities?

- What do those activities depend on, across people, third parties, technology systems and data?

- How long could the organisation cope if one or more of those dependencies were disrupted?

- Is there a documented plan for sustaining critical activities during a crisis?

- Can that plan be accessed in practice if offices or systems are unavailable?

In practice, Hughes emphasised that this clarity must be matched by a **pre-established crisis team** and **clear accountability for internal and external communications** so that decisions and messaging do not stall.

CONCLUSION

Enterprise risk is increasingly shaped by intangible value and human judgement, yet many organisations still treat risk governance and people governance as separate disciplines.

While traditional risk frameworks remain essential for baseline control, resilience now depends on organisational readiness when information is incomplete and decisions must be made under pressure.

In this context, HR is not the owner of enterprise risk management as a system, but a critical contributor to risk capability by shaping the conditions that determine decision quality, surfacing early human signals and strengthening readiness across mission-critical activities.

The core shift is from managing risk on paper to building the people and leadership capacity to respond well when disruption arrives.

REFERENCES AND READING LIST:

Ibrahim, I. and Melhem, B. (2016). Impact of the Human Resources on the Risk Management and the Company Performance. International Journal of Economics & Management Sciences, 05(02). doi:https://doi.org/10.4172/2162-6359.1000320.

Ocean Tomo (2020b). Intangible Asset Market Value Study. [online] Ocean Tomo. Available at: https://oceantomo.com/intangible-asset-market-value-study/.

Guggenberger, P., Maor, D., Park, M. and Simon, P. (2023). The State of Organizations 2023: Ten shifts transforming organizations | McKinsey. [online] www.mckinsey.com. Available at: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-state-of-organizations-2023.

AON (2025). Top 10 Global Risks | Global Risk Management Survey. [online] Aon. Available at: https://www.aon.com/en/insights/reports/global-risk-management-survey/top-10-global-risks?collection=18a5358e-4f8c-4e2d-8fb3-291c7672dfaa&parentUrl=/en/insights/reports/global-risk-management-survey#aon-collection-detail-item- [Accessed 18 Jan. 2026].

Bremen, J.M. (2025). Why Are More CHRO's In Board Rooms Today? People, Risk, And More. Forbes. [online] 29 May. Available at: https://www.forbes.com/sites/johnbremen/2025/05/29/why-are-more-chros-in-board-rooms-today-people-risk-and-more/.

Shai Ganu (2025). Beyond the balance sheet: Human capital as an asset. [online] WTW. Available at: https://www.wtwco.com/en-ke/insights/2025/11/beyond-the-balance-sheet-human-capital-as-an-asset [Accessed 27 Jan. 2026].

CIPD. (2023). CIPD | FTSE 350 firms risk reputational damage with 'people insight deficit' on boards. [online] Available at: https://www.cipd.org/uk/views-and-insights/thought-leadership/cipd-voice/reputation-risk-boards/.

Tonello, M. and Tonello, M. (2025b). The Evolving Role of the CHRO in the Boardroom. [online] The Harvard Law School Forum on Corporate Governance. Available at: https://corpgov.law.harvard.edu/2025/05/08/the-evolving-role-of-the-chro-in-the-boardroom/.

Recruiter.co.uk. (2019). How to respond to rise of AI-generated workplace grievances | Recruiter. [online] Available at: https://www.recruiter.co.uk/news/2025/11/how-respond-rise-ai-generated-workplace-grievances [Accessed 27 Jan. 2026].

Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, [online] 132, p.103372. doi:https://doi.org/10.1016/j.cose.2023.103372.

CRF. (2025). Future-Ready Talent Management

OECD. (2025). OECD Employment Outlook 2025: Full Report. [online] Available at: https://www.oecd.org/en/publications/2025/07/oecd-employment-outlook-2025_5345f034/full-report.html.

World Economic Forum (2025). The Future of Jobs Report 2025. [online] World Economic Forum. Available at: https://www.weforum.org/publications/the-future-of-jobs-report-2025/.

Department for Education (2025). Employer skills survey: 2024. [online] GOV.UK. Available at: https://www.gov.uk/government/statistics/employer-skills-survey-2024.

RESEARCH PARTICIPANT LIST:

Alison O'Connor, Chief People Officer, Arriva

Julia Graham, CEO, Airmic

Nick Dalton, Former EVP HR, Unilever

Orla Leonard, Senior Partner, RHR

Jane Storm, CPO, Insurance, Wealth & Retirement, Aviva

Furat Ashraf, Partner, Bird & Bird

Gabrielė Zakaitienė, Head of People, Hostinger

Marcus Willett, Senior Advisor for Cyber, International Institute for Strategic Studies

Maria Antoniou, Chief Human Resources Officer, Morgan Advanced Materials

Mark Hughes, Chief Security Officer, The National Lottery

Jonathan Kohn, CPO, Bibby Line Group

Nicki Auret, CPO, ICBC Standard Bank

Jane Cathrall, Executive Director for People, Bank of England

Professor Elmar Kutsch, Professor of Risk Management, Cranfield University

SCENARIO PLANNING TEMPLATES: DRIVER MAPPING AND POLARITY MAPPING

The following is a summary guide of scenario planning frameworks presented by Professor Elmar Kutsch at our event, outlining how the key concepts and tools may be applied in practice.

Scenario planning is a way to deal with uncertainty when traditional forecasting and probabilistic risk analysis are not enough. Instead of trying to predict one future, it explores several realistic and evidence-based possibilities to understand how different conditions could affect outcomes.

Step 1: Define a strategic problem.

Scenario planning begins by defining a strategic problem. The problem is defined from the perspective of stakeholders, clarifying not only what is happening, but why it matters, to whom and under what conditions.

It is framed in negative terms, focusing on what is going wrong or could plausibly go wrong, as per Kutsch's example: "Key stakeholders are beginning to disengage from the transformation programme, and early signs of resistance are emerging in critical business units."

Step 2: Identify potential drivers of change

The next step is to identify drivers, which are the factors that could influence how the strategic issue develops over time. These drivers can come from inside or outside the organisation and are usually not fully within managers' control. Examples include political and regulatory changes, technological developments and internal factors such as staff turnover or leadership alignment. The aim at this stage is to identify a wide and inclusive range of drivers.

Step 3: Assess and plot drivers using the Uncertainty-Uncontrollability framework.

To prioritise drivers for scenario development, each driver is assessed along two dimensions.

Uncertainty describes how hard it is to predict how a driver will affect the strategic problem in the future.

A driver is highly uncertain when its direction or impact is unclear, when there is little past experience to draw on, or when different stakeholders interpret it in different ways, for example public sentiment toward organisational restructuring.

Uncontrollability refers to the extent to which the organisation lacks the ability to directly influence how the driver develops.

Highly uncontrollable drivers cannot be meaningfully steered, even if their effects can be anticipated or managed, for example the introduction of new statutory employment requirements.

The drivers are then plotted on a matrix based on their relative levels of uncertainty and uncontrollability. Drivers that are both highly uncertain and highly uncontrollable appear in the top-right quadrant of the matrix. These drivers are not suitable for prediction-based planning and therefore become the focus of scenario development.
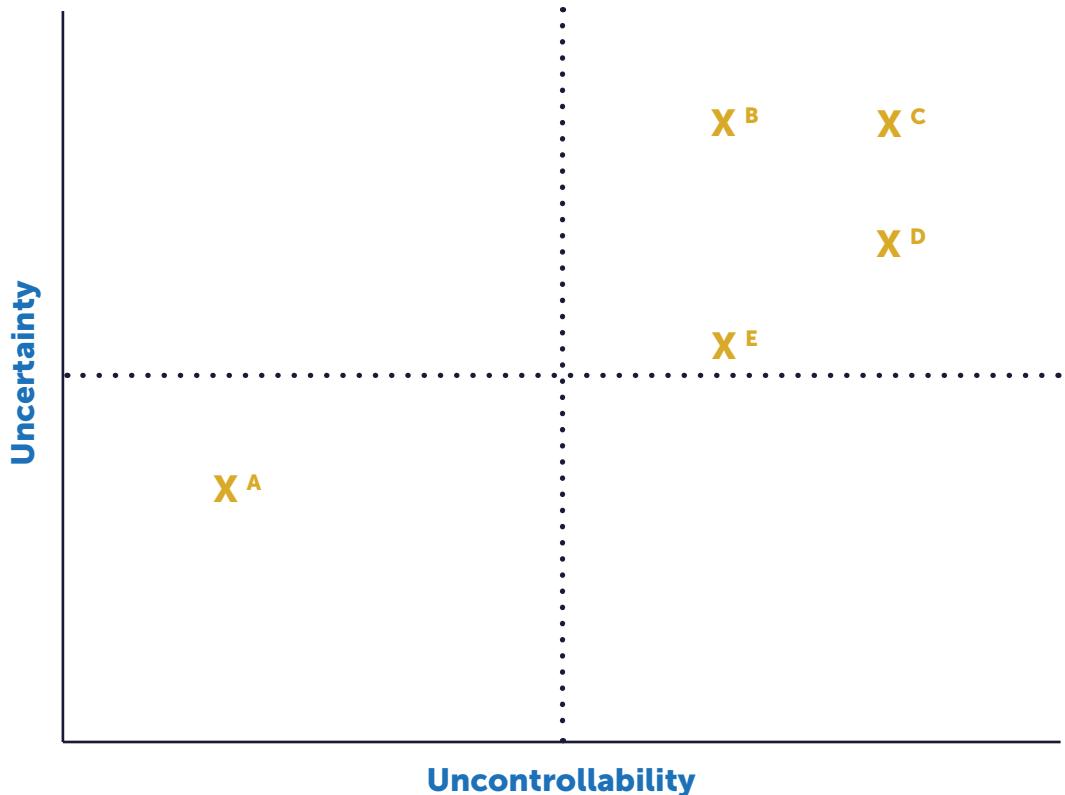

Step 4: Select two critical drivers and define plausible extremes

From the drivers that fall in the high-uncertainty and high-uncontrollability quadrant, two are selected that are both highly influential and sufficiently distinct to create clearly different futures.

For each of these drivers, two opposing but plausible extremes are defined. These extremes reflect meaningful differences in how the future could unfold, rather than idealised best- or worst-case scenarios.

Step 5: Construct the polarity map

The two selected drivers are placed on perpendicular axes to create a four-quadrant map. Each quadrant represents a distinct scenario. These scenarios are not forecasts. They are thinking tools designed to expand strategic thinking beyond linear or single-future assumptions.

Extreme Positive C

Scenario 2 | Scenario 1

Extreme Negative B — **Extreme Positive B**

Scenario 3 | Scenario 4

Extreme Negative C
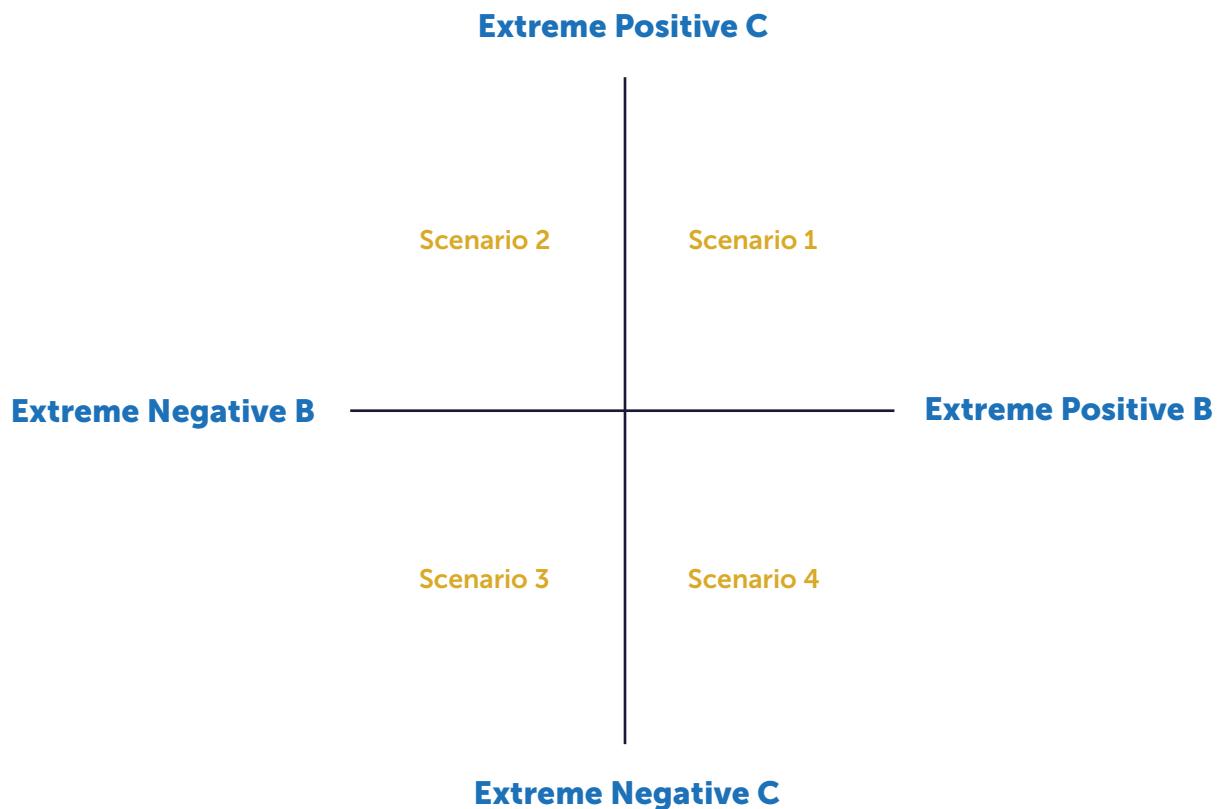
Step 6: Develop scenario narratives

For each scenario, a narrative is developed to bring the future into view. Scenario narratives translate abstract drivers into situations that show how people, organisations and strategies might be affected.

Each scenario narrative typically:

- has a clear and memorable name
- describes the broader environment created by the interacting drivers
- explores changes in stakeholder power, relationships, and behaviour
- clearly links back to the original strategic problem
- ends with a strategic question or challenge that connects the scenario to present-day decision-making

Step 7: Use scenarios to inform strategic action

The value of scenario planning lies in how the scenarios are used. By considering multiple plausible futures, organisations reduce their reliance on a single forecast and improve their ability to notice emerging change.

Scenarios can be especially useful in revealing areas where teams may be overly confident, where assumptions go unchallenged and where blind spots exist.