KPMG

Building a shock-resilient supply chain

How business leaders can move from risk management to enterprise resilience amid energy-linked disruption and geopolitical uncertainty



AI generated image

KPMG. Make the Difference.

kpmg.com

Foreword

Over the years, I've had the opportunity to work with leaders across industries as they navigated financial crises, supply chain disruptions, geopolitical shocks, and periods of rapid change. What strikes me today is not the scale of any one challenge, but the way so many of them are converging at the same time.

Geopolitical tensions, shifting trade relationships, resource constraints, cyber threats, regulatory shifts, and energy-linked disruption are creating ripple effects that extend far beyond their original source. A disruption in one corner of the world can quickly affect supply chains, customer relationships, investment decisions, and growth plans somewhere else. The connections are becoming harder to predict and, in many cases, harder to manage.

What makes this moment different is that risks no longer arrive one at a time. They overlap, reinforce one another, and can create cascading consequences across industries and geographies. In a world increasingly defined by interdependence, traditional approaches that evaluate risks in isolation are often not enough. Leaders need a broader view of how events connect and where vulnerabilities may emerge. This reflects the comments from the report that risks are "colliding at once" and creating "domino effects" across systems. While the impacts of these disruptions will vary significantly from one industry to another, the challenge of managing multiple concurrent shocks is increasingly a shared reality across sectors.

This research explores those dynamics through the lens of energy-linked disruption, but the lessons extend well beyond energy. The findings reveal how organizations are responding to a more complex operating environment by strengthening supply chains, enhancing scenario planning, and building greater resilience into decision-making.

What encourages me most is that many organizations are already adapting. They are looking beyond immediate risks and asking deeper questions about how their business can remain resilient in an increasingly interconnected world. They recognize that resilience is no longer simply about responding to disruption. It is about anticipating change, adapting quickly, and finding opportunities amid uncertainty.

The organizations that will thrive in the years ahead are unlikely to be those that can predict every disruption. They will be the ones that can learn, adapt quickly, and respond when the unexpected occurs.

It is our hope that this research helps leaders better understand the forces reshaping today's business environment and provides practical insights to strengthen resilience, support growth, and build confidence for whatever comes next.



Regina Mayor
Global Head of Clients & Markets
KPMG International

Biography here

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Table of contents

Executive summary

Key findings

01 New imperatives in a changing world

02 Redefining organizational risk

03 Understanding risk

04 Resilience is increasingly an ecosystem capability

05 KPMG Dynamic Risk Assessment

06 Global and regional risks and opportunities

07 Cross-sector risks and opportunities

08 Building the capabilities for resilience

09 Building a risk-aware culture

10 Transformation path

Conclusion

How KPMG can help

Authors and acknowledgments

Methodology



Click on each theme to read more

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Executive summary

Risk has moved outside the enterprise

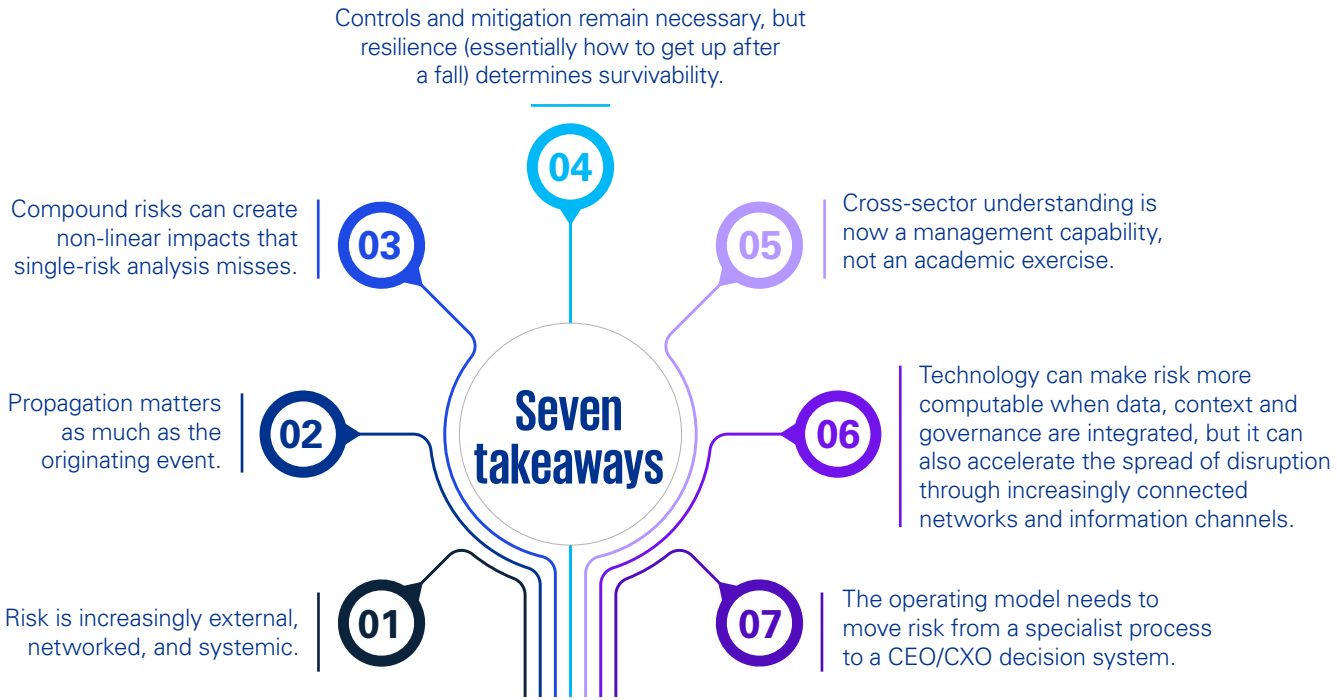
For much of the modern risk-management era, organizations could reasonably assume that their most controllable threats were also among their most important. The discipline therefore grew around internal controls, compliance, insurance, contractual allocation, business continuity, and periodic scenario analysis.

That assumption is weakening. The risks occupying CEOs and boards increasingly originate outside the organizational boundary: geopolitical conflict, geoeconomic fragmentation, maritime chokepoints, cyber-physical disruption, extreme weather, trade restrictions, resource concentration, technology discontinuity, and financial-market spillovers. The World Economic Forum's 2026 survey ranks geoeconomic confrontation first and state-based armed conflict second among risks most likely to trigger a material global crisis in 2026; half of respondents expect a turbulent or stormy two-year outlook.[1]

Energy sits close to the center of this new risk landscape. It is globally traded, infrastructure-intensive, financially connected, and essential to almost every other sector. A disruption in an energy corridor can rapidly become a freight problem, an industrial-input problem, a food production problem, an inflation problem, a liquidity problem, and eventually a growth problem.

The management question is changing from 'How do we prevent bad events?' to 'How do we see, absorb, respond and adapt when external shocks are unavoidable?'

[1] The Global Risks Report 2026, World Economic Forum, 14 January 2026



This paradigm shift from containing risk to building resilience may require large enterprise-wide transformation of strategy, systems and processes, and technology. Given the significant change, it is important to act fast but also calibrate the change to ensure organizational readiness.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Key findings

The risk landscape is becoming more complex and interconnected

70% of survey respondents said their organization's risk exposure has increased over the past 2 years

56% of survey respondents said that external disruptions involving factors such as geopolitical issues, energy, cyber, trade or climate will cause severe operational disruption or have a significant impact on their organization's costs and performance over the next 3-5 years

Risks most likely to have greatest impact on their organization over the next two years:

64% Technology and AI disruption

58% Geopolitical conflict

48% Macroeconomic uncertainty

Supply chain risk is a matter of

growing, interconnected, and global ecosystems

Risks seldom happen in isolation

Risks often occur in clusters, influencing and being influenced by other risks

The stage in supply chain that is currently most exposed to disruption:



Technology and digital dependencies



Delivered costs/ price volatility



Shipping and logistics

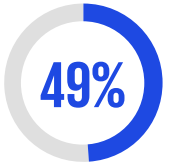
Resilience has become a strategic priority

28% of survey respondents felt that energy security and resilience has become a significant strategic priority for their organization's senior leadership

70% of respondents indicated they were either confident or very confident that their organization could maintain critical operations during a major external disruption

Organizations are adapting their resilience strategies

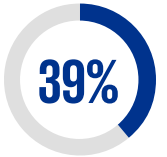
Prioritized actions to strengthen resilience:



AI and predictive analytics



Scenario planning and stress testing



Alternative sourcing strategies

31% identify focusing on efficiency and cost optimization as their organizations approach to resilience over the next 3-5 years

Note: Key findings from the KPMG Dynamic Risk Assessment and global pulse survey conducted by Ipsos. Read more here.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

01

Introduction

New imperatives in a changing world



AI generated image

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

In today's business world, one thing is certain — the rise of global uncertainty. We are witnessing a tectonic shift away from an era of relative stability, free trade, and US-protected international markets to a fragmented and multipolar world marked by forces that seem well beyond the control of any one region, country, market, corporation or economic power.

These changes and uncertainties demand new ways of thinking about supply chains for CEOs, COOs, CROs, and supply chain leaders across energy intensive sectors. In the past, supporting supply chain operations and performance was a matter of internal risk management, much like how a corporation maintains an ERM system or other enterprise-level platforms. Now, the preponderance of risks is outside corporate boundaries and involves issues that are well beyond the ability of any corporation to resolve.

Growing nationalism and protectionism have made sovereignty a business continuity issue. The ongoing conflict in Iran is impacting energy access, prices, and subsidiary markets around the world. Countries both large and small are now questioning or restructuring long-standing political relationships, treaties, and trade agreements. AI and new technologies are disrupting planning and operations. Scarcity for key resources and infrastructure is an increasing risk. Finally, all these developments are being shaped by the evolving realities of climate risk. While perceptions of climate risk may be declining, the frequency and severity of extreme weather events continue to rise.

Now is the time to question long-held assumptions about the design, operation, and strategic development of today's supply chains as part of a broader enterprise resilience framework.

Resilience is no longer just a supply chain function, it has become a board-level imperative shaped by energy-linked disruption and a broader set of interconnected risks spanning technology, financial stability operations, and global value chains. This report provides an overview of supply chain risks and strategies for resilience based on multiple, in-depth interviews with KPMG industry experts from around the world. Their insights were closely analyzed using our Dynamic Risk Assessment (DRA) methodology and combined with a global pulse survey conducted by Ipsos. In addition, we review global and regional risk environments, as well as common risks we have identified at the sector and cross-sector levels.

Equally important, we discuss supply chain management strategies at the organizational level. For corporations, we believe that these strategies are best developed and carried out through a multi-level approach according to the severity, influence, nature, velocity, and magnitude of risk. This approach is divided into four areas of action: regular assessments and control; risk mitigation for specific issues; larger initiatives for resilience; and re-envisioning the business, if necessary, through capital reallocation.

Supply chains serve as the backbone of our global economy, a true reflection of our interdependence on one another even as that interdependence is now threatened with conflict and fragmentation. This report is designed to help decision makers better understand the vital need for supply chain resilience in today's increasingly uncertain business world.



Anish De
Global Head of Energy, Natural Resources and Chemicals
KPMG International

Biography here

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

02

Redefining organizational risk



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Nearly 70 percent of the pulse survey respondents reported that their organization's risk exposure has increased over the past two years, highlighting a growing perception of volatility and uncertainty across the risk landscape. Also, more than half of survey respondents said that external disruptions involving factors such as geopolitical issues, energy, cyber, trade, or climate will have a severe operational disruption or a significant cost and performance impact on their organization over the next three to five years.

70%

of organization's risk exposure has increased over the past two years

However, risk is not simply on the increase; it is undergoing a basic restructuring. In fact, we could say that the risk stack has been inverted. Traditional enterprise risk management was strongest at the bottom of the stack: internal, organizational risks that could be owned, controlled, and audited. Today's most consequential threats increasingly emerge at the top — global and cross-sectoral — before affecting external risks at the sectoral and organizational levels.

The externalization of risk does not make internal control less important. It changes what control can achieve. An organization cannot control a war, a sovereign sanctions decision, a blocked maritime corridor, a global cyber campaign or a climate-driven physical event. It can control its exposure, preparedness, options, and speed of response.

The new four-level risk stack

Layer	Illustrative risks	Management action
Global	Geopolitics, conflict, climate, macroeconomics, technology, pandemics	Sense and interpret external change early
Cross-sectoral	Energy, technology, finance, automotive, logistics, digital infrastructure, food, water, critical minerals, manufacturing	Map dependencies and transmission across systems
Sectoral	Commodity cycles, regulation, asset concentration, market design, resource access	Translate systemic change into sector economics
Organizational	Operations, cyber, liquidity, people, counterparties, projects	Control what can be controlled; build recovery capacity

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Hormuz 2026: A stress test for supply-chain risk management

The Iran conflict has turned a familiar chokepoint risk into a prolonged operating condition. The precipitous drop in traffic through the Strait of Hormuz has resulted in disruptions to global energy markets.[2] Not surprisingly, more than a quarter of our pulse survey respondents felt that energy security and resilience has become a significant strategic priority for their organization's senior leadership. However, the lesson of Hormuz is not simply that closing a critical route can compromise energy supply. It is that conventional risk mitigation can degrade simultaneously. Diversified suppliers can still share the same maritime chokepoint. Contractual rights do not create vessels, insurance capacity or physical throughput. Alternative crude may not be refinery-equivalent. Product markets can tighten even when headline crude volumes appear available. FX, freight, financing and working capital can amplify the physical disruption. Diversification by supplier is not resilience if suppliers share the same route, infrastructure, financing channel, technology dependency or geopolitical exposure.

What Hormuz reveals

Traditional assumption	2026 reality	Required shift
Multiple suppliers = diversified risk	Different suppliers may share one chokepoint	Map common dependencies, not supplier count
Contracts allocate disruption risk	Contracts cannot manufacture physical capacity	Model physical and commercial substitutability
Inventory buys time	Duration and product mismatch can exhaust buffers	Simulate stock-flow states through time
Commodity exposure is the main issue	Freight, FX, insurance, refining, and liquidity interact	Model compound effects and feedback loops
Crisis teams respond after escalation	Velocity can outrun governance cadence	Use continuous sensing and trigger-based decisions

As the chart above suggests, organizations exposed to complex shared dependencies, supply-chain resilience may benefit from a system model in addition to supplier-risk registers and organizational controls.

[2] The Strait of Hormuz: Security Developments and Impacts on Oil, Gas, and Other Commodities, U.S. Congress, 7 August 2026

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

03

Understanding risk: From isolated events to interconnected systems



AI generated image

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

A risk event is only the beginning. Enterprise consequence depends on where the shock enters, the channels through which it travels, the organization's exposure at that moment, the interaction with other risks, the receiving system's vulnerability, and the event's duration.

The key implication is that organizations should monitor upstream signals and pathway conditions, not only actual losses. Waiting for a risk to become an internal incident sacrifices the most valuable resource in resilience: time.

Cross-sector footprint

Energy risks are rarely confined to energy. Fuel and power are inputs to mobility and logistics, mining, chemicals, agriculture, manufacturing, data centers and households. Financial systems price the inflation and growth consequences; governments respond through subsidies, taxes, reserves, sanctions or trade measures. Each response can create another round of effects.

How risks combine: Compounding, feedback and velocity

Single-risk analysis implicitly assumes separability. Real crises often violate that assumption. A geopolitical disruption can raise crude prices, freight and insurance while weakening a currency; those effects can increase working-capital needs just as product availability tightens. The combined outcome can be materially worse than the arithmetic sum of each standalone shock.

Velocity is increasingly important. Digital networks transmit cyber events in minutes; markets reprice in seconds; trade and sanctions decisions can change cargo economics overnight. Physical systems may move more slowly, but the mismatch between fast financial repricing and slower physical adaptation can itself become an amplifier.

Uncertainty also has to be represented honestly. The objective is not to turn every geopolitical scenario into a precise probability. It is to distinguish facts, inferred relationships and scenario assumptions; quantify ranges where defensible; and identify the thresholds at which management choices change.

A generic energy transmission pathway

Stage	Illustrative pathway
Originating shock	Conflict, sanction, cyberattack, weather event, regulatory discontinuity
System transmission	Energy -> shipping -> industrial inputs -> inflation -> rates/FX -> demand
Enterprise entry points	Supplier, route, asset, contract, customer, technology, financing
Amplifiers	Low inventories, concentrated routes, high leverage, poor data, slow decisions
Business consequences	Supply loss, margin compression, cash/WC stress, service failure, strategic delay
Second-order effects	Policy intervention, customer behavior, competitor response, capital reallocation

Note: This is a conceptual risk principle rather than a quantified conclusion.

The compound-risk lens

Question	Management output
What is interacting?	Risk constellation and interaction graph
Why does it interact?	Physical, economic, contractual, technological or behavioral mechanism
Where can it propagate?	Cascade pathway across enterprise and external systems
How fast?	Velocity, lag and time-to-threshold
What is shared?	Common dependencies, geographies, infrastructure, counterparties or technology
Where can we interrupt it?	Break-points that disproportionately reduce propagation

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

04

Cross-sector linkages: Resilience is increasingly an ecosystem capability



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The same interconnectedness that transmits risk can also transmit resilience. Energy security depends on shipping, ports, finance, telecoms, power, industrial suppliers, and government. Those systems in turn depend on reliable energy. The result is a web of reciprocal dependencies that no single corporation can fully manage.

The World Economic Forum's 2026 analysis explicitly links geoeconomic confrontation with disruption to systemically important supply chains, concentration of strategic resources, natural-resource shortages, and state-based conflict.[3] In energy, those connections are tangible: a maritime disruption can become a refinery-feedstock problem; a refinery problem becomes a product and logistics problem; higher fuel costs become an inflation and financing problem.

Collaboration does not require assumptions about a cooperative world. In a fragmented world, it becomes more pragmatic: identify mutual dependencies, pre-agree protocols where possible, and preserve channels that function under stress.

The collaboration agenda

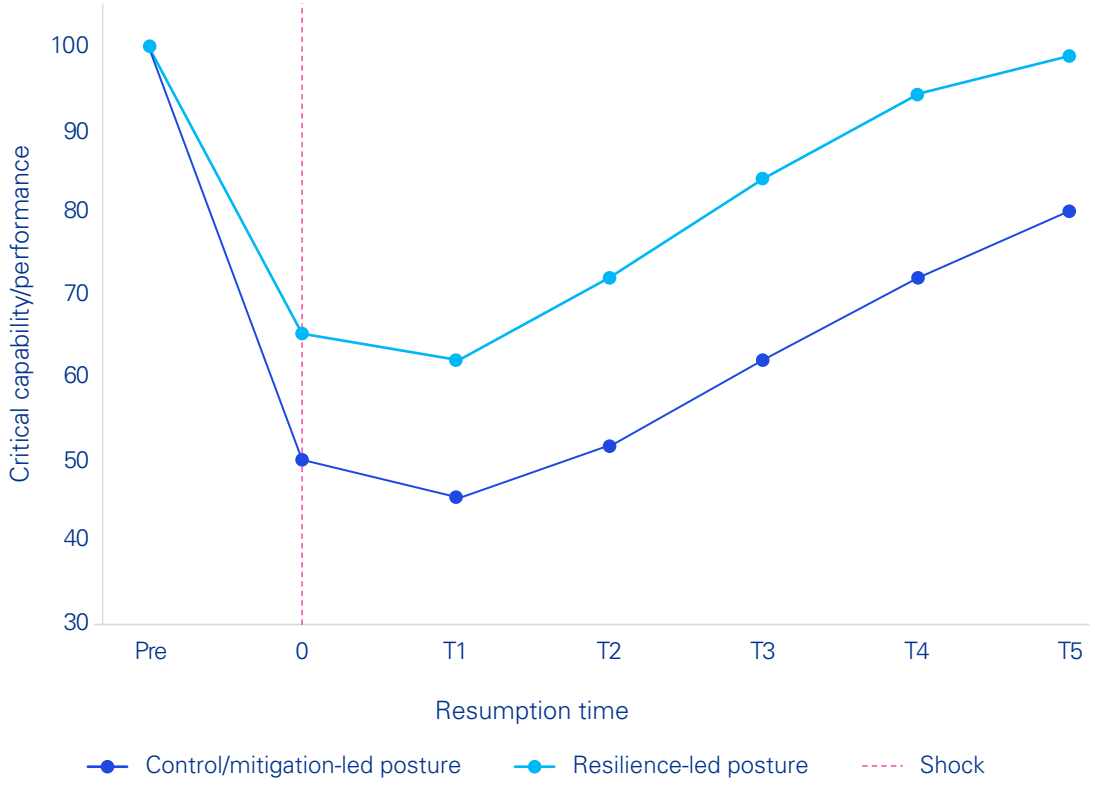
Across	What to share/coordinate	Potential common benefit
Energy + shipping/ports	Capacity, route status, recovery priorities, critical cargoes	Faster rerouting and restoration
Energy + finance/insurance	Exposure, liquidity needs, war-risk capacity, trade finance	Ability to avoid financial amplification of physical disruption
Energy + digital/telecom	Critical dependencies, cyber threat intelligence, recovery sequencing	Protection of cyber-physical continuity
Energy + mining/chemicals/ manufacturing	Critical inputs, demand priorities, substitution possibilities	Better allocation under scarcity
Energy + agriculture	Fertilizer and fuel availability, water and irrigation requirements, crop production risks, food supply priorities, land use trade-offs including the use of arable land for renewable energy versus food production	Stronger food security and reduced cascading impacts across energy and agricultural value chains
Corporate + government	Strategic stocks, emergency rules, infrastructure priorities	Coherent public-private response
Across geographies	Chokepoints, alternative corridors, reciprocal capacity	Resilience despite geopolitical fragmentation

[3] The Global Risks Report 2026, World Economic Forum, 14 January 2026

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Controls and mitigation remain foundational. But when the dominant risks are external, no feasible control environment can prevent every fall. Resilience asks a different question: **How much critical capability is lost, for how long, and how quickly can the organization restore or reconfigure it?**

Illustrative example of critical capability and restoration time



The curve in the chart is conceptual. A resilience-led organization may still experience a severe initial shock; its advantage is shallower degradation, faster stabilization, quicker recovery and greater ability to reconfigure. This shifts attention from incident counts toward recovery time, service continuity, liquidity endurance, substitution capacity and decision velocity.

A resilience-led organization also understands the critical importance of specific responses and how they work together. These levers can be used at different management levels of the organization and across different business functions, further enhancing a flexible yet tightly integrated approach to supporting resilience.

Four response levers work together

Lever	Purpose	Examples
Assess and control	Reduce preventable risk	Process controls, cyber hygiene, safety barriers, limits
Mitigate	Reduce or transfer exposure	Hedges, insurance, contracts, diversification
Build resilience	Absorb and recover	Buffers, alternate routes, modularity, crisis operating models
Reallocate capital	Change future exposure	Invest, redesign, acquire, divest, exit, build optionality

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

05

KPMG Dynamic Risk Assessment



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

> **The state of current geopolitics has made supply chains very unreliable. Supply chain security has become a core business continuity issue, and the assault on supply chains has become far too high and unpredictable.**

Anish De
Global Head of Energy
Natural Resources and Chemicals
KPMG International

We use a different approach to study risk. Traditional risk assessment methodologies have their roots in a simpler time when national economies were markedly more isolated. Our economies and societies today are more connected and interdependent than ever before — giving individual risks a wide variety of opportunities to interconnect and spread. As a result, while measuring the likelihood and severity of individual risks remains common, it is no longer adequate. Risk contagion and velocity must be measured as well.

KPMG Dynamic Risk Assessment (DRA) methodology is an evolution of traditional risk assessment designed to:

- Incorporate future trends and their potential downstream exposures into risk management processes, injecting a forward-looking analysis and assessment and making results no longer solely reliant on historical data
- Expand the analysis of resulting risks to estimate how these risks might connect to each other and the velocity (speed) by which the consequences will be felt once a risk occurs, in addition to more traditional measurements of severity and likelihood
- Apply the sciences of expert elicitation and behavioral finance to extract the information
- Use "knowledge graphs" that map the complex relationships between and among factors, as well as the magnitude, direction of travel, and impact of these factors

Based on this methodology, our DRA report seeks to capture the wisdom of a selected crowd of experienced professionals through a scientifically structured approach, harnessing their diverse collective knowledge and representing the findings mathematically as a network. This process can generate network-based insights that may be difficult to capture through a traditional two-by-two likelihood and severity heat map.

This approach is designed to produce a collective quantitative perspective and to reduce the influence of individual bias or dominance by any single individual. It draws on the judgment of an industry or issue's most capable thinkers, embedding their views on present and emerging risks into a mathematical network through a structured, scientific, and replicable process. When applied rigorously, expert elicitation can yield insights during periods of rapid environmental, macroeconomic, and geopolitical change that are more insightful than those generated by any single expert model or forecast.

The DRA exercise was conducted during June — August 2026. It analyzed responses by senior leaders from across sectors, including economists, geopolitics experts, and functional specialists who identified the supply chain imperatives given energy-linked disruption and geopolitical uncertainty for the various sectors. Click here to explore the 20 risks assessed as part of the DRA.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

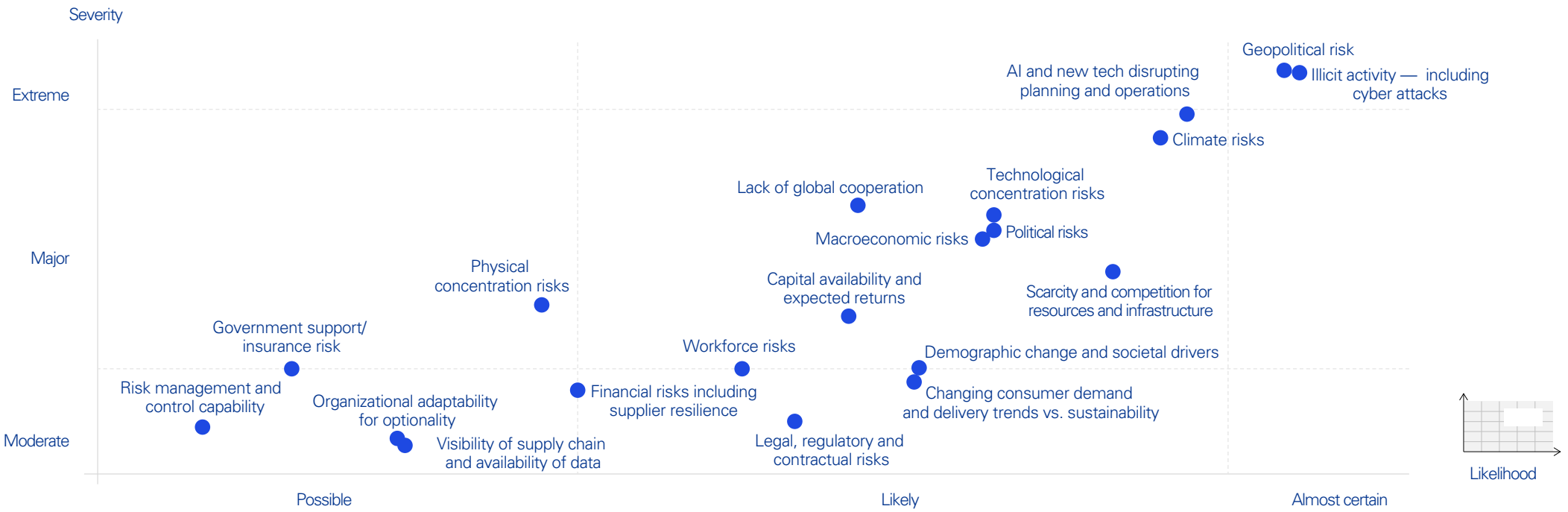
06

Global and regional risks and opportunities



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Global supply chain risks — Severity and likelihood



Note: In assessing risk, the two concepts of severity and likelihood are best considered together since each one involves the other. Throughout our DRA survey, geopolitical risks often played a prominent role in responses, followed closely by cyber attacks, new technology including AI, and climate change. A key observation is that visibility of supply chains and data availability were considered less important compared to other risks.

As illustrated in the chart, the ongoing conflict in Iran is increasing risk across multiple markets, starting with the supply of oil, which in turn affects related markets such as fertilizers. Russia's war against Ukraine adds further global risk to food supplies such as wheat. Disputes between the US and China range from technology to trade agreements, and these issues have introduced new levels of supply chain risks across the Pacific and around the world. These geopolitical risks are almost matched by AI, technology, and cyber attacks.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Other developments include the massive consolidation of sources and suppliers, talent scarcity (and also AI-driven job cuts), and attacks on infrastructure such as cutting cables, the destruction of desalinization plants, cyber attacks on data centers, etc.

At the regional level, these global risks are accompanied by a number of issues unique to each region. In the Americas, supply chain risk is increasing due to the changing roles, policies, and ambitions of the US. Currently, these new developments involve the ongoing conflict in Iran, tensions between the US and NATO, increased competition with China, and reassessments of trade agreements such as USMCA. Risks in the US also include AI development (and pushback against AI), political tensions, and changing state and federal regulatory environments. Companies are changing from just-in-time to just-in-case supply chains as they work to contain costs without compromising performance.

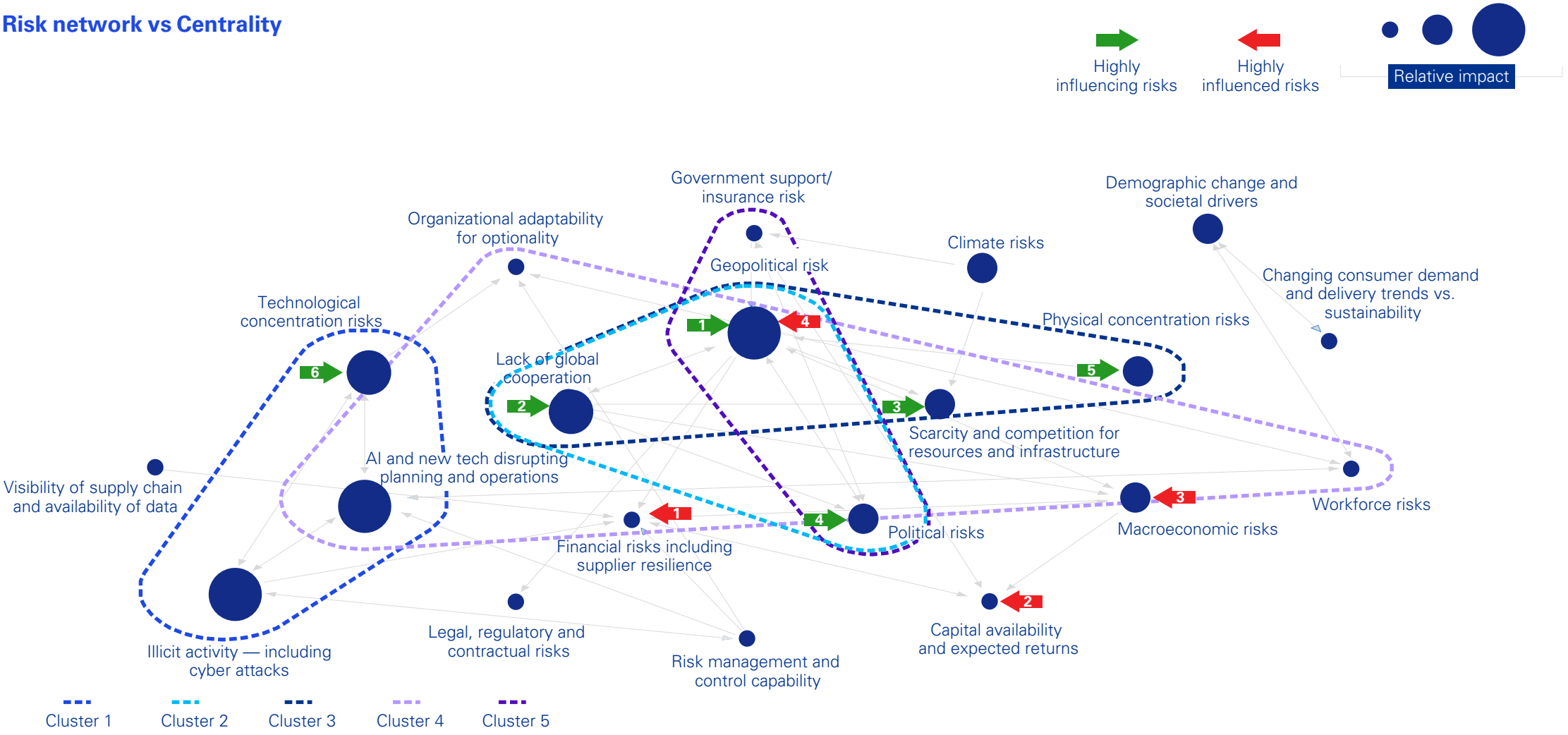
In Europe, the Middle East, and Africa, military action is a local issue with global economic implications. The Russia–Ukraine stalemate has lasted more than four years. The conflict has affected inflation, GDP growth, trade, and industrial capacity across Europe. Europe is reconsidering its energy dependence on Russia and increasing their defense budgets. The disruption of the Strait of Hormuz and attacks on regional energy infrastructure has destabilized global oil and LNG markets, directly affecting Europe's energy system. These military actions have increased supply chain risks across the region, compounded by increased market competition with Chinese manufacturing, rapidly changing US tariff policies, rising input and production costs, regulatory mandates, rising national debt levels, and the lack of guaranteed access to rare earths and strategic metals.

Across the Asia Pacific (ASPAC) region, the growing presence of China is inescapable, both as the leading market and supplier of goods and services. However, an era of global multilateralism is ending with no clear replacements to that order. China will likely continue to dominate the regional economy, but countries are adopting a more nationalistic position, showing less confidence in traditional supply chains as they pivot away from the Middle East for energy supplies or renegotiate trade agreements. Rapid growth is increasing the risk of 'bigger is better' — companies depending on a fewer number of larger sources. Growth can also impede multi-tier supply chain visibility. Other risks include widespread inflation and cost escalation, legal and regulatory instability, cyber risks, changing tariff policies, and uncertain access to working capital.

> "We're seeing movement by corporates in terms of understanding where there are pinch points in the supply chains by geography and not just by product, while also seeking ways to get more real-time feedback on risks to those supply chains."
>
> **Roy Waligora**
> Global Lead for Third Party Risk Management
> KPMG in the UK

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risk network vs Centrality



Note: Centrality is a useful way to quickly assess the key risks in a crowded field of multiple risks The red and green distinction between highly influenced and highly influencing risks adds another important element in assessing risks.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risks seldom happen in isolation. For example, geopolitical tensions can exacerbate the occurrence and magnitude of cyber-attacks, especially in an age of hybrid warfare. The interconnectivity of global supply chain risks is well reflected in the DRA network diagram, which shows how risks can directly, and in turn, indirectly influence and be influenced by all the other global supply risks.

Certain risks are more 'vulnerable' or influenced by the other supply chain risks, such as the financial risks pertaining to supplier resilience, or the risk that capital may not be available to invest in new supply chains or infrastructure. These risks are all exacerbated by risk interconnections and dependencies. Correspondingly, if certain risks were reduced, contained, or terminated, that would be influential and highly beneficial in mitigating the entire risk network. These risk dynamics are relevant to all supply chains, which by their very nature cross and interconnect multiple geographical, political, economic, and technological areas.

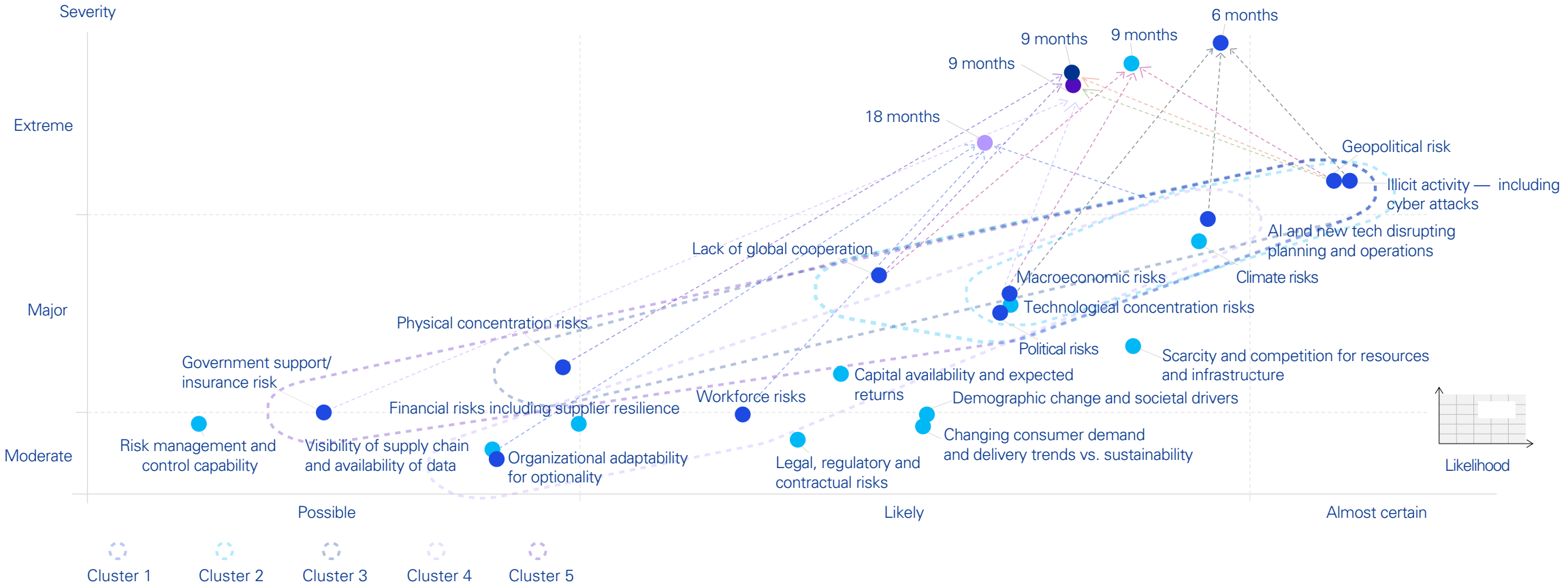
While a network perspective of risks reveals the most influencing and influential of risks and their transmission effects, the identification of groups of risks that are most expected to occur in combination (or, 'clusters'), clearly present valuable opportunities for scenario planning, and stress testing.

The DRA exercise identified five risk clusters depicted in the colored cluster shadings above, tabulated below, and labeled thematically. For example, cluster 4 'Future-ready organizations' is comprised of the three risks of 'AI and new tech disrupting planning and operations', organizational adaptability for optionality' and 'workforce risks'. If any one of these three risks occurs, it is expected that it will trigger and/or make more severe the other two risks in its cluster, resulting in a cumulative 'extreme' severity impact which is more severe in impact than any other individual, discrete risk. Should one of these risks occur in this cluster, then the consequential negative effects on supply chains and GDP could be felt within 18 months.

In summary, by virtue of risk interconnectivity and in the context of current geopolitical uncertainty and energy disruptions, the overall threat to global supply chains is far greater than currently meets the eye. Organizations across sectors and geographies would do well to revisit their risk management practices with a view to transformation and resilience.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risk clusters and velocities



Note: As we have identified, risks cannot be considered in isolation, and that applies to time and velocity as well. Every initiative for increasing supply chain resilience must be continuously monitored for progress and tracked according to regular milestones. They must also be a part of a company's strategic, long-term planning.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risk clusters

Cluster	Risks	Cluster themes	Severity
1	AI and new tech disrupting planning and operations, Illicit activity — including cyber attacks, Technological concentration risks	Tech vulnerabilities	**Extreme**
2	Geopolitical risk, Lack of global cooperation, Political risks	Changing world-order	**Extreme**
3	Geopolitical risk, Lack of global cooperation, Physical concentration risks	Physical concentrations	**Extreme**
4	AI and new tech disrupting planning and operations, Organizational adaptability for optionality, Workforce risks	Future-ready organizations	**Extreme**
5	Geopolitical risk, Government support/insurance risk, Political risks	Risk pooling/ Insurance	**Extreme**



Note: Another way to understand the interconnectedness of risks is to recognize how they often occur in clusters. Each cluster can be identified by overarching themes such as tech vulnerabilities and changing world order. In effect, a risk cluster is three or more risks that are so bidirectionally connected that if one of those risks occur, all the risks in the cluster will occur.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

07

Cross-sector risks and opportunities



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

> There's a lot of diversification, redundancy, and options being built … but this paradigm shift from efficiency to resilience comes at a cost, particularly in the short term.

Stefano Moritsch
Global Geopolitics Lead
KPMG International

Automotive: Resilience is no longer a crisis response

For automotive companies, supply chain resilience is increasingly shaped by three interconnected risk domains: energy, geopolitics, and evolving operating models.

Energy has become a strategic factor as Automotive manufacturers face volatile costs, infrastructure constraints, and growing competition for power from technology companies and data-center operators. At the same time, energy is influencing the economics of electric mobility, from battery production to charging infrastructure and consumer adoption. Companies that align energy strategies with their EV ambitions, particularly in China, are gaining a competitive advantage.

Geopolitical uncertainty and sustainability discussions are as well strongly impacting the automotive landscape. Trade disputes, tariffs, sanctions, and shifting customs frameworks are forcing OEMs and suppliers to rethink sourcing, production footprints, and market access decisions. As automotive value chains become more regionalized, companies must balance efficiency with resilience. At the same time, differing regulations, from supply chain due diligence requirements in Europe to localization policies elsewhere, are adding further complexity.

These developments are amplifying supply chain risks at a time when the transition to electrification and software-defined vehicles is already fundamentally changing operating models. Increasing dependence on critical minerals, batteries, semiconductors, and specialized software capabilities are aligned to these developments. Combined with supplier disruptions, logistics bottlenecks, financial instability, and quality risks across supplier networks, supply chains are becoming more exposed and more complex in the automotive industry than ever before.

As a result, resilience is moving from an operational priority to a strategic imperative. Yet resilience cannot be built the same way in every market. Differences in energy availability, regulatory frameworks, geopolitical exposure, and industrial ecosystems require companies to combine global coordination with regional adaptation. The ability to anticipate disruption and respond decisively will increasingly determine competitiveness and long-term growth.

> Resilience is no longer a crisis response. It has become a core leadership capability. The companies that succeed will likely be those that can steer the transition from fossil-based to carbon neutral electrification across products and operations, navigate increasingly divergent regional market conditions, secure critical supply ecosystems, and adapt quickly to a more complex risk environment.

Dr. Andreas Ries
Global Head of Automotive
KPMG International

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consumer and Retail: Managing interconnected risks across the value chain

For consumer and retail companies, resilience can no longer be built around known risks alone. The sector spans agricultural production, raw material sourcing, manufacturing, consumer goods, apparel and textile production, beauty and personal care supply chains, logistics, distribution and retail, where geopolitical fragmentation, trade realignment, technological disruption, climate pressures and resource constraints increasingly interact in unpredictable ways.

Producers, manufacturers, suppliers and retailers across consumer sectors are managing rising energy, fertilizer, labor and transportation costs, alongside climate-related disruption and volatile commodity markets. Recent increases in cocoa prices, disruptions to grain and fertilizer markets, and ongoing trade tensions have demonstrated how quickly shocks can move through the value chain.

New pressures are also emerging. Tariffs continue to reshape global sourcing and manufacturing footprints, while the rapid expansion of AI infrastructure is increasing demand for energy, water and land. Although these trends may appear unrelated, they increasingly compete for the same resources. Growing demand for power, water and suitable land in one part of the economy has the potential to influence costs, availability and investment decisions elsewhere, including across agriculture, manufacturing, consumer products production and logistics.

For consumer goods companies and retailers that are operating in a low-margin environment, those pressures are often difficult to absorb. What begins as an input cost, resource or supply challenge further upstream can quickly affect margins, product availability, affordability and consumer demand. At the same time, changing consumer expectations continue to raise the stakes, requiring organizations to respond to shifting purchasing behaviors, evolving preferences and higher expectations around availability, service and product choice.

A resilience strategy is therefore about more than managing risks within their own operations, but is intrinsically linked to the resilience of the wider ecosystems, supply networks and resource systems that underpin consumer and retail value chains.

> “Regarding resilient food supply chains, I think there is a real need to be thinking about what a low-carbon future environment looks like and how economic models could evolve to improve outcomes at both ends of the value chain for farmers, growers and consumers.”
>
> **Ian Proudfoot**
> Global Head of Agribusiness
> KPMG International

> “One of the biggest shifts we’re seeing is from managing individual physical flows of goods to managing the interdependencies within broader industry ecosystems that underpin long-term performance.”
>
> **Isabelle Allen**
> Global Head of Consumer, Retail & Leisure
> KPMG International

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Financial Services: Resilience as a competitive advantage

The Financial Services sector is addressing new risks and demands for resilience driven by nationalism, shifting international trade relationships, cyber crime, changing regulations, and new technology.

Nationalism is driving a more insular, protectionist stance around the world. Countries are making business decisions based on short-term, politically expedient reasons instead of long-term gain. Protectionism is often encouraging an over-reliance on one supplier or group of domestic suppliers, thereby reducing resilience, and adding risk to the delivery of services across borders.

Sector organizations recognize innovative technology such as AI as a way to support increased security, efficiency, and compliance. But they are also aware that this technology can be a potential tool for cyber crime, fraud, theft, and reputation damage. This increases the need for internal monitoring as well as more third-party risk management, including the need for greater visibility into second-, third-, and fourth-level suppliers.

Human rights and labor laws present another risk area, so resilience requires organizations to maintain their sustainability goals and continue monitoring for compliance.

Despite the cost and effort required for supply chain resilience, organizations can consider investments in supply chain and third-party risk management as a competitive advantage rather than simply a compliance requirement. Proper monitoring can identify vulnerabilities, inefficiencies, and potential opportunities for supply chain improvements leading to increased security, cost-efficiency, and revenue.

> “A big risk is assuming that supply chains just work because globalization has worked in our favor for so many years.”
>
> **Frank Pfaffenzeller**
> Global Head of Insurance
> KPMG International

> “To make supply chains more resilient, you can diversify a base of energy sources and suppliers. You want as many options as possible.”
>
> **Geoff Rush**
> Global Head of Banking and Capital Markets
> KPMG International

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Industrial Manufacturing: Resilience for the future

Industrial manufacturers face four primary risks: global uncertainty, changing global demographics, insufficient knowledge sharing between organizations and governments, and risking protectionism and nationalism. Together, these forces are creating a more complex and unpredictable operating environment, challenging organizations to rethink how they build and sustain resilient supply chains.

While organizations in the Industrial Manufacturing sector often depend on significant capital expenditures, global uncertainty is discouraging commercial investments, especially over the long term. In addition, changing global demographics are increasing uncertainty about where food and energy will be needed. The lack of sufficient knowledge sharing between organizations and governments only exacerbates these risks and hampers supply chain resilience. Protectionism and nationalism add further risks such as the hoarding of rare earths and strategic metals.

Mitigating these risks requires a serious commitment to strategic planning and redesigning their supply chains. Organizations can consider a transition to near shoring or friend shoring with business and government allies. These restructurings can involve multiple sectors such as Automotive or Defense, thereby leveraging greater market demand and improving resilience.

Energy supply can be improved with innovative technology. Manufacturers are increasingly diversifying their energy and power supply using onsite distributed generation (such as commercial solar, combined heat and power, and microgrids) backed by multi-sourcing geographic procurement strategies to insulate operations from rising grid costs, capacity constraints, and volatile lead times. Other planning involves hiring workers and upskilling the existing workforce to increase productivity and support new and more sophisticated ways of working.

The greatest risk remains an over-reliance on old technologies, old manufacturing processes, and old assumptions about unlimited access to resources and backup suppliers. Supply chain resilience cannot be assumed, but proper planning can mitigate risks and improve supply chain performance, both now and in the years ahead.

> “With the advent of additive manufacturing, advanced manufacturing techniques, and 3D printing, we can really change how we look at supply chains and redesign the supply chain model altogether.”
>
> **Jonathon Gill**
> Global Head of Industrial Markets and Aerospace
> KPMG International

Infrastructure and Transport: Dealing with significant growth

Global infrastructure investment is accelerating across sectors and geographies simultaneously, creating an environment in which demand is increasingly outstripping available capacity. The result is intensifying competition for specialist skills, manufacturing capability, critical materials, energy, water and suppliers, removing the historic ability to shift scarce resources between markets as investment cycles rise and fall.

The most significant vulnerabilities may sit deep within the supply chain and outside traditional areas of focus. Relatively small dependencies, such as highly specialized equipment or workers, can become critical bottlenecks capable of delaying multibillion-dollar programs by years. These constraints, combined by geopolitical uncertainty, tariffs, and energy-price volatility, make costs and availability of supply increasingly difficult to predict over 10-to-20-year infrastructure investment horizons.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Stop start investment cycles and underinvestment in technology has constrained sector productivity. AI, automation, modularization and industrialized construction offer the potential to fundamentally change how infrastructure capacity is delivered.

Building resilience requires a shift from transactional, project-by-project procurement to long-term, portfolio-led capacity planning. Infrastructure owners need deeper visibility into lower-tier dependencies, stronger strategic supplier relationships, and a clear view of demand over the next decade and beyond. This enables them to aggregate requirements, provide suppliers with greater certainty, stimulate investment in new capacity and secure preferential access to constrained supply.

> Unpredictability around global supply chains means that organizations need to move from supplier relationships to long term partnerships and work harder to understand lower-tier dependencies. Organizations that actively secure or create capacity will be better positioned to manage disruption, protect delivery and gain competitive advantage in an increasingly constrained global infrastructure market.

Lisa Kelvey
Global Head of Infrastructure and Transport
KPMG International

Technology, Media and Telecommunications: Bringing the world together

The Technology, Media and Telecommunications (TMT) sector plays a central role in the modern economy, connecting people, businesses and governments through the digital infrastructure, platforms, networks and services that enable communication, commerce and innovation. As organizations accelerate the adoption of AI, cloud computing and data-driven technologies, resilience increasingly depends on understanding and managing a complex web of interconnected dependencies. Reliable energy supplies, digital infrastructure, global supply chains and trusted ecosystems are all critical enablers of growth and innovation. Disruption in one area can quickly cascade across others, while geopolitical tensions, regulatory uncertainty and resource constraints amplify vulnerabilities across the system.

This interconnectedness is particularly evident in the infrastructure that underpins the digital economy. Data centers, telecommunications networks, subsea cables and cloud platforms are increasingly viewed in many jurisdictions not only as commercial assets, but also as strategic national infrastructure. Concerns around sovereignty, national security and technological independence are influencing government policy, investment decisions and cross-border business operations. At the same time, cyber attacks, state-sponsored threats, trade restrictions and shifting international alliances are creating new challenges for organizations operating across global markets.

The rapid growth of AI is further intensifying these pressures. AI innovation depends on access to advanced semiconductors, critical minerals, energy capacity, computing infrastructure and highly skilled talent. Constraints or disruption in any part of this ecosystem can have significant knock-on effects for technology providers, telecommunications operators, media organizations and the broader industries that increasingly rely on digital services.

Building resilience therefore requires organizations to look beyond individual risks and strengthen the resilience of the wider ecosystem on which their operations depend. This includes understanding critical services and dependencies, strengthening cyber and operational resilience, and embedding resilience considerations into strategic, investment and technology decisions. The most resilient organizations will likely be those that can not only withstand disruption, but also adapt at pace, maintain customer trust and continue to innovate amid increasing uncertainty.

> TMT companies rely on substantial energy resources to power the digital infrastructure that underpins today's economy. They are looking to diversify where their energy is coming from and become much more self-sufficient with self-generation.

Anna Scally
Global Head of Technology, Media, Telecommunications
KPMG International

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

08

Building the capabilities for resilience



AI generated image

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Technology can be both a risk and an opportunity. Technology and AI disruption were cited by respondents of our pulse survey as key risks for their organization over the next two years. But AI and predictive analytics, scenario planning and stress testing, and alternative sourcing strategies were cited most often by respondents when asked about the actions they are prioritizing to strengthen resilience. At the same time, technology offers the opportunity to move beyond standalone dashboards toward more integrated decision architectures that can make external risk, transmission, consequence, and response more visible and computable.

Capability	CEO/CXO question	Role
Risk Control Tower	What is changing and what needs attention?	Continuous sensing, connection, assessment and escalation
Risk Compounder	Which risks are reinforcing one another?	Interaction intelligence, cascades, amplification, break-points
Strategic Optionality Engine	What can we do, and what is the option value?	Generate, compare and trigger response options
Risk Digital Twin	If this state changes, what happens through the enterprise?	Twin sources, flows, stocks, dependencies and economics for simulation

The control tower is the natural first step because it creates the information and integration spine: external sensing, enterprise context, graph relationships, provenance, timing, and executive escalation. Once that spine exists, the organization can add deeper analytical modules without rebuilding the foundation. The application space for the control tower could well extend beyond the supply chain area. Indeed, in the modern enterprise and the current operating context, it is impossible to assess the supply chain independent of other connected business functions and overall enterprise performance.

The KPMG ENRC Global Tech Report 2026 highlights digital twins among the emerging technologies energy leaders are considering as a key investment. Technologies like digital twin can simulate real-time environments and modeling scenarios to support smarter decisions. In fact, 78 percent of organizations aim to be scaling up or fully scaled in advanced simulation and digital twin by 2026.[4] Value realization will depend on strong data foundations, governance, and enterprise-wide implementation. Those requirements are directly relevant to risk technology: sophisticated models without trusted context create false precision.

64%

of respondents say technology and AI disruption will have the greatest impact on their organization over the next two years

Respondents are prioritizing the following actions to strengthen resilience:

49% AI and predictive analytics

44% Scenario planning and stress testing

39% Alternative sourcing strategies

[4] KPMG Global tech report 2026: Energy, Natural Resources and Chemicals, KPMG, February 2026

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

09

Building a risk-aware culture



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The operating model must change with the risk model. A controls-based process managed primarily by the CRO can remain effective for compliance and internal control, but it is not sufficient for external, strategic and cross-functional risks.

The CEO/CXO model does not displace the CRO. It changes the CRO's role from owner of a periodic risk process to orchestrator of enterprise risk intelligence, challenge and response — alongside strategy, finance, operations, supply chain, technology and business leadership.

The board and C-suite should repeatedly ask:

- **What is changing?**
- **What is interacting?**
- **How does it reach us?**
- **What critical capability is at risk?**
- **What can we change now?**
- **When does this become structural rather than temporary?**

Traditional posture	Resilience-led posture
Risk discussed periodically	Risk embedded in strategic and tactical decisions
Risk ownership concentrated in specialist functions	Business and functional leaders own exposures and response choices
Focus on likelihood/impact ratings	Focus on pathways, thresholds, velocity, vulnerability and options
Escalation after internal impact becomes visible	Escalation when external signals and pathways become decision-relevant
Mitigation plans owned risk-by-risk	Response portfolios designed for compound scenarios
Lessons captured after events	Models, assumptions and decision rules recalibrated continuously

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risk governance becomes decision governance

A modern risk system culminates in a small number of decisions, not a large number of risk reports. The governance design therefore needs explicit thresholds, owners and decision rights.

Role	Primary contribution
Board	Risk appetite, resilience ambition, structural exposure, and capital choices
CEO/ExCo	Cross-business trade-offs, enterprise priorities, escalation, and strategic response
CRO/Risk	Risk architecture, challenge, integration, scenario discipline, and independent view
CFO/Treasury	Liquidity, financial transmission, hedging, capital capacity, and value-at-stake
COO/Supply/Trading	Physical exposure, substitution, continuity, and operational response
CIO/CISO/Data	Technology dependencies, cyber resilience, data trust, and analytical platform
Strategy/Corporate Development	Optionality, portfolio consequences, and invest/divest/partner choices

Useful performance measures include the percentage of priority alerts judged decision-relevant, anticipation lead time before material impact, critical dependencies mapped, time from signal to validated enterprise view, time to executive decision, recovery performance, and the rate at which assumptions are updated after events.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

10

Transformation path: Seed, spread, embed



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The end-state is enterprise-wide, but the starting point should be deliberately narrow. Today's risk is inherently cross-functional, but trying to transform every risk process, data source and business unit simultaneously will hamper learning and dilute ownership. A target end-state is for leaders to identify material external changes earlier, understand enterprise pathways, assess compounding risks, estimate value at stake, compare response options, and clarify decision rights before disruptions escalate internally.

Phase	Objective	Illustrative actions	Exit test
Seed	Prove decision value in one business/risk domain	Select one high-value scenario; map exposures and pathways; integrate public and selected internal data; build executive workflow	Leaders make a better/faster decision than with existing process
Spread	Extend the proven patterns	Add businesses, scenarios, dependencies, response modules and common data objects	Cross-business decisions use the same risk language and state model
Embed	Make it part of management	Integrate into planning, capital allocation, operating reviews, crisis governance and Board reporting	Risk intelligence changes routine strategic and tactical choices

A practical 12-month roadmap

0-8 weeks
Define 25-40 enterprise-significant risks; choose environment; map 5-10 compound scenarios; inventory data and decisions.

2-4 months
Build control tower demonstrator; external sensing; enterprise graph; a centralized digital dashboard; pathway and trigger logic.

4-8 months
Connect selected internal exposures; add compounder and response option objects; establish governance and validation.

8-12 months
Add digital twin, integrate with planning and capital processes; spread to adjacent businesses.

What good looks like and what to avoid

A CEO should be better positioned to see a material external change, understand how it reaches the enterprise, see which risks are compounding it, quantify the critical capability and value at stake, compare response options, and know which decision is required — before the disruption becomes an internal surprise.

Equally important, CEOs should have some guardrails designed to avoid situations like the following:

- Starting with a giant taxonomy or exhaustive risk graph
- Treating AI-generated correlations as causal relationships
- Building dashboards before defining executive decisions
- Assuming supplier diversification removes shared route or infrastructure dependencies
- Using a single black-box risk score where mechanism and uncertainty matter
- Separating resilience investment from capital allocation
- Scaling technology before the organization has learned how it wants to use the insight

Within these objectives, methods and guardrails, each organization needs to determine the pathway that serves its context without losing the perspective of a radically altered operating environment.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Conclusion

From risk reduction to enterprise adaptation

Energy is not a new source of uncertainty. What is different now is the density of connections, the external origin of many threats, the speed at which they spread, and the declining reliability of assumptions that once underpinned diversification, contracts, and stable trade corridors.

The central question is no longer whether the next disruption can be predicted. It is whether the organization has built the intelligence, resilience, and optionality to remain effective when the future refuses to play out as planned or envisaged. The response is not to abandon traditional risk management. It is to place it inside a broader resilience architecture. Controls reduce preventable failures. Mitigation reduces or transfers exposure. Resilience protects critical capability when prevention fails. Capital reallocation changes the organization's future exposure and creates strategic optionality.

Technology can now support that architecture in ways that were previously impractical: continuous sensing, knowledge graphs, compound-risk analytics, option engines and digital twins can connect external change to enterprise consequence. But technology is only useful when paired with trusted data, explicit mechanisms, governance and a management culture willing to act on weak signals before certainty arrives.

For large organizations, the pragmatic path is seed, spread and embed. Begin where the external system meets the enterprise most visibly. Prove that the new architecture improves a real decision. Spread what works. Then embed risk and resilience into the way the organization allocates attention, resources, and capital.

How KPMG can help

KPMG helps organizations transform their supply chains by combining deep industry experience, tested methodologies, advanced analytics, AI enabled decision intelligence, and technology solutions intended to support more resilient, responsive, and cost-effective supply chains. KPMG also offers strong alliances with major technology vendors and the ability to integrate strategy, operations, technology, and sustainability into one transformation program.

Specific offerings can include DRA surveys, scenario modeling, supplier visibility mapping and enhancements, energy resilience improvements, and governance advisory. KPMG can also develop platforms for supply chain analytics with AI, logistics and supply network optimization, and other technology enhancements for added supply chain optimization.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Authors



Anish De
Global Head of Energy, Natural Resources and Chemicals
KPMG International

Anish serves as the Global Head for Energy, Natural Resources and Chemicals (ENRC) bringing more than 25 years of experience. Anish is an acclaimed energy sector expert, having pioneered work in corporate strategy, reform and restructuring, policy and regulation, commercial and financial advisory, capital projects, energy markets, smart grids and digital.



Stefano Moritsch
Global Geopolitics Lead
KPMG International

Stefano leads KPMG's efforts, globally, helping companies and governments deal with today's geopolitical challenges. By joining the dots between the macro political trends and their commercial implications in various sectors, Stefano helps global businesses not only survive but thrive in geopolitical volatility.



Roy Waligora
Lead for Third Party Risk Management
KPMG in the UK

Roy is a Chartered Accountant and Head of Investigations and Corporate Forensics at KPMG in the UK. He has been conducting forensic investigations and disputes in many countries for 21 years. Roy has acted on behalf of several regulators and many multinational clients to conduct regulatory driven financial investigations of fraud, financial statement misstatements, misconduct and money laundering — often together with leading law firms in cross border work.

Acknowledgments

Thank you to all KPMG participants involved in the DRA, and to the KPMG cross-sector leaders for their valuable contributions and expertise:

Anna Scally
Global Head of Technology, Media, Telecommunications
KPMG International

Dr. Andreas Ries
Global Head of Automotive, KPMG International

Frank Pfaffenzeller
Global Head of Insurance, KPMG International

Geoff Rush
Global Head of Banking and Capital Markets, KPMG International

Ian Proudfoot
Global Head of Agribusiness, KPMG International

Isabelle Allen
Global Head of Consumer, Retail & Leisure, KPMG International

Jonathon Gill
Global Head of Industrial Markets and Aerospace, KPMG International

Lisa Kelvey
Global Head of Infrastructure and Transport, KPMG International

We extend our sincere thanks to the DRA Centre of Excellence, led by Dr. Kerry Jenkins, Global Lead, DRA CoE, KPMG International, for their research, analysis, and contributions that helped inform this report.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Methodology

KPMG risk and resilience pulse survey methodology

A portion of the quantitative data in this report is based on a global pulse survey conducted by Ipsos on behalf of KPMG International's Energy, Natural Resources and Chemicals practice. The research explored how organizations are responding to an increasingly complex risk environment shaped by geopolitical uncertainty, cyber threats, supply chain volatility, climate-related events, and energy-related disruptions.

A total of 109 senior executives and business leaders participated, representing organizations across Automotive, Consumer and Retail, Financial Services, Industrial Manufacturing, Infrastructure and Transportation, Technology and Telecommunications, and Energy, Natural Resources and Chemicals. Respondents held leadership roles spanning executive management, finance, operations, risk, technology, supply chain, strategy, and transformation.

The survey was conducted across major global markets including Australia, Brazil, Canada, China, France, Germany, India, Ireland, Italy, Japan, Korea, Mexico, the Netherlands, Saudi Arabia, South Africa, Spain, Switzerland, the United Kingdom, and the United States. Topics included risk exposure, resilience maturity, supply chain vulnerabilities, energy security, disruption preparedness, and resilience priorities over the next three to five years.

Results reflect participant views in September 2026.

DRA methodology

The other quantitative portion of this report is the DRA methodology which comprises four steps that can be applied at industry, company, business unit, project, and risk theme levels.

- The first two steps form the risk identification phase, which aims to capture past risks that may re-occur, over-the-horizon risks, and completely new risks.
- The third step introduces technology into the process in the form of an interactive software tool. The tool facilitates the collection and quantification of independent, anonymous expert views on relevant risks.
- The fourth and final step identifies key steps for prioritization, mitigation, and controls as numerical analyses highlight historically unobservable risk combinations and relationships.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Overview of the DRA methodology as applied by KPMG to answer the question: In the light of geopolitical challenges, and the impacts on energy, what are the risks to supply chains?

Step 1

Expert identification and interviews

A total of 56 experts were interviewed for their perspectives on supply chains. Their background includes a variety of roles across KPMG, multiple continents, and different parts of the value chains. They represent the following sectors and specialist areas:

- Energy and Natural Resources
- Infrastructure
- Consumer and Retail
- Automotive
- Industrial Manufacturing
- Technology, Media and Telecoms
- Financial Services
- Risk Services
- Geopolitics
- Economics

Individual interviews were structured in accordance with Expert Elicitation protocols and were conducted with a cross-section of these experts. The objective of the interviews was to obtain a base-level understanding of supply chain risks across sectors.

Step 2

Workshops

Experts from across sectors and the specialist areas participated in a group interview process, structured in accordance with Expert Elicitation protocols. This included de-biasing training elements techniques and guidance to consider both internal and external risks, as well as trends that may pose current or downstream risk consequences to supply chains.

Step 3

Risk estimation

Each expert was invited to access and complete KPMG's patented, interactive software tool which facilitates the collection of data points on their individual perspective of the four dimensions of each risk:

- Likelihood
- Severity
- Interconnectivity
- Velocity

The survey is scientifically structured to:

- Apply non-linear thinking processes
- Reduce the effects of survey fatigue
- Debias results
- Avoid categorical analyses
- Promote continuous-valued data collection
- Support consistent quantification of even the most challenging risks

Step 4

Analysis and discussion

A risk network was generated and analyzed to produce key insights.

We presented the results back to the experts and discussed the findings with them.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

DRA scales

Risk rating criteria severity

Criteria	Event leading to a loss of 0% of real GDP growth which is 3.44% in 2026	Value of impact — loss of real GDP growth in x% per annum
Extreme	100%	>3.44% (no growth or recession)
Major	33%	1.14% (a loss of 1.14% from real GDP growth)
Moderate	11%	0.38% (a loss of 0.38% from real GDP growth)
Low	3%	0.1% (a loss of 0.1% from real GDP growth)
Minor	0.1-1%	0.03% (a loss of 0.03% from real GDP growth)

Risk rating criteria — Likelihood

Description	Likelihood of risk occurrence (% probability per year)
Almost certain	90%
Likely	50%
Possible	25%
Unlikely	10%
Rare	5%

Risk rating criteria — Velocity



© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

20 key risks

Risk name	Risk description
AI and new tech disrupting planning and operations	Tech evolution such as AI, quantum, ICE-to-EV, 3D, advanced manufacturing, smart materials, satellite data. Innovative tech is triggering unexpected demand peaks, diverting capital away from the physical economy, and creating new dependencies. This is both an opportunity and a threat.
Capital availability and expected returns	Reduced availability of capital/funding to invest in new supply chains and infrastructures. For example, AI investment is currently reducing available capital and hampering investment in sectors such as Defense. This situation is exacerbated by a mismatch between required investment periods and short-term investor return expectations.
Changing consumer demand and delivery trends versus sustainability	Changing consumer preferences that distort consumption patterns and buying behavior. For example, a surge in instant commerce during games is straining technology and energy systems. Affordable GLP-1s will potentially affect resource supply chains.
Climate risks	Climate change and extreme weather, heat, drought, and other climate effects. These events can disable transport, ports, rail, routes, and productive capacity. They can reduce raw material availability and boost operating costs. They can also increase the importance of sustainability factors such as the environment, decarbonization, and the circular economy.
Physical concentration risks	High dependence on one geography, country, supplier, or transport route. This physical concentration can involve energy, critical minerals and materials, refining capability, or logistic chokepoints such as the Hormuz Strait. It exposes supply chains to disruption, ecosystem lock-ins, price leverage, and loss of continuity.
Technological concentration risks	Migration to cloud technologies through a limited number of hyperscalers and LLMs. This can result in risks involving access to technology and continued operational control. Similarly, denial of access to international payment systems affects operations and supply chains.
Political risks	Unstable political regimes, changing political cycles and policies, and politically driven export controls. These risks can involve rising nationalism and corruption, with an 'every country for itself' attitude. In general, political risks involve the lack of alignment between government and industry. Policy interventions can override economics and require corporations to make decisions not for business reasons but to exclude foreign owners and suppliers.
Demographic change and societal drivers	Aging populations, lower birth rates, and public opinion. Changing societal structures drives politics and spending on public assistance programs and pensions. Other drivers include ideological differences involving western lifestyle aspirations or community backlash involving data centers, nuclear plants, and transmission lines.
Geopolitical risk	Growing uncertainty about a predictable world order and freedom of the seas. Global order and free passage have traditionally enabled supply chains. Risks include increasing polarization between the US and China, wars, conflicts and interference that disrupts trade flows. Also, the lack of trust, growing localization, and friend/nearshoring which impacts supply chains.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Risk name	Risk description
Government support/insurance risk	Decreased availability of insurance and risk pooling. In the face of force majeure declarations, wars or other crisis-zone risks, ships and other supply chain participants may lose their coverage. If governments do not intervene, trade through exposed corridors may stop or become unviable.
Illicit activity including cyber attacks	Increasing dependence on digital platforms, data infrastructure, payment systems, models, cables (energy and telecom), and control systems. This increases the risk of infrastructure and cyber attacks, terrorism, rogue actors, drone and hybrid warfare, fraud, shadow fleets, and capacity failure in providers.
Lack of global cooperation	Countries not willing to cooperate as they once did — for example, on strategic fuel reserves. This development includes less reliance on global organizations such as the UN, WTO, and USMCA. The number of trade agreements under review is increasing even as trading partners need more bilateral agreements.
Legal, regulatory and contractual risks	Protectionism, tariffs and misaligned regulations that fragment supply chains. Markets are being impacted by anti-bribery, financial crime, and broader human rights laws across the supply chain. More complex contractual and legal arrangements are increasing frictions.
Financial risks including supplier resilience	Supplier insolvencies and inadequate financial monitoring by organizations that could result in supply shocks. Some sectors are already squeezed by cost pressures and transition demands. Long-term projects require difficult assumptions that are hard to forecast. Security of supply is now more important than cost.
Macroeconomic risks	A volatile, uncertain economic environment marked by slower growth, inflation, interest rates, and increasing costs. Globally, more than 3,000 tariffs are affecting trade levels and supply chains. Cost increases and uncertainties involve energy, commodities, freight rates, manufacturing costs, hoarding, stockpiling, and working capital.
Organizational adaptability for optionality	Years of optimization for lowest cost, lean inventories and just-in-time delivery that have reduced buffers, optionality, and resilience. Many businesses are unable to adopt new strategies, business models, organizational processes, and capabilities. Decision paralysis and/or wrong responses can occur.
Risk management and control capability	Risks that organizations do not have the risk management capabilities and controls to identify, model, stress test, and respond to changing risks and increased complexity. Organizations need accountability for supply chains in terms of procurement, risk, and other functions.
Scarcity and competition for resources and infrastructure	Scarcity and competition for resources and infrastructure could constrain production and force difficult allocation of choices. Affected resources might include data centers, renewables, EVs, and food production. Scarce raw materials, fertilizers, rare earths, water, land, electricity, infrastructure could leave demand unmet and/or divert resources.
Visibility of supply chain and availability of data	Opaque supply chains that prevent visibility of the layers and parties at multiple levels. Available and reliable data does not exist or is difficult to obtain. Risks also involve not understanding supply chains and connected ecosystems. Organizations can find it difficult to map out suppliers, sources, and needs over various timeframes.
Workforce risks	Limits in the size, skills, adaptability, and growth potential of the workforce. Issues include workforce shortages and weak specialist talent pipelines, long training lead times, rising levels of retirement, and unclear career paths. Organizations might not be hiring enough entry level workers or, as in Germany, required to upskill and retrain factory workers to produce defense equipment. New technology and a digital workforce require flexibility and continued training.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com



At KPMG, every idea starts with human ingenuity. KPMG professionals combine their insight and creativity with AI tools, applying them thoughtfully and responsibly under the KPMG Trusted AI framework to develop imagery and content.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more details about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the KPMG global organization, to KPMG International Limited ("KPMG International"), and/or to one or more of the member firms of KPMG International, each of which is a separate legal entity.

Designed by Evalueserve.
Publication name: Building a shock-resilient supply chain | Publication number: 140651-G | Publication date: November 2026