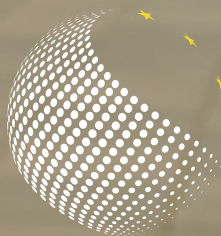


NEXT



New EXposure Trends
Report 2025



FERMA

Anticipating changes
Shaping the future



Content

FOREWORD	04
<hr/>	
1 - Short-termism and bias: Blind spots when considering emerging risks	06
<hr/>	
2 - Overcoming short-termism and bias in risk management	09
<hr/>	
3 - Risks facing Europe	12
3.1 - Geopolitical risks and the future of the European Union	14
3.2 - Technological acceleration; navigating the rapids of change	18
3.3 - Climate change risk	23
3.4 - Human capital risks; reshaping the future of business	26
<hr/>	
END NOTES	29
<hr/>	
MEMBERS OF THE FORESIGHT COMMITTEE	30
<hr/>	

FOREWORD

Today's risk environment is characterised by dynamic and evolving threats and opportunities. Recent and current events highlight just how quickly things can change and how the factors affecting organisations' ability to operate, trade and grow never remain static.

Against that backdrop, organisations are increasingly aware of the need to build resilience, to be ready to anticipate and be prepared to tackle uncertain and evolving threats using foresight capabilities. Foresight has been highlighted by both the Organisation for Economic Cooperation and Development (OECD) and the United Nations' Summit of the Future as a discipline that will be vital for organisations to complement traditional risk management to navigate the challenges ahead.

As well as 'known knowns', those current and near-term threats that Risk Managers deal with on a daily basis, and 'known unknowns', those strategic risks voluntarily accepted by companies to generate returns, organisations are facing a series of 'unknown unknowns'.

Those 'unknown unknowns' are uncontrollable, sudden and unexpected shocks. They are the surprises that might occur in ten years' time that may, as yet, be overlooked, unrecognised or insufficiently analysed.

All too often, the short-termism and bias in the thinking of Risk Managers, the organisations they work for and the governments and regulators whose activities affect their business operations mean that emerging risk trends may be overlooked. This, in turn, hampers long-term risk management strategies and means that the approach to emerging risk trends is too often reactive rather than proactive.

FERMA wants to equip Risk Managers and their companies to prepare for those risks often referred to as 'Black Swan' events; events that are unforeseen or unexpected but which have dramatic, potentially far-reaching effect, or 'Grey Rhinos'; events that are high impact and highly probable, but which are often ignored or overlooked until it is too late. We also want to highlight them to our insurance industry partners and to the European authorities and beyond to foster a culture of collective long-term thinking and preparedness.

The Foresight Committee was set up to give meaningful insights on emerging topics for FERMA and our members. This paper, the fruit of the exchange of views by the Foresight Committee, provides thoughts and actionable recommendations that will guide FERMA's activities in 2025 and serve as a foundation for future discussions with key stakeholders and in our advocacy work.



► **Philippe Cotelle,**
FERMA Board Member
and Chairperson of the
Foresight Committee



► **Charlotte Hedemark,**
President of FERMA



Our goal is to establish Risk Managers as leaders in risk foresight and as enablers of opportunity, to contribute to the elevation of the standing of our profession and to ensure its voice is heard in turbulent times. ”

With that aim in mind, last year we established a Foresight Committee, made up of recognised European experts with international experience from outside of our immediate scope of stakeholders.

The report is intended to be a reflection tool for Risk Managers and to help them to become more future-focused. We hope it will encourage and enable Risk Managers to think about the mid-to-long term threats to their companies, to the societies in which they live and work and to the European economy. This paper will initiate internal discussions in our members' organisations as well as provide practical guidance that will equip Risk Managers with tools to assess these risks in a dynamic fashion and adopt proactive strategies to managing them.

For the first iteration of this report, we identified four global, interconnected and potentially systemic trends of crucial relevance to European Risk Managers and their organisations in the next ten years. Those trends are, in no order of importance: geopolitical shifts; technological acceleration; climate change; and human capital.

In this paper you will read thoughts on those topics from a variety of international experts with legitimacy and expertise in fields outside of the risk and insurance world. The Foresight Committee does not necessarily provide a consensus view, but its work is intended to stimulate further debate and give Risk Managers ideas to consider on these emerging and evolving risk areas.

This report, New EXposure Trends – or NEXT, is intended to be food for thought and to inspire continued discussion and new ways of thinking about these emerging risk areas and how to overcome the short-termism and bias inherent in the decision-making of many organisations today.

With thanks to the members of the first Foresight Committee who have contributed to this report: **Typhaine Beaupérin**, CEO of FERMA; **Professor Bruno Colmant**; **Philippe Cotelle**, FERMA Board member and chairperson of the Committee; **Paulino Fajardo**, Head of Disputes for Europe, Middle East and Africa, **Herbert Smith Freehills LLP**; **Charlotte Hedemark**, President of FERMA, Risk Management Expert, Field Risk Management, SAP; **Daria Krivonos**, CEO, Copenhagen Institute for Futures Studies; **Sean Lyons**, Corporate Defense Authority, Writer, and Speaker, Consultant; and **Sebastian Wieczorek**, CEO, Mantix.

The Foresight Committee is not a closed club, it is a living entity to which we hope to attract experts from other fields to discuss and examine future trends. This report is, therefore, the first of many. We aim to enrich the debate and provide thought-provoking insights for our Risk Management community, our insurance and broking partners and the European authorities with whom we communicate on these emerging trends.

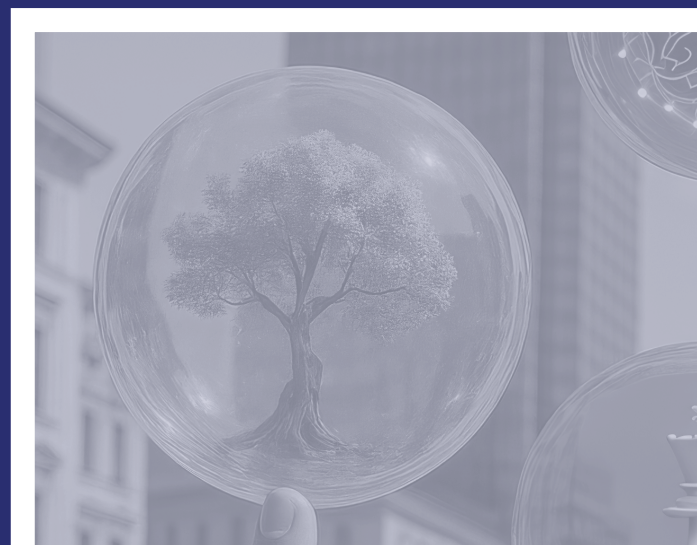
1

Short-termism and bias: Blind spots when considering emerging risks

In the current climate of accelerating change and uncertainty, strategic foresight is indispensable for Risk Managers. The past few months have underlined the speed at which situations can escalate and risks emerge and evolve. Yet, despite the increasing dynamism and complexity of global challenges, decision-makers often fall prey to short-term thinking and cognitive biases that hinder their ability to anticipate and mitigate emerging risks. This can lead to strategic blindness. At a time when there is a widespread sense of existential threats on the horizon, this sense of foreboding often can – ironically – exacerbate a human tendency to be reluctant to think too far into the future and instead to focus on the short-to-medium term.

It is vital, however, that Risk Managers are equipped with tools to help them look further into the future, to help their organisations to be better prepared to address risks – however rapidly they change and unexpected they might previously have appeared.

Here we explore the systemic barriers that prevent effective long-term risk management, highlighting the role of cognitive biases and structural constraints in shaping an approach that is too often reactive rather than proactive.



1.1 THE PITFALLS OF SHORT-TERMISM IN RISK MANAGEMENT

Short-termism—the tendency to prioritise immediate gains or agendas over long-term resilience—is deeply embedded in corporate and governmental decision-making. This is particularly problematic in Risk Management, where emerging threats often develop over extended time horizons. These threats are sometimes referred to as ‘Grey Rhinos’; hazards of high probability and high impact but which are not addressed until the risk is actually upon us. The focus on quarterly financial results, election cycles and immediate operational concerns leaves organisations ill-prepared for disruptive events and slower-moving systemic risks such as climate change, demographic shifts and technological disruption. It is a particularly unfortunate tendency given that the nature of emerging risks and trends actually often leaves ample room to identify, monitor and mitigate these threats. This short-term focus is usually driven and exacerbated by:

► Market pressures:

Investors and shareholders often prioritise short-term returns, discouraging investments in long-term resilience.

► Regulatory and political constraints:

Policies and regulations frequently operate within short electoral cycles, limiting the ability to enact long-term risk mitigation strategies.

► Operational priorities:

Organisations often focus on crisis response rather than scenario planning, leaving them vulnerable to unforeseen disruptions. We spend our time on the ‘what now?’ rather than the ‘what if?’ conversations.

1.2 COGNITIVE BIASES THAT CLOUD DECISION-MAKING

In addition to the market and governance forces that erode long-term thinking, cognitive biases play a significant role in reinforcing the focus on the short-term. Research in behavioural economics and strategic foresight has identified several key biases that impede effective risk planning:

► Status Quo bias:

Decision-makers tend to resist change, preferring familiar solutions over novel but necessary adaptations. This can lead to inaction in the face of emerging risks.

► Confirmation bias:

Organisations often seek information that supports their existing views, ignoring evidence that contradicts their preferred strategies.

► Optimism bias:

Many leaders overestimate their ability to manage risks, underestimating the probability of disruptive events. Sometimes, we even acknowledge the risk but somehow think we will be exempt from its effects.

► Availability Heuristic:

Decision-makers give disproportionate weight to risks they have recently encountered or that are widely publicised, while neglecting less visible but potentially more significant threats. This is especially true for emerging risks, which by their nature are less visible early on, but can easily be identified, if one's focus and risk governance allows it.

► Persistence of discredited beliefs:

Even when presented with evidence that contradicts existing assumptions, organisations and policymakers may continue adhering to outdated strategies, leading to a failure to adapt.

► Group Think:

Often a group prioritises consensus and harmony over critical evaluation and diverse perspectives. Dissenting opinions are often suppressed, leading to decision-making that lacks rigorous scrutiny and fails to consider alternatives. This phenomenon, often referred to as “herd mentality” or ‘following the bandwagon’, can result in a collective lack of focus on emerging risks and over-confidence in the agreed plan.



1.3 THE CONSEQUENCES OF FAILING TO ADDRESS BIASES

The failure to recognise and mitigate these biases has real-world consequences. Recent events, such as the global shortage of semiconductors stemming from the concentration of producers, or the energy supply constraints in mainland Europe caused by geopolitical turmoil, highlight the dangers of underestimating emerging risks. In many cases, these crises are not unforeseen. Warning signals are often visible but overlooked or dismissed due to cognitive biases and short-term incentives or priorities.

1.4 THE SYSTEMIC RISK CONTEXT

In today's interconnected, dynamic and uncertain environment, organisations need to consider threats and opportunities in the context of systemic risk. Systemic risk, whereby a crisis causes the breakdown of an entire system not just one of its constituent parts, can result in a severe global economic downturn.

The current geopolitical climate could give rise to unprecedented systemic economic risks as the world shifts toward a multipolar landscape defined by technological, climatic and territorial rivalries. These threats, rooted in the interdependence of financial, commercial, and energy systems, cannot be mitigated through diversification because they will simultaneously impact all economic actors on a global scale. Their unpredictability and magnitude will exceed traditional adaptation capacities, exposing economies to shocks of universal scope.

Systemic risks could take the form of, among other things; a cyber war that could cripple financial markets within hours; a water conflict that could trigger a global food crisis; technological blockades that could paralyse worldwide trade; or a conflict over resources that could trigger disruption to energy supplies just as the world is grappling with the strain of the energy transition.

A foresight approach could help Risk Managers to understand and prepare for the effects of systemic risk on their organisations and the markets in which they operate.

2

Overcoming short-termism and bias in risk management

To build more resilient organisations and societies, Risk Managers must adopt a long-term perspective and actively counter cognitive biases. This can be done by:

► **Embedding strategic foresight:**

Organisations should consider integrating foresight practices such as scenario planning, trend analysis and horizon scanning into their decision-making processes to anticipate and prepare for future risks. This should be done in a governance framework that separates long-term risk processes from short-term operational risk management.

► **Cultivating a culture of long-term thinking:**

It is of great benefit if organisational leadership champions a forward-looking mindset, emphasising the value of proactive risk management over reactive crisis response.

► **Redefining metrics:**

Moving beyond short-term financial metrics to include long-term resilience and adaptability as key performance indicators.

► **Leveraging technology:**

AI-driven analytics and predictive modelling can enhance risk detection and provide objective insights that mitigate human biases.

► **Undertaking regular critical reviews** with peers of the parameters used to establish strategic targets, to avoid biases

► **Employing holistic thinking** and developing greater awareness of how risks can be intertwined, interconnected and interdependent.

The future is not an abstract concept but a tool that can and should be used to make informed decisions today. Most Risk Managers recognise the limitations of short-termism and the narrow operational focus on known risks but lack the tools or support to devote time and organisational attention to the emerging risk landscape. This paper proposes that by adopting strategic foresight methodologies and fostering a culture of long-term thinking, organisations can enhance their resilience and better navigate an increasingly uncertain world.

2.1 FORESIGHT IN RISK MANAGEMENT

In recent years, foresight has emerged from the field of strategic planning as a distinct and formal discipline. It is now increasingly recognised as a core competency requirement in many organisations. Some have even established new roles, such as Chief Foresight Officer. This underscores the relevance of the discipline and the importance that many large organisations attach to it.

Strategic foresight considers medium-to-long-term time horizons; the aim is not to predict the future. Rather, at a time when forecasts, projections and linear decision-making methods are not enough, strategic foresight aims to achieve a view of how the future might appear in the form of new assumptions, behaviours and realities.

The starting point for practising foresight, therefore, should always be to challenge the tendency to favour a 'business as usual' future and instead to explore viable alternatives. This approach can certainly enable more effective preparedness and future-proofing, but it requires a future-thinking mindset.

In an increasingly dynamic environment, as foresight becomes more mature as a discipline we are seeing foresight frameworks, methodologies and tools evolve as innovative approaches develop. Traditional risk management has always involved elements of hindsight, insight and, to a degree, foresight to help analyse the probability and impact of identified risks. However, many of today's major emerging risks could potentially have been avoided, prevented or at least minimised if a foresight approach had been adopted. This not only applies to the four emerging risk trends outlined in this report, but – crucially – will also apply to those risks appearing on the horizon. Future-focused Risk Managers would benefit from adopting a foresight approach to their toolkit and scope to be better equipped to assess how risk assumptions, parameters and dimensions should be viewed going forward.

Risk foresight involves adopting a scientific and systematic approach to applying foresight techniques in risk management. And this is particularly true in the case of identifying and managing emerging risks. A foresight focus can help Risk Managers to be better prepared to deal with surprises posed by the Volatility, Uncertainty, Complexity and Ambiguity (VUCA) environment of the 21st century.

This FERMA *NEXT* report provides examples of foresight tools that are available for forward-looking risk professionals when considering and addressing emerging risks.

2.2 STRATEGIC RISK MANAGEMENT TOOLS TO ADDRESS EMERGING RISKS

Risk Managers employ various methodologies to address the emerging risks facing their organisations.

These tools, often used in combination with one another, can be used to help Risk Managers spot emerging trends, assess their potential impact and put in place strategies to manage, mitigate and transfer some of their effects.

The most widely used techniques include:

► 1. Scenario planning

- **Purpose:** Helps organisations explore multiple plausible future scenarios and prepare for uncertainty.
- **How it works:** Develops narratives based on key uncertainties and assesses their potential impact on strategy.

► 2. Horizon scanning

- **Purpose:** Systematically tracks early signals of change across industries, technologies, regulations, and societal trends.
- **How it works:** Uses sources like research papers, patents, expert opinions and trend databases to detect weak signals.

▶ 3. Bowtie analysis

- **Purpose:** Provides a **visual representation** of risk causes, consequences, and controls, allowing organisations to identify leading indicators of emerging risks, explore and perhaps manage vulnerabilities by mitigation measures.
- **How it works:** Divides risk analysis into **causal factors** (on the left) leading to an event (in the centre) and **consequences** (on the right), with preventive and recovery measures mapped accordingly.

▶ 4. Leading indicators for risk detection

- **Purpose:** Identifies measurable and trackable (not necessarily quantitative) key performance indicators (KPIs) that serve as early warnings of emerging risks.
- **How it works:** Focuses on **proactive risk management** by analysing data trends and detecting anomalies before a crisis unfolds.

▶ 5. The futures wheel

- **Purpose:** Helps organisations **map the ripple effects** of a particular trend or event to better understand its cascading impact.
- **How it works:** Starts with a central issue (e.g. AI adoption in finance) and branches out into first-order, second order, and third-order consequences, uncovering interdependencies and contagion risks.

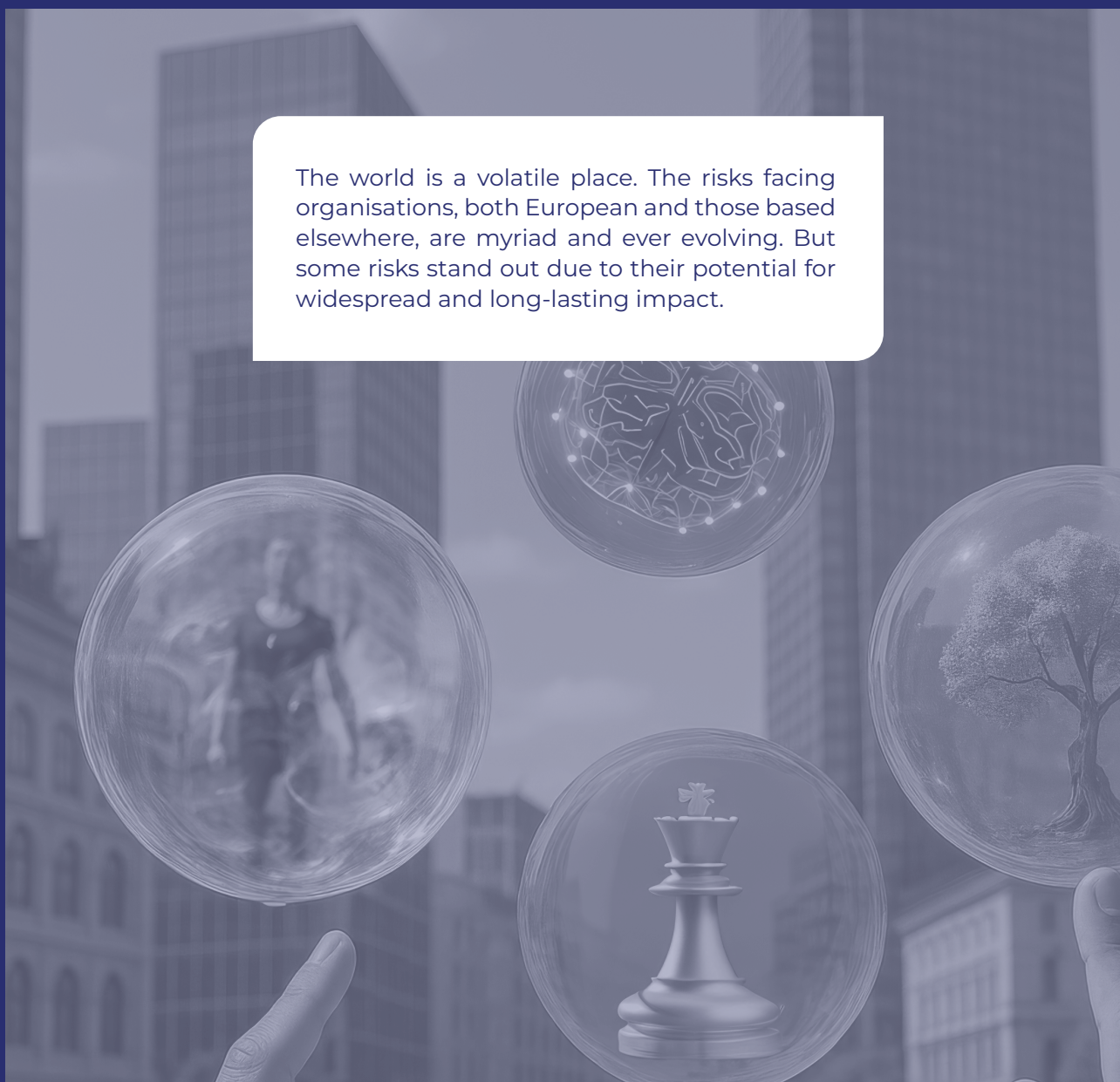
In this report, we will discuss some of the key risks facing European companies today and in the future, and explore potential applications of selected tools from this list.

Each trend will be illustrated by a 2x2 scenario matrix. Such tools can help prepare for the very different future pathways of a risk. A scenario matrix is constructed by using two key uncertainties that will significantly shape the risk landscape for European companies.

3

Risks facing Europe

The world is a volatile place. The risks facing organisations, both European and those based elsewhere, are myriad and ever evolving. But some risks stand out due to their potential for widespread and long-lasting impact.



The FERMA Foresight Committee has highlighted four critical areas that will demand particular attention for the years to come. These risks, described in more detail throughout this report, are:

► **Geopolitical Shifts:**

The global political landscape is undergoing a period of significant transformation, with rising tensions, shifting alliances and the emergence of new global powers. These changes create uncertainty and instability, affecting trade, investment and supply chains.

► **Technological Acceleration:**

Rapid advancements in technology, particularly in areas like artificial intelligence (AI), automation, and biotechnology, are transforming industries and societies at an unprecedented pace. While these advancements offer opportunities, they also present challenges, including the potential for job displacement, ethical dilemmas, a

decline in European competitiveness and increased cybersecurity risks.

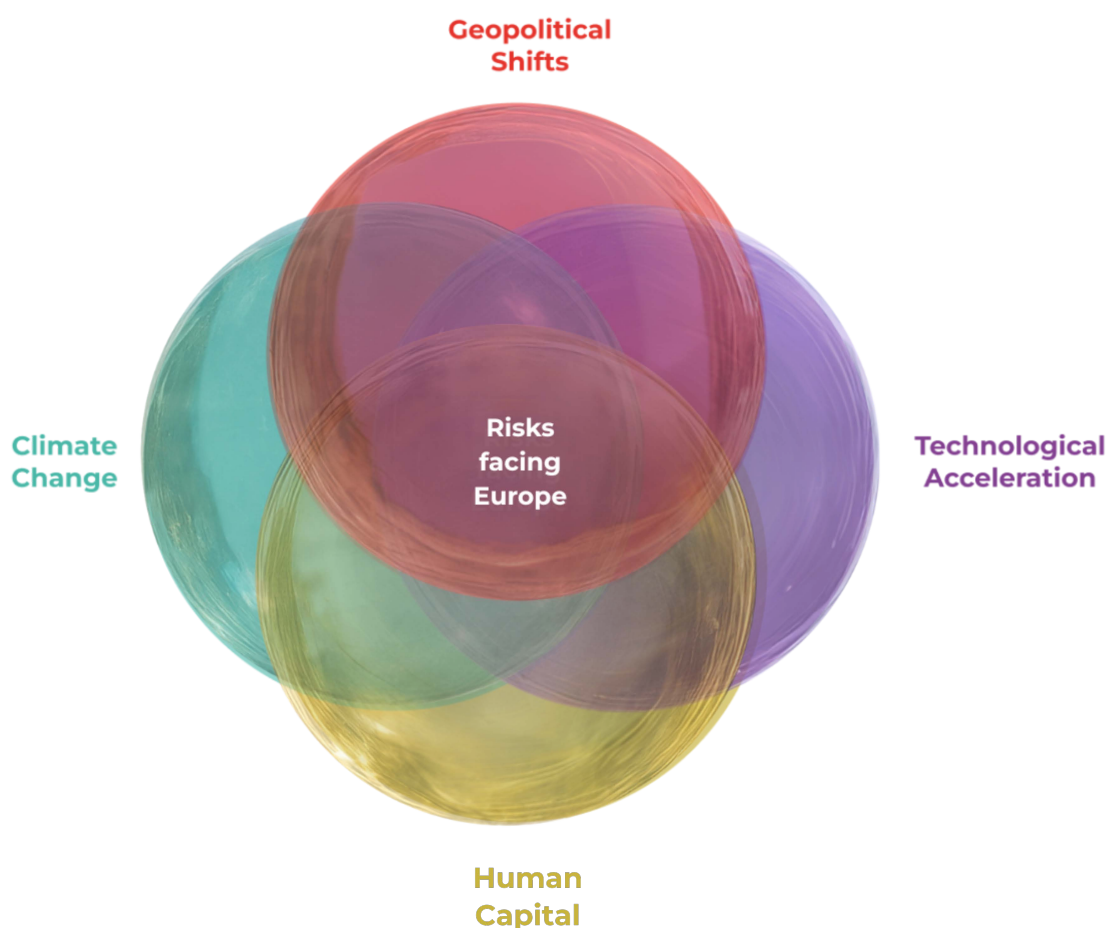
► **Human Capital:**

Attracting, developing, and retaining talent is becoming increasingly challenging in a rapidly changing world. Demographic shifts, evolving skills requirements and changing employee expectations require organisations to rethink their approach to managing human capital.

► **Climate Change:**

The impacts of climate change, including extreme weather events, rising sea levels and resource scarcity, pose significant risks to businesses, the insurance landscape and society as a whole. Organisations are aware that they must adapt to these changes and contribute to mitigating their impact.

These four areas represent interconnected and complex challenges that will shape the risk landscape for years to come.





3.1 | GEOPOLITICAL RISKS AND THE FUTURE OF THE EUROPEAN UNION

The European Union faces a complex and evolving geopolitical landscape fraught with challenges that could significantly impact its future stability and prosperity. These risks stem from various sources, including weakened global governance structures, shifting international alliances and the rise of new global powers. This chapter will explore some of the key geopolitical risks confronting the EU and their potential implications.

Multilateralism and Global Governance Challenges

The existing multilateral system is facing significant strain. Institutions like the United Nations are often rendered ineffective by power imbalances and a lack of consensus among major players. This weakness in global governance is further exacerbated by geopolitical flashpoints such as the conflicts in Gaza and Ukraine, which have highlighted the lack of enforcement mechanisms within multilateral institutions. The complexities surrounding the regulation of technology, and particularly artificial intelligence (AI), are adding to the list of things that keep leaders and policy-makers awake in 2025. These issues demand international cooperation, yet solutions remain elusive, increasing the risk of escalation, meaning low predictability in planning and further instability.

Adding to these uncertainties are the changes that the new US administration is bringing about in terms of significant shifts in foreign policy and national priorities, further disrupting international cooperation on critical issues like climate change, trade and global security. Such changes could have far-reaching consequences for the European Union, undermining its ability to address its own internal challenges, as well as its capacity to navigate and weather regional and global shifts. EU solidarity may also be impacted by the fact that only certain member states are involved in discussions at G7 and G20 levels.

EU and US Decoupling

The transatlantic relationship, a cornerstone of European security and stability for decades, is facing growing uncertainty. The recent and abrupt shift in US foreign policy, particularly regarding its commitments to the historically strong US-Europe alliance as well as its stance on Ukraine and Taiwan, could create a power vacuum with significant implications for the global (dis)order. This could result in new security and intelligence risks due to the European Union's lack of access to Five Eyes Intelligence briefings. These dynamics are compounded by a growing trend of bilateral agreements between the United States and individual European countries, bypassing the European Union as an institution and potentially weakening its collective bargaining power.

Furthermore, there is a growing perception within Europe that the US may pose a threat to EU stability. This sentiment is fuelled by the early signals from President Trump, which have exacerbated concerns about potential US disengagement from international commitments and a more unilateralist and aggressive foreign policy approach. Such a shift, combined with the tense political dynamics in some of the largest European countries, could leave the European Union increasingly vulnerable.

The Future of the European Union

In addition to the external shifts, the European Union faces internal challenges that could further complicate its response to external pressures. The rise of populism and nationalism across Europe poses a threat to democratic institutions and the European project itself.

These dynamics are coinciding with concerns about the declining global influence of the European Union. Economic stagnation and lagging innovation, coupled with political fragmentation, has weakened the European Union's standing on the international stage.

This decline is particularly evident in the context of rising global powers like China and the North-South recalibration of the 21st century, which are increasingly altering the established institutions and rules of engagement of the last century. The ongoing development of BRICS+ as an increasingly coherent grouping will present its own challenges. A rebalancing is not necessarily a negative development in itself, but any transition of such magnitude has the potential to create instability.

The European Union's over-reliance on its transatlantic allies means that changes in the foreign policy priorities of those allies could leave it exposed and without adequate capacity to address emerging security challenges. This dependence underscores the urgent need for the European Union to strengthen its collective capacity-building efforts, including joint investments in defence and strategic technologies.

Deglobalisation, Technological Shifts and Geopolitical Tensions

The general trend of deglobalisation presents further challenges. Increased barriers to trade and investment create difficulties for European companies seeking to diversify their operations and manage risks. This trend also threatens the nation-state structures that underpin the European project, as market economies prioritise competition over solidarity. And the sheer size and influence of large companies potentially exacerbates social and economic inequalities.

The escalating tensions between the United States and China, further fuelled by the United States' increasingly confrontational rhetoric, risk further destabilising the global economy before an orderly power rebalance can occur, pushing the two regions closer to a new Cold War scenario. This rivalry could have significant consequences for the European Union, forcing it to choose sides or navigate a complex web of competing interests.

The very real threat that respect for international law could be further undermined and diminished, and the potential shift away from the prevailing rule-based international order, may present additional challenges for the European Union.

War and Geopolitical Instability

The threat of war and geopolitical instability looms large. The conflict in Ukraine and the fragile peace agreement in the Middle East highlight the fine line between order and chaos and the potential for rapid escalation. These conflicts also underscore the importance of strong legal frameworks and diplomatic cooperation to enforce international rules and prevent further violence. So far, the regulatory frameworks and international bodies have come up short on any meaningful enforcement. European defence strategy is also likely to be further complicated by NATO's strategy given the intersection of EU and NATO membership.

The increasing use of economic sanctions as a foreign policy tool adds another layer of complexity. While sanctions can be effective in exerting pressure on target countries, they also have unintended consequences, disrupting global trade and investment flows and impacting businesses operating in affected regions.

Furthermore, the increased targeting of critical infrastructure by cyberattacks and physical damage poses a significant threat to European security. The digitalisation of societies and economies increases the potential impact of cyber warfare. A uniform global approach to cyber crime is needed, to ensure efficient prosecutions that may act as a real deterrent to criminals.

Finally, the potential for currency wars and instability in the global financial system adds to the economic risks facing the European Union. These risks are further compounded by the fragile position of Russia. While no major power benefits from a complete destabilisation of Russia, the potential for unintended consequences remains a significant concern.

To sum up, the European Union faces a multitude of geopolitical risks that could significantly affect its future. Addressing these challenges will require strong leadership, effective international cooperation, and a renewed commitment to strengthening the European Union's collective capacity to act decisively in the face of growing global uncertainty.

KEY RISK MANAGEMENT TAKEAWAYS

• Expand resilience-planning for extreme scenarios:

Business continuity plans must now account for high impact geopolitical risks that were once considered unlikely, such as democratic destabilisation in Europe, conflict with Russia or nuclear escalation. These scenarios should be stress-tested and integrated into contingency and recovery strategies.

• Embed geopolitical risk into strategic decision-making:

Risk Managers should work closely with leadership and external partners to ensure that geopolitical risk is central to strategy and risk frameworks. This includes: challenging regional biases with diverse geopolitical perspectives; using real-time intelligence and expert input; proactively monitoring political, economic and security developments.

• Drive internal dialogue on structural adaptability:

Risk Managers should initiate internal discussion on regional autonomy for faster response to local disruption; resilient supply chains through diversification or near-shoring; and strategic positioning by balancing diversification against market concentration.

EXAMPLE: Applying scenario planning to geopolitical risk

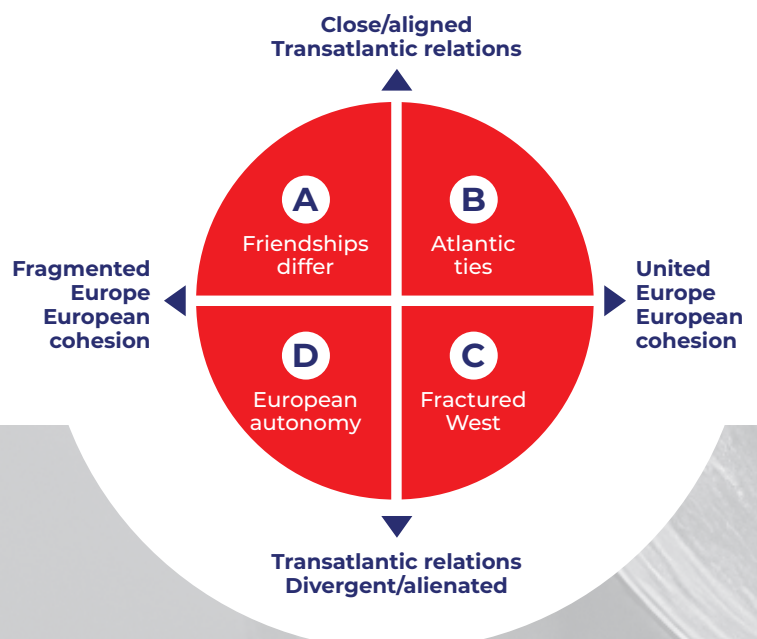
Axes:

► 1. Atlantic relations (EU/US):

- **Aligned Agendas:** The EU and US maintain close coordination on strategic, political, and economic agendas, continuing a historically strong partnership.
- **Separate Ways:** The EU and US diverge in their geopolitical goals, economic strategies, and global governance, leading to reduced cooperation and competition in key areas.

► 2. EU cohesion:

- **EU United:** The EU remains a strong, cohesive bloc with member states aligned on major policies, creating a unified European approach to internal and external challenges.
- **EU Fragmented:** The EU experiences internal divisions, with member states pursuing divergent national interests, reducing the ability of the bloc to act in a coordinated manner.



This provides us with the following four scenarios:

A Aligned agendas & EU fragmented: “Friendships differ”

While transatlantic relations remain strong, internal fragmentation within the European Union limits its capacity to act as a unified bloc. Key issues like climate policy, migration and defence spark divisions among EU member states, weakening Brussels’ ability to negotiate as a single voice. Despite these internal challenges, individual member states (especially larger ones like Germany and France) maintain close ties with the United States. This scenario leads to a two-speed Europe, where smaller states are sidelined while stronger economies take the lead in shaping the future of EU-US relations.

Implications:

Europe remains relevant but lacks strategic coherence, relying on US leadership rather than shaping global affairs itself.

B Aligned agendas & EU united: “Atlantic ties”

In this scenario, the European Union and the United States continue to work closely together, aligning on key strategic and geopolitical issues such as defence, trade and technology. A united European Union strengthens its position as a reliable partner to the United States, reinforcing multilateral institutions and global governance structures. Together they address challenges like climate change, AI regulation and security threats from Russia or China. This cooperation enhances global stability, and the European Union emerges as a cohesive political and economic force, able to project influence beyond its borders.

Implications:

A stable, influential Europe with strong international partnerships, benefiting from economic growth and shared security.

C Separate ways & EU fragmented: “Fractured West”

In this scenario, both transatlantic relations and EU cohesion deteriorate. The European Union struggles to maintain internal unity due to diverging national interests, while the United States and the European Union drift apart on

major geopolitical issues. Without a coherent strategy, the European Union is unable to form a strong collective stance on defence, climate policy or trade, leaving individual member states to pursue separate strategies. This fragmentation weakens the European Union’s influence on the global stage, and both Europe and the United States become more inward-looking, resulting in a less stable and less cooperative international order.

Implications:

A weak, divided Europe that struggles to maintain economic and geopolitical relevance, vulnerable to external pressures.

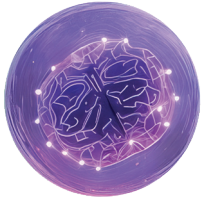
D Separate ways & EU united: “European autonomy”

In this scenario, the European Union takes a more independent approach, distancing itself from the United States on issues like trade, defence and global governance. Rising strategic autonomy becomes a core principle for the European Union, which remains united internally but pursues its own path globally, perhaps driven by shifting geopolitical interests or dissatisfaction with US foreign policy. The European Union strengthens internal solidarity, reinforcing its institutions and focusing on European self-reliance in areas such as defence, digital technologies and energy. A stronger European Union works closely with other global partners, but its transatlantic relations cool significantly.

Implications:

A resilient Europe that charts its own course, but with risks of geopolitical tensions and economic realignments.





3.2 | TECHNOLOGICAL ACCELERATION; NAVIGATING THE RAPIDS OF CHANGE

There is little doubt that artificial intelligence (AI) is reshaping economies, industries, and societies at an unprecedented pace. For European Risk Managers, the imminent challenge is to support the realisation of the immense opportunities AI offers while mitigating the long-term uncertainties it brings.

Europe stands at a crossroads, competing with global AI powerhouses in the United States and China and struggling to match the scale, speed, and investments seen in platform-based technologies elsewhere. Currently, Europe lacks dominant platform companies that control data flows and compute the power needed to create its own AI ecosystem. This asymmetry not only affects European competitiveness but also exacerbates wealth concentration, as the network effects favour a handful of global players. While the European Union has developed some strengths in AI-driven applications, the increasing platform-dependency of these AI applications continues to challenge Europe's digital sovereignty.

Regulation will play a crucial role in shaping the development of AI in Europe. The balance between regulation and innovation remains precarious. While Europe leads the charge on AI ethics through initiatives like the EU AI Act, stringent policies risk stifling innovation and pushing talent and capital towards less regulated markets. At the same time, insufficient guardrails could lead to AI systems that reinforce bias, exploit vulnerabilities or undermine public trust.

Business Model & Market Disruption

AI is much more than just a technological advancement. It is a fundamental force reshaping business models, industries, and market structures. The acceleration of AI-driven automation, decision-making and personalisation means that companies across all sectors are

facing both immense opportunities and existential threats. The speed at which AI can optimise processes, substitute traditional services and scale operations poses a challenge for yesterday's leaders that struggle to keep pace with their AI-first competitors.

One of the most immediate disruptions is **hyper-automation**, whereby AI eliminates inefficiencies and reduces the need for human intervention across entire value chains. In industries such as finance, healthcare, legal services and customer support, AI-driven solutions are replacing traditional workflows. While this enhances productivity, it also reshapes market competition by enabling a small number of AI-powered companies to dominate sectors that were previously fragmented. For European businesses, the risk is twofold; incumbents that fail to integrate AI effectively risk obsolescence, while smaller players struggle with the cost of AI adoption.

Beyond automation, AI enables **entirely new business models** that challenge traditional service-based industries. For example, AI-generated content is disrupting media and entertainment, robo-advisors are transforming wealth management and AI-driven diagnostics are reshaping healthcare. The ability of AI to provide real-time, scalable and cost-efficient alternatives to human-driven services threatens existing providers that cannot adapt to AI-driven cost structures.

AI's ability to learn and improve autonomously creates powerful network effects, where the company with the best data and most advanced AI models gains an exponential advantage over its competitors. This favours AI-first companies that operate on a global scale and can leverage vast data pools, often centralised by non-European-based platforms. As a result, many European businesses risk increasing their **dependency on AI infrastructure, models and APIs** provided by a handful of global players

rather than owning AI capabilities themselves. Without a strong European AI platform economy, local businesses may be reduced to application-layer consumers rather than true AI innovators.

AI-Driven Labour Market Disruptions

AI is redefining the nature of work itself. Unlike previous waves of automation that primarily impacted manual labour and manufacturing, AI-driven automation is also disrupting highly-skilled professions, such as finance, healthcare, legal services and journalism. While AI offers significant efficiency gains, its ability to replace or augment knowledge-based tasks at scale creates profound economic, social and political challenges.

One of the most immediate concerns is the **displacement of jobs** in sectors that were previously considered immune to automation. AI-driven technologies such as natural language processing, predictive analytics and generative AI can now analyse contracts, generate reports, write articles and provide medical diagnostics - tasks traditionally performed by highly skilled professionals. While AI can enhance productivity, reduce errors and lower operational costs, it also threatens job security for employees who find their expertise increasingly replicated by AI systems.

This rapid shift presents a critical challenge in **workforce planning and reskilling**. AI creates new jobs but also demands a different skill set, requiring workers to adapt or risk redundancy. European businesses and policymakers face the challenge of transitioning displaced workers into roles that complement AI, rather than compete with it. Without proactive measures, the skills gap also referred to as digital divide will continue to grow.

The risk extends beyond individual job losses to broader **economic inequality and social unrest**. As AI-driven automation consolidates productivity gains among a small number of AI-powered firms, wealth concentration may accelerate, leading to greater disparities in income and employment opportunities. Sectors with high automation potential may see

wage stagnation or declining job availability, exacerbating existing social inequalities. The resulting economic strain could fuel political backlash, with growing resistance to AI adoption, demands for stronger labour protections and calls for redistribution policies such as universal basic income (UBI).

The disruption of labour markets by AI is not just an economic issue. It is a fundamental societal transformation. Managing this shift effectively will determine whether AI becomes a force for economic growth and opportunity or a driver of social instability.

European Risk Managers must actively support policies and strategies that ensure a balanced transition. This should include investments in AI literacy and workforce re-skilling to equip employees with the skills needed to collaborate with AI.

Cybersecurity & AI-Enabled Threats

As AI becomes more deeply embedded in critical systems, the risks associated with AI-driven cyber threats grow exponentially. While AI enhances cybersecurity defences through automated threat detection and rapid response capabilities, the ability of AI to automate and enhance malicious activities presents a new generation and scale of cybersecurity risks.

One of the most concerning developments is the rise of **AI-powered cyberattacks**, where AI is used to increase the speed, precision and effectiveness of cyber threats. Deepfake fraud is an emerging risk, whereby AI-generated audio, video and text convincingly impersonate individuals for social-engineering attacks, identity fraud and disinformation campaigns. Similarly, autonomous hacking tools can rapidly identify and exploit vulnerabilities in IT systems. Additionally, AI-enhanced phishing campaigns leverage machine learning to craft highly personalised messages, making them much harder for traditional security measures to detect.

Beyond direct attacks, AI's **increasing role in critical infrastructure** and supply chains expands the potential attack surface for malicious actors. Many essential sectors, including energy grids,

financial institutions, transportation networks and healthcare systems, are integrating AI-driven automation for operational efficiency. While this improves functionality, it also creates new points of failure, where compromised AI systems could trigger cascading disruptions. A cyberattack on an AI-controlled power grid or financial market system, for instance, could have far-reaching economic and societal consequences.

The growing sophistication of AI-powered cyber threats requires a proactive approach to AI security. The failure to anticipate and mitigate these risks could lead to unprecedented security breaches, economic losses, and erosion of public trust in AI technologies.

Bias, Ethics & Trust in AI Systems

As AI becomes increasingly embedded in decision-making processes, concerns about bias, ethics and trust are growing. AI models are often perceived as objective, but in reality they may **inherit biases from the data** they are trained on, leading to significant risks of discrimination, unfair outcomes, and a **lack of transparency**. These issues are particularly critical in high-stakes applications such as hiring, lending, law enforcement and healthcare,

where biased AI decisions can reinforce societal inequalities and erode public trust. A concern that AI may not always be a reliable decision-making tool likely will increase resistance to AI adoption, slowing down technological progress and increasing regulatory scrutiny.

As AI takes on more decision-making authority, questions of **legal responsibility** and accountability become increasingly complex. The EU AI Act is introducing stricter guidelines on AI Risk Management, requiring high-risk AI systems to meet transparency, fairness and explainability standards. However, legal frameworks around AI liability remain underdeveloped, leaving organisations in uncertain territory when it comes to accountability. Addressing these challenges will require robust AI governance frameworks, clear liability structures and legal mechanisms that ensure fair and responsible AI deployment.

The risks associated with AI bias, ethics and trust are not just technological. They are deeply societal. If managed responsibly, AI has the potential to promote fairness, enhance decision-making and improve efficiency. But without the right safeguards, AI could just as easily exacerbate discrimination, erode public trust and expose organisations to legal and reputational risks.



KEY RISK MANAGEMENT TAKEAWAYS

• AI as a driver of systemic business disruption:

AI is not just a technology risk but a transformative force reshaping entire industries and business models. Risk Managers must anticipate value-chain disruptions, assess business model resilience and support strategic adaptation to AI-driven market shifts.

• AI as a critical supply-chain dependency:

AI capabilities—such as foundational models, APIs, and cloud-based platforms—are increasingly supplied by a small number of global providers. This creates concentrated external dependencies across digital value chains. Risk Managers should treat AI as a strategic supply-chain risk, assessing exposure to third-party platforms and reinforcing operational resilience through diversification, procurement oversight and contingency planning.

• Labour market impacts as a socio-economic risk:

AI is automating tasks in high-skill sectors, with broad implications for workforce planning, employment patterns and social stability. Managing these risks requires early collaboration between HR, strategy and public policy to support upskilling, workforce transition and social cohesion.

• AI as a growing security risk:

AI expands the threat landscape across both physical and digital domains. While it strengthens some defences, it also enables new classes of attack—from deepfakes and automated hacking to AI-driven misinformation and infrastructure sabotage. As AI systems are integrated into critical sectors like energy, finance and healthcare, they create new points of failure. Risk Managers must ensure that security strategies evolve to address AI-specific vulnerabilities, operational dependencies, and cascading risks in AI-reliant environments.

• Challenges in AI insurability and ethical liability:

AI systems often operate as opaque decision-makers, raising ethical and legal concerns around bias, fairness and explainability—especially in high-stakes domains like hiring, lending, or healthcare. These concerns complicate accountability and pose difficulties for insurers in assessing liability. Risk Managers must proactively address these gaps by supporting transparent AI governance, embedding ethical safeguards and working with legal and insurance partners to define responsibility in the event of biased or erroneous AI outcomes.

EXAMPLE: Applying scenario planning to AI-related risks

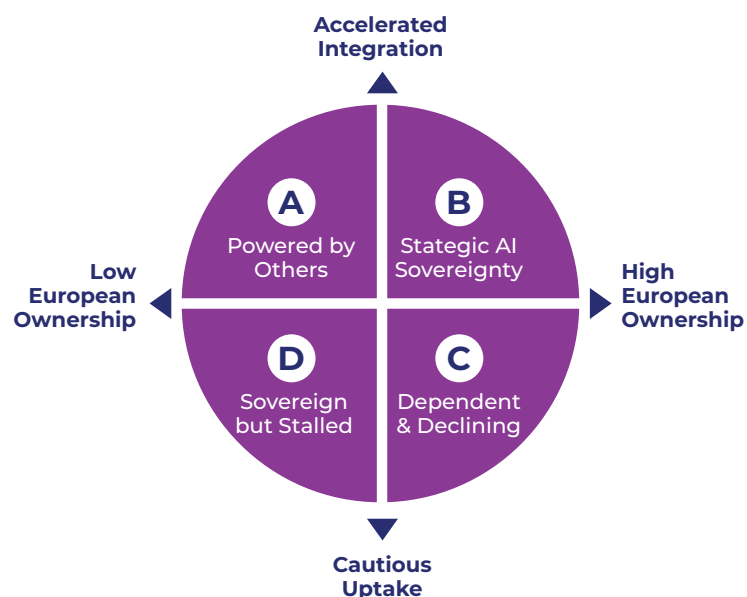
Axes:

► 1. Pace of AI Adoption in Europe:

- **Accelerated Integration:** AI is rapidly deployed across sectors, transforming business models, labour markets and services.
- **Cautious Uptake:** Europe adopts AI more slowly, constrained by regulation, fragmented capabilities or societal resistance.

► 2. European Control of Core AI Technologies:

- **High European Ownership:** Europe develops its own foundational models, platforms, and compute infrastructure, reducing dependency.
- **Low European Ownership:** Core AI technologies remain dominated by non-European actors, leaving Europe reliant on external platforms and ecosystems.



This yields four plausible scenarios:

**A Accelerated Integration
& Low European Ownership:
“Powered by Others”**

AI adoption surges across European industries, but foundational models, platforms and compute power are sourced externally. Local businesses scale rapidly but become deeply reliant on global tech giants. Regulatory alignment is difficult, and platform lock-in becomes a strategic vulnerability.

Implications:

High productivity gains but loss of digital sovereignty, weak influence over AI norms, and increasing vulnerability to pricing, access, and ethical drift driven by non-European providers.

**B Accelerated Integration
& High European Ownership:
“Strategic AI Sovereignty”**

Europe both accelerates AI integration and builds its own AI ecosystem through investment, regulation, and cross-border collaboration. Domestic platforms flourish, and AI is deployed across sectors within robust governance frameworks.

Implications:

Competitive advantage through responsible innovation. Economic gains are retained within Europe, reinforcing industrial strength, resilience and public trust.

**C Cautious Uptake
& Low European Ownership:
“Dependent & Declining”**

Europe is slow to adopt AI and lacks control over core technologies. Businesses fall behind global competitors, particularly in data-intensive sectors. Foreign platforms dominate AI infrastructure, and European firms are relegated to the application layer.

Implications:

Severe competitiveness loss across industries, rising economic dependency, weakened productivity and long-term threats to wealth creation and social welfare. Strategic stagnation compounds inequality and fuels political frustration.

**D Cautious Uptake
& High European Ownership:
“Sovereign but Stalled”**

Despite developing its own AI platforms and governance systems, Europe remains slow in adopting AI at scale. Strict regulatory environments and fragmented implementation reduce momentum.

Implications:

Digital sovereignty is preserved, but economic and competitive benefits are delayed. Missed productivity gains strain public budgets and limit Europe's ability to invest in welfare, inclusion, and long-term industrial leadership.





3.3 | CLIMATE CHANGE RISK

The evolving risks posed by climate change have profound implications for European companies, spanning economic, regulatory and reputational dimensions. While the urgency of mitigating climate risks is widely acknowledged, the reality of implementing risk management strategies presents significant hurdles. The global response to climate change has been fragmented, with disparities in policy approaches, financial commitments and strategic priorities among key economic blocs and emerging economies. As a result, European businesses find themselves navigating a complex landscape of shifting regulations, economic pressures and heightened public scrutiny.

Organisations must adapt to increasing demands for sustainability while mitigating risks associated with regulatory shifts, supply-chain disruptions and financial instability driven by climate-related catastrophes.

Deprioritisation of climate action: Urgency versus reality

Despite growing recognition of climate change as an existential threat, a noticeable deprioritisation trend has emerged. The United States has demonstrated increasing pushback on green initiatives, with a resurgence of hyper-capitalist policies that prioritise short-term economic gains over long-term sustainability. Meanwhile, within the European Union, climate action is increasingly balanced against the need to maintain economic competitiveness, leading to a slower approach to green transitions.

At the global level, CO₂ reduction targets remain largely unmet, and the effectiveness of international climate summits, such as COP and discussions at the G20, is regarded with increased scepticism. The lack of binding agreements and concrete enforcement mechanisms further exacerbates the credibility gap, leaving organisations uncertain about the long-term regulatory landscape. Additionally, many emerging economies continue to prioritise industrial growth over environmental responsibility, further complicating global climate action efforts.

Climate change as a systemic risk

Climate-related risks represent systemic threats that intersect with economic stability, geopolitical shifts and social structures. A restriction in access to collective protection mechanisms, particularly in the insurance sector, exacerbates corporate vulnerabilities. As climate-related disasters increase in frequency and severity, insurers face mounting losses, potentially leading to reduced coverage availability and higher premiums for buyers. This dynamic creates a systemic risk within a systemic risk, where the financial protection that companies have traditionally relied upon is itself under threat.

Furthermore, climate risks are deeply interconnected with geopolitical and human capital concerns. For instance, disruptions caused by extreme weather events, war or migration crises impact workforce availability, supply-chain continuity and infrastructure resilience. The compounding effects of these risks underscore the need for European companies to adopt a more holistic approach to climate risk management, integrating it into broader strategic foresight or scenario-planning efforts.

Economic impact and cost distribution

The financial burden of transitioning to a low-carbon economy and adapting to climate change is substantial, and how that burden will be shared remains highly contested. A restriction in capacity and coverage from sectors of the insurance market is leading to increased reliance on state intervention. However, high public debt levels in many European countries means the ability of governments to provide sustained financial support remains uncertain.

Climate change is also a significant legal risk for corporations. Recent legal decisions not only emphasise violations of the European and UN Conventions on Human Rights for omissions or shortcomings in public policies regarding climate change, there have also been several judicial actions brought against private corporations and/or their directors.

To bridge this gap, there is a growing need to deploy more private-sector capital into climate-resilience initiatives. This includes mechanisms such as public-private partnerships and mandatory insurance or risk-pooling structures that mutualise climate risks. But these financial shifts raise concerns about potential impacts on political stability, as the perceived burden of climate transition may lead to lower public and corporate ambition levels.

Regulatory compliance, policy uncertainty and competitiveness

As climate policies evolve, European organisations must navigate an increasingly complex regulatory environment. The European Union remains a global leader in climate legislation, particularly with its commitment to a 55% CO₂ reduction by 2030. But regulatory fragmentation across regions poses compliance challenges for businesses operating across multiple jurisdictions. There is also growing concern that the current stance being taken by the United States may cascade to other countries.

Profitability is increasingly affected by stringent environmental regulations, legal liabilities and rising compliance costs. And litigation risks are mounting. For businesses, the challenge lies in balancing regulatory adherence and meeting the Environmental, Social and Governance (ESG) expectations of stakeholders with maintaining financial viability in a competitive global market.

International cooperation: the missing link

Addressing climate risks requires global cooperation, yet current efforts remain fragmented. While the European Union continues to push forward with ambitious policies, its ability to drive meaningful change is constrained by the limited impact of unilateral actions.

Emerging economies, particularly those with high biodiversity risks, are demanding greater compensation and support from industrialised nations, which bear the greatest responsibility for historic emissions. At the same time, the vacuum left by US disengagement from green initiatives has opened opportunities for developing nations to take a more prominent role in green-technology leadership. However,

without stronger international agreements, these dynamics risk further delaying the transition to a more sustainable global economy.

Corporate and governmental responsibilities

Climate change is morphing from an ethical consideration to a legal responsibility. Increasingly, climate change is recognised as a Human Rights issue, with growing demands for accountability from both governments and corporations. Climate litigation and activism are on the rise, placing pressure on businesses to demonstrate genuine commitment to sustainability.

Organisations are increasingly caught between public expectations, legal risks and operational constraints. The credibility and ethics gap in corporate climate action directly impacts reputation and brand value, making sustainability a critical factor in long-term business success. In this landscape, firms must integrate climate risk management into their core strategies, rather than treating it as a peripheral concern.

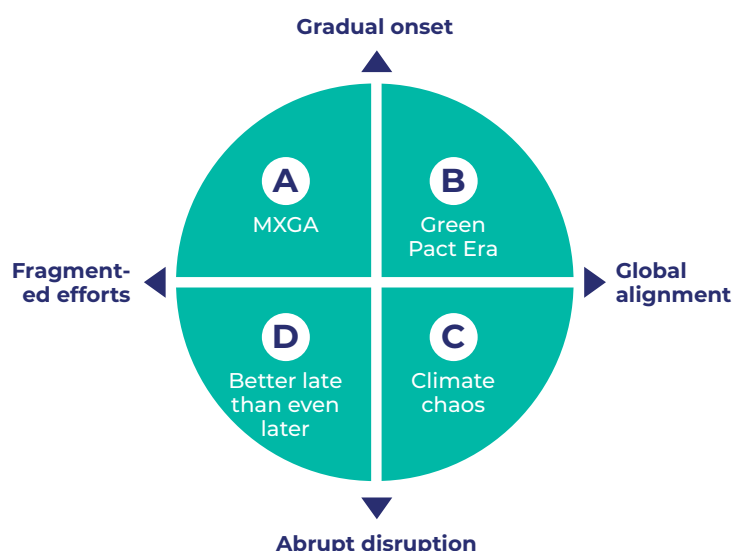
KEY RISK MANAGEMENT TAKEAWAYS

- **Integrate climate risk into core strategy:** Climate change should be treated as a systemic risk and embedded into Enterprise Risk Management frameworks and scenario planning.
- **Strengthen crisis and continuity planning:** Business continuity and disaster recovery plans should be regularly stress-tested for climate-driven disruptions.
- **Prioritise critical functions:** Organisations should protect essential functions and consider exiting highly vulnerable or unsustainable business lines.
- **Monitor legal and regulatory exposures:** Risk Managers should stay ahead of evolving regulatory and litigation risks, particularly around fiduciary duty.
- **Plan for business model shifts:** Risk Managers should assess the viability of business lines under climate stress and prepare for potential divestments or transformations.

EXAMPLE: Applying scenario planning to climate change risk

Axes:

- ▶ **1. Level of global climate policy alignment:**
 - **Global alignment:** Coherent and binding international agreements drive coordinated climate action.
 - **Fragmented effort:** Fragmented, competitive or nationalistic approaches dominate; little global coordination.
- ▶ **2. Pace of physical climate impact:**
 - **Gradual onset:** Climate change effects emerge steadily and predictably.
 - **Abrupt disruption:** Extreme weather events, tipping points or feedback loops accelerate climate impacts unpredictably.



This provides us with the following four scenarios:

A Fragmented efforts & Gradual onset: “MXGA”

In this scenario, global climate cooperation breaks down. Nations adopt fragmented policies benefitting their own interests and protectionism rises. Climate risks emerge slowly, allowing time to prepare but dulling the political urgency of taking action. European firms face stricter local rules but limited global alignment.

Implications:

Navigating divergent regulations and green tariffs becomes costly. Companies must localise operations and develop strategies to balance compliance with competitiveness. Green innovation continues, but without global coordination, and scaling it becomes harder.

B Global alignment & Gradual onset: “Green Pact Era”

In this scenario, international climate cooperation takes hold. Global agreements, carbon pricing and green finance align policy across regions. Physical climate impacts remain manageable, giving businesses time to adapt. European companies operate in a rules-based environment that rewards sustainability and innovation.

Implications:

Firms benefit from policy predictability and rising consumer demand for sustainable products. Early movers in clean tech and ESG leadership thrive but keeping pace with compliance and innovation is essential to stay competitive.

C Global alignment & Abrupt disruption: “Better late than even later”

In this scenario, global climate policy aligns but the environment deteriorates faster than expected. Extreme weather events and infrastructure failures become frequent. Insurance markets falter, necessitating public-private risk-sharing mechanisms. Even well-prepared companies struggle to maintain operations.

Implications:

Building resilience becomes critical. Companies must invest in crisis response, scenario planning and supply-chain flexibility. Success depends less on emissions targets and more on the ability to adapt to constant disruption.

D Fragmented efforts & Abrupt disruption: “Climate chaos”

In this scenario, climate impacts accelerate dramatically while international coordination collapses. Crises such as natural disasters, displacement, supply-chain failures and social unrest are compounded. Regulatory responses are reactive and unpredictable. Markets contract and public trust erodes. Systemic risks take hold.

Implications:

Survival depends on extreme adaptability. Companies must exit high-risk geographies, protect reputation and refocus on core resilient assets. The cost of inaction rises sharply, and public scrutiny becomes unforgiving. Regulation is erratic and reactive, in desperate attempts to create structure in chaos, ironically only adding to the grievances of businesses and citizens.



3.4 HUMAN CAPITAL RISKS; RESHAPING THE FUTURE OF BUSINESS

Human capital risks will transform the future of European businesses, making it imperative for companies to rethink talent strategies, employment models and long-term workforce planning.

Organisations that prioritise adaptability, life-long learning and well-structured workforce policies will be best positioned to navigate an increasingly complex labour market. Meanwhile, society as a whole needs to adapt to an ageing world, including securing sustainable funding for retirement.

New work-life symbiosis

The evolving relationship between work and personal life is redefining human capital risks for European companies. Younger generations increasingly prioritise careers that they deem to have a greater purpose and work-life balance over traditional job security. Organisations that fail to adapt to this shift run the risk of reduced employee loyalty, lower engagement and difficulty in attracting top talent.

The growing focus on employee well-being means that organisations that offer greater job flexibility will have a competitive edge in talent retention. Businesses need to create environments that accommodate hybrid work models, prioritise mental-health support and foster a culture of trust and autonomy to enhance employee satisfaction and long-term commitment.

The changing expectations of employees require organisations to rethink traditional career paths. Instead of linear progressions within a single company, many professionals now seek varied experiences across industries and geographies. Employers that offer cross-functional training, career mobility programmes and internal entrepreneurship opportunities will be better positioned to retain talent and mitigate the risks associated with high turnover rates.

Employees may frequently switch jobs and many will opt for multi-employer engagements, leading to challenges in workforce stability. This volatility increases the likelihood of knowledge loss, which can affect the quality of products, services, and business processes. Organisations therefore need to be adaptable in their approach to talent and human capital.

Longevity and multigenerational teams

People are living longer. And this means that European companies must navigate the complexities of multigenerational teams. Project groups may include employees spanning three or more generations, each with different approaches to technology, communication and work structures. Integrating these diverse perspectives can lead to innovation but requires intentional management and tailored workflows/structures to avoid conflicts that might arise from differing work habits and expectations.

Lifelong learning initiatives will become critical to ensure that employees across all age groups and fields of expertise stay relevant in rapidly evolving industries. Organisations must prioritise continuous reskilling and upskilling programmes at all levels to help workers adapt to new technologies and industry shifts. Additional education can no longer be perceived as a bonus but must be treated as a necessity. New approaches to knowledge management, such as reverse mentoring programmes can foster an inter-generational knowledge exchange in addition to more formal continuous training.

An ageing workforce requires companies to rethink employment policies and pension structures. Employers may need to implement phased retirement plans, offering part-time opportunities to older employees who wish

to remain engaged in the workforce while reducing their workload. Creating incentives for later-life employment can help retain valuable expertise while alleviating pressure on remuneration and pension systems.

Task definition and value assessment

The increasing integration of artificial intelligence (AI) and automation means that humans will primarily manage and oversee processes rather than perform routine tasks themselves. As a result, companies will need to redefining job roles, shifting from execution-based responsibilities to strategic oversight and problem-solving functions. This will require more focus on humans to define workflows, monitor execution and assess output quality, for example.

Organisations must recognise the growing importance of soft skills—such as emotional intelligence and creative problem-solving—in a world increasingly dominated by uncertainty. As technology takes on more routine tasks, human capital will be valued primarily for its ability to navigate complexity and adapt to unexpected developments. Employers would benefit from increasing their focus on and investments in leadership development programmes and cross-disciplinary training to ensure their workforce remains agile in

the face of changing circumstances and demands.

Pension protection gap

As Europe's population ages, the need for private pension schemes is increasing as public systems become less sustainable. In light of the growing proportion of public debt that will be allocated to fund the ageing population, governments may be forced to reform pension structures, potentially increasing corporate tax obligations.

A shift toward automation will reduce the number of pension-eligible employees, raising ethical and financial questions about future workforce contributions. Some proposals suggest implementing taxation on robotic labour or introducing universal basic income models to compensate for lost human income-generating employment, and corresponding losses in savings as well as income taxes.

The broader challenge remains ensuring solidarity within an evolving economic landscape. Companies that take a proactive approach to pension planning—by offering hybrid financial support structures, incentivising lengthier participation in the workforce, or collaborating with policymakers on sustainable pension models will be better equipped to navigate these demographic shifts.



KEY RISK MANAGEMENT TAKEAWAYS

- **Integrate human capital into risk frameworks:** Human capital risks should form part of ERM frameworks and dependencies on talent should be mapped. Workforce resilience metrics, including HR trends, should be included in risk registers.
- **Scenario plan for workforce disruption:** Risk teams should run simulations on workforce volatility, AI displacement or generational shifts. This should include scenarios in which up to 30% of functions are impacted by talent shortages or automation.
- **Collaborate on strategic workforce planning:** Risk Managers should work with HR counterparts and business units to assess long-term skills gaps, identify vulnerable roles and functions and support upskilling/reskilling investment decisions.
- **Assess and monitor pension liabilities:** Risk Managers should evaluate the impact of demographic trends on pension commitments and labour costs and collaborate with finance and legal teams to address exposures and regulatory risks.
- **Monitor legal and ESG trends in employment:** Risk teams should track human rights-related litigation and ESG expectations linked to employment practices, diversity and fairness as part of a growing reputational and liability risk.

EXAMPLE: Applying scenario planning to human capital risk

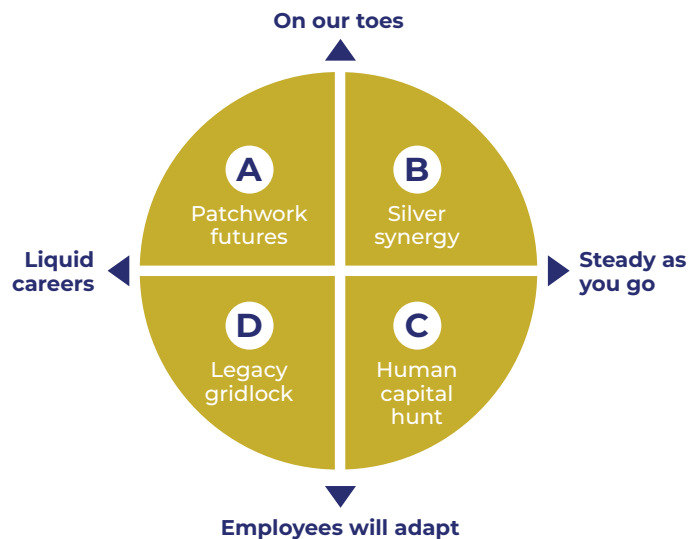
Axes:

► 1. Career stability:

- **Steady as you go:** Predictable, structured paths, clear roles, continuity across time and generations
- **Liquid careers:** Fragmented gigs, frequent job changes, fluid teams, uncertain paths

► 2. Organisational adaptiveness:

- **On our toes:** Agile, inclusive, proactive in learning, tech, multigenerational needs
- **Employees will adapt:** Static organisational models, weak learning culture, rigid structures



This provides us with the following four scenarios:

A Liquid careers & On our toes: "Patchwork Futures"

Here, jobs are fluid and careers are built across projects, platforms and employers. Organisations adapt by building agile learning cultures, using short-term contracts and portfolio-based teams. Ageing workers must continuously reskill or risk marginalisation. Some thrive as flexible experts, while others struggle with fragmented pensions and inconsistent work.

Implications:

Firms stay competitive by embracing change, but must invest in continuous onboarding and health support. Cross-generational equity becomes a flashpoint, especially around retirement security.

B Steady as you go & On our toes: “Silver Synergy”

In this scenario, organisations create strong internal talent pipelines, valuing both experience and agility. Long-term career models are refreshed through constant upskilling and cross-generational mentoring. Ageing workers phase into part-time and advisory roles while younger talent thrives in structured but evolving career tracks. Intergenerational collaboration is seen as a competitive edge.

Implications:

Organisations maintain deep expertise while fostering innovation. They reduce turnover, manage pension burdens proactively and leverage longevity as an asset—not a cost.

C Steady as you go & employees will adapt: “Legacy Gridlock”

Organisations retain traditional structures and career models but fail to keep pace with changing needs. Ageing employees dominate senior roles, with limited upward mobility for

younger generations. Skills become outdated, and knowledge transfer lags. Resistance to hybrid work, new tech and agile processes creates internal friction.

Implications:

Workforces stagnate. Costs rise, engagement falls and companies struggle to attract talent aged under 40. Pension liabilities grow unchecked, and productivity plateaus.

D Liquid careers & employees will adapt: “Human Capital Hunt”

In this scenario, the labour market is chaotic and companies are unprepared. Jobs are short-lived, learning is self-funded and ageing workers are sidelined. Younger workers churn frequently; older employees are seen as too expensive. No one feels secure. Trust in employers collapses.

Implications:

Talent shortages worsen. Knowledge loss is rampant. Organisations face reputational risk, operational fragility and growing legal and political pressure to fix systemic workforce failures.

END NOTES

This report is aimed at helping Risk Managers to take a forward-looking approach to anticipate unknown and evolving threats that transcend traditional risk frameworks. The use of structured foresight tools like scenario planning, horizon scanning and future wheels can help us to explore how risks may evolve and interact under different future circumstances.

A foresight approach focuses on understanding trends and exposures and mapping vulnerabilities and interdependencies to ultimately strengthen risk management strategies.

Rather than aiming to predict one, definitive future, a foresight-driven philosophy broadens the spectrum of potential scenarios. This fosters a culture of proactive adaptation, shared insight and enhances organisations' capability to navigate and influence and increasingly uncertain global risk environment.

The Foresight Committee is not a one-off, static event; we are open to further contributions and will continue to welcome inputs from experts. And this NEXT report is the first of many more.

Let's become future-focused Risk Managers.



MEMBERS OF THE FORESIGHT COMMITTEE

Daria Krivonos,
CEO, Copenhagen Institute
for Futures Studies

Sebastian Wieczorek,
CEO, Mantix

Bruno Colmant,
Professor, Board member
of several companies/hospitals

Paulino Fajardo,
Head of Disputes for Europe, Middle East
and Africa, Herbert Smith Freehills LLP

Sean Lyons,
Corporate Defense Authority,
Writer, and Speaker, Consultant

Philippe Cotelte,
FERMA Board Member
and Chairperson of the
Foresight Committee

Charlotte Hedemark,
President of FERMA

Typhaine Beaupérin,
CEO of FERMA



About FERMA

The Federation of European Risk Management Associations brings together 23 national risk management associations in 22 European countries. FERMA represents the interests of 6.000 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at **www.ferma.eu**



Federation of European Risk Management Associations

Avenue de Tervuren 273 B12 - 1150 Brussels (BELGIUM)

Tel: +32 2 761 94 32 - Email: enquiries@ferma.eu



@FERMARISK