MGC
GLOBAL RISK ADVISORY LLP

GEOPOLITICAL RISK ADVISORY · ENTERPRISE RESILIENCE

When the Likely Scenario Becomes the Operating Reality

What happens when uncertainty stops being a scenario to monitor ; and becomes the environment in which the business has to operate?

From our earlier scenario analysis to today's operating environment

Allinial Independent Member of GLOBAL®

113
COUNTRIES

48,000+
PROFESSIONALS

~US$7.6B
COMBINED REVENUE

Executive summary

The question has changed.

When we published our earlier assessment of April 02, 2026, the question was relatively straightforward: which geopolitical scenario would materialize?

We considered three possibilities (01) rapid de-escalation; (02) regional escalation; and (03) prolonged uncertainty. The evidence today suggests that the third scenario has not simply materialized; it has persisted. And that changes the nature of the risk.

The issue is no longer whether businesses can withstand one disruption. The issue is whether they can continue to operate effectively when disruption becomes recurring, interconnected and difficult to time.
In other words, uncertainty itself is becoming an operating condition.

01

Evidence, not forecast

The evidence is increasingly visible in the operating environment: elevated energy prices, *(Brent crude oil price has increased by 38% YoY)*, disrupted trade routes, changing sanctions exposure and higher logistics costs. None of these, individually, constitutes a systemic crisis. The concern is the accumulation; and the fact that businesses are having to plan around it for longer.

02

Risk no longer isolates

Energy, trade, finance, compliance, technology and people can no longer be viewed as separate risk categories. A disruption that begins in one area can quickly create consequences in several others.

03

Maturity beats prediction

The organizations best positioned for this environment will not necessarily be those that predict geopolitical developments most accurately. They will be those that can **sense earlier, quantify faster, decide sooner and adapt better.**

WHAT THIS MEANS FOR BOARDS AND CXOs

Geopolitical risk cannot remain a periodic item in a risk register. It needs to become an operating mechanism, linked to financial exposure, decision triggers, accountable owners and board visibility. Geopolitical resilience therefore needs to move from the risk register into the operating model - with financial thresholds, decision triggers, accountable owners and board visibility.

The objective is not to predict every disruption. It is to be ready for the consequences of the disruption you cannot predict.

But the likely case did not pass. It persisted.

Our earlier thought leadership, West Asia Conflict: Implications for Businesses, framed the future through three scenarios.

The best case assumed rapid de-escalation. The worst case assumed regional escalation. The likely case assumed something more uncomfortable: **prolonged uncertainty**.

We are increasingly operating in that third scenario.

Importantly, this does not mean that the worst case has arrived. It means something more subtle and potentially more consequential for business planning: the likely case has lasted long enough to change how businesses need to operate.

BEST CASE

Rapid de-escalation

Trade flows restore and the environment returns to normal within a defined window.

WORST CASE

Regional escalation

Energy and trade routes suffer prolonged disruption, triggering a broader global economic shock.

LIKELY CASE - CONFIRMED

Prolonged uncertainty

Intermittent escalation, disrupted trade, elevated energy and logistics costs and shifting sanctions exposure, without a single systemic tipping point.

A temporary shock can be absorbed through contingency planning. A persistent shock is different. It requires organizations to make decisions while the disruption is still unfolding; and to do so repeatedly.

$92.15

Brent crude per barrel, as of August 20, 2026

SOURCE: BLOOMBERG, 2026

6

Commodity vessels transited the Strait of Hormuz on August 18 - materially below historical traffic

SOURCE: REUTERS, 2026

0

Trade and financial transactions the UAE now permits with Iran, following renewed attacks

SOURCE: DECCAN HERALD, 2026

This is no longer simply a geopolitical story. It is an enterprise operating-environment story.

But a geopolitical event is only the beginning. The risk model is moving from event → cascade.

The traditional mental model is simple: an external event causes a temporary disruption, the business activates its contingency plan and operations eventually return to normal.

That model becomes less useful when disruptions recur.

A geopolitical shock can affect markets first, then operations, then cash, contracts and compliance and eventually force management to make strategic decisions that were never contemplated when the original event occurred.

THE OLD MODEL

Geopolitical event → **Temporary disruption** → **Recovery**

THE EMERGING MODEL

Geopolitical shock

↓

Market disruption

↓

Operational exposure

↓

Financial exposure

↓

Control / compliance exposure

↓

Strategic decision

WHAT THIS MEANS FOR BOARDS AND CXOs

A business does not need one catastrophic event to sustain material damage. Repeated, interconnected disruptions can create a cumulative exposure that is harder to see and harder to reverse. The important point is not that every disruption will travel through every stage. It is that the enterprise is connected enough for one disruption to create consequences far beyond its original point of entry.

Disruption no longer arrives as a single event. It propagates.

The exposure does not stay in one risk box.

This is where the traditional risk framework begins to break down.

Geopolitical risk does not arrive neatly labelled as “energy risk”, “supply-chain risk” or “sanctions risk”. It moves across the enterprise.

Energy affects costs. Trade affects supply. Finance affects liquidity. Sanctions affect counterparties. Technology affects the ability to operate. People determine whether critical activities can continue.

The real exposure appears where these risks intersect.

01	**Energy**	Oil, gas, electricity, fuel and input-cost volatility.
02	**Trade & supply chain**	Shipping, ports, lead times, inventory, supplier concentration.
03	**Finance**	Working capital, FX, interest rates, insurance, liquidity.
04	**Compliance & technology**	Sanctions, counterparties, cyber threats, tech dependencies.
05	**People & operations**	Travel, workforce availability, facilities, continuity.

Example: How one disruption becomes five

Shipping disruption	→	Longer lead times
Higher inventory	→	More working capital
Higher financing cost	→	Margin compression
Sanctions change	→	Supplier unavailable
Costlier alternative	→	Contract mispriced

Customer dispute & revenue risk

The same external event can therefore become a supply-chain problem, a liquidity problem, a contractual problem and ultimately a strategic problem.

The risk lives in the connections, not the categories.

Having more suppliers does not necessarily mean having more resilience.

Supplier diversification sounds reassuring. But the number of suppliers can create a false sense of security.

Two suppliers may be geographically different but depend on the same shipping lane. They may be contractually independent but use the same raw material, logistics provider or infrastructure. The business may therefore appear diversified while remaining exposed to a single underlying system.

The relevant question is not simply whether an alternative supplier exists. It is whether the alternative can actually operate when the original system fails and how quickly it can be activated.

Does the second supplier depend on the same geography?

Does it use the same shipping route?

Does it depend on the same raw material?

Does it rely on the same logistics provider?

Can it actually deliver during a regional disruption?

How quickly can we switch and at what cost?

The test should therefore move beyond "Do we have an alternative?" it should become: "Can the alternative actually work when we need it and how quickly can we activate it?"

WHAT MANAGEMENT SHOULD TEST

Dependency → Alternative → Time to switch → Cost to switch Capacity

Quality → Upstream dependency

Move from "alternative supplier" to "alternative system."

KEY TAKEAWAY

Five suppliers can still represent one source of risk if they depend on the same underlying system.

Energy volatility is a margin variable - not just an input cost.

Energy volatility is often monitored as a market indicator. For management, that is only the starting point.

In an Indian business, higher energy costs can travel through raw materials, manufacturing, transportation, warehousing, aviation, packaging and employee mobility before they ultimately appear in prices and margins. The relevant question is therefore not simply “What will oil cost?”

It is: “At what point does our business economics begin to break?”

- **Raw materials**
- **Manufacturing**
- **Transport**
- **Warehousing**
- **Aviation**
- **Packaging**
- **Employee mobility**
- **Consumer prices**

THE CFO QUESTIONS

- At what oil price does our margin model break?
- At what freight cost does a key customer contract turn loss-making?
- How many additional days of working capital does a 30-day supply delay require?

These are not questions for a commodity desk. They are questions about pricing power, contracts, margins and cash.

WHAT THIS MEANS FOR BOARDS AND CXOs

Energy exposure should be translated into margin thresholds, pricing decisions, contract exposure and working-capital requirements - not monitored only as a market indicator. Oil-price volatility is the entry point. The real exposure is what happens after it enters the cost base.

Oil-price volatility is the entry point, not the endpoint. It travels through the full cost base before it reaches the customer.

The balance sheet can deteriorate before the income statement tells the story.

Geopolitical disruption often creates a financial lag.

Lead times lengthen. Inventory rises. Production cycles extend. Billing is delayed. Customers may take longer to pay. Management may agree to revised commercial terms simply to preserve the relationship.

None of these necessarily creates an immediate P&L shock. But cash can quietly become trapped in the business.

This makes geopolitical resilience a CFO issue, not simply a risk-management issue.

Disruption → Longer lead times

↓

Higher safety stock

↓

Cash trapped in inventory

↓

Delayed production & billing

↓

Receivables rise → Liquidity pressure

WHAT THIS MEANS FOR BOARDS AND CXOs

Stress-test the incremental cash requirement associated with 30-, 60- and 90-day disruption scenarios and identify which suppliers, customers and contracts create the greatest liquidity exposure.

Recent Indian credit analysis confirms the pattern: Longer supply-chain cycles and elevated procurement costs are increasing working-capital requirements across vulnerable sectors (Crisil, 2026).

By the time margin damage becomes visible, liquidity pressure may already be here.

A contract can remain legally valid and still become a bad business decision.

Contracts are designed around assumptions: prices, freight, insurance, currency, sourcing, delivery routes and regulatory conditions.

Geopolitical disruption can change those assumptions without changing the legal validity of the underlying contract.

The result is a dangerous gap between what the contract requires and what it still makes economic sense to perform.

- Force majeure
- Price escalation
- Change in law
- Sanctions
- Delivery obligations
- Incoterms
- Insurance
- Currency
- Termination
- Alternative sourcing

THE CRITICAL QUESTION

If the cost of performing a contract rises by 20%, 30% or 50%, the critical question is not merely whether the contract remains enforceable.

It is: Who absorbs the economic consequence nand did we price that risk when we signed the contract?

The dispute often does not create the risk. It merely makes the unpriced risk visible.

Knowing your counterparty is no longer enough.

A transaction rarely involves only two parties.

Ownership, beneficial ownership, intermediaries, distributors, logistics providers, banks, payment routes and ultimate destinations can all influence whether a transaction remains commercially and legally viable.

A relationship that was acceptable at onboarding can therefore become problematic as geopolitical conditions change.

The UAE's suspension of trade and financial dealings with Iran shows how fast a viable relationship can become a compliance liability *(Deccan Herald, 2026)*.

Customer

Beneficial owner

Intermediary

Distributor

Logistics provider

Bank

Payment route

Ultimate destination

THE QUESTION HAS CHANGED

Yesterday's question was "Can we transact?".

Today's question is: "Can we still transact safely, legally and economically?"

Answering that question requires visibility that is dynamic, not a compliance assessment performed once a year.

A commercially viable relationship yesterday can become a compliance liability tomorrow.

The dependency may not be physical. It may be digital.

Geopolitical disruption does not need to reach a company's factory, office or warehouse to interrupt operations.

It can arrive through a cloud provider, SaaS platform, bank, telecom network, logistics platform, managed service provider or another critical third party.

The result is a new dimension of geopolitical exposure: digital dependency.

- **Cloud providers**
- **SaaS platforms**
- **Banks & payment systems**
- **Telecom networks**
- **Logistics platforms**
- **Third-party vendors**
- **Managed service providers**
- **Industrial control systems**
- **Customer portals**

THE BOARD QUESTION HAS CHANGED

Not "Are we secure?" but "Can we keep operating if a critical digital dependency goes dark?" That moves cyber into the business-continuity conversation. That question moves cybersecurity out of a purely technology conversation and into the broader conversation about business continuity and enterprise resilience.

WHAT THIS MEANS FOR BOARDS AND CXOs

Critical digital dependencies should be identified, ranked by business impact and tested for continuity, failover and recovery.

Digital dependency is now geopolitical dependency.

The most critical dependency may be a person.

Resilience programs are generally good at mapping suppliers, systems, facilities and financial exposures. They are often less disciplined about mapping human dependency.

Yet a disruption can affect where critical employees can travel, whether they can access facilities and whether their responsibilities can be transferred or performed remotely.

A business can therefore have resilient systems and still have a single-person point of failure.

The Government of India has already institutionalized cross-ministry monitoring of geopolitical developments and their implications for maritime trade and supply chains *(Press Information Bureau, 2026)* indicating this is no longer treated as a foreign-policy issue alone.

Who are the 20 people without whom the business cannot operate?

Where are they and can they travel?

Can someone else perform their role?

Can the role be performed remotely if not?

The practical test is simple.

Who are the people whose absence would stop a critical activity?

Where are they? Can they travel? Who can replace them? Can their role be performed remotely?

WHAT THIS MEANS FOR BOARDS AND CXOs

Identify critical-person dependency in the same way the organization identifies critical suppliers and systems and define a viable alternative before disruption occurs.

Identify the people whose absence creates operational failure, before disruption identifies them for you.

India: Exposed to the shock. Positioned to capture the shift.

India sits on both sides of the geopolitical equation. It remains exposed to imported energy, shipping disruption, freight costs, currency volatility, Gulf trade and aviation disruption. But the same global reconfiguration is encouraging companies to diversify supply chains, manufacturing footprints and service delivery.

That creates a different strategic question for Indian businesses. "Where are we vulnerable; and where can we become more competitive because the world is being forced to reconfigure?"

India's exposure is direct: the impact of energy volatility does not remain confined to fuel costs; it extends into currency pressures, trade and logistics, aviation costs and inflation, widening its relevance across the corporate cost base *(Business Standard, 2026)*.

DEFENCE

Protect the business from disruption.

OFFENCE

Position the business to capture the opportunity created by disruption.

Resilience should not mean avoiding risk. It should mean becoming better positioned to operate through it.

The same shock does not hit every business in the same place.

The transmission mechanism may be common. The financial consequence is not.

A shipping disruption can be an immediate margin problem for one company, an inventory problem for another, a liquidity problem for a bank and a technology or third-party dependency problem for a digital business.

The relevant question is therefore not simply "Is our sector exposed?". It is "Where does the exposure enter our business and where does it ultimately appear in financial performance?"

HIGH DIRECT EXPOSURE

Oil & gas · Chemicals · Fertilizers · Aviation · Shipping · Logistics

Energy → Supply → Freight → Insurance → Margin

HIGH INDIRECT EXPOSURE

Manufacturing · Automotive · Consumer goods · Retail · Construction

Inputs → Inventory → Logistics → Margins

FINANCIAL EXPOSURE

Banks · NBFCs · Insurers · Asset managers

Credit → Liquidity → Market volatility → Counterparty

DIGITAL EXPOSURE

Technology · IT Services · SaaS · Fintech

Cyber → Sanctions → Third-party dependency → Cross-border data

PEOPLE / SERVICE EXPOSURE

Professional Services · Healthcare · Education · Travel

Mobility → Workforce → Client demand → Continuity

Geopolitical exposure is not a sector label. It is a dependency map.

From risk awareness tom geopolitical resilience.

Most organizations today are not starting from zero. They have risk registers, monitoring mechanisms, contingency plans and crisis-management procedures.

The question is whether those mechanisms actually change decisions.

There is a significant difference between knowing that a risk exists and knowing what the organization will do when a predefined trigger is reached.

01 Reactive

Responds after disruption. Crisis management.

02 Aware

Maintains a risk register. Periodic monitoring. Risk identification.

03 Prepared

Has scenarios and contingencies. Stress testing.

04 Resilient

Links scenarios to financial and operational decisions. Integrated resilience.

05 Adaptive

Uses disruption to create strategic advantage. Strategic resilience.

At Level 3, the organization can respond.
At Levels 4 and 5, it can make better decisions before and during disruption.
The objective is not perfect prediction. It is decision readiness.

Boards should not need another geopolitical forecast.

A board does not need to predict what happens next in the Middle East, what oil will trade at next month or which disruption will occur next. It needs to know something more useful - If a critical dependency fails tomorrow, what happens to our business; and what will we do about it? That requires evidence, numbers, ownership and predefined decisions.

The following ten questions translate geopolitical risk from a broad external concern into specific questions of exposure, financial impact, continuity and decision-making.

01
What are our five most significant geopolitical dependencies?

02
Which supplier, route, customer, bank or provider is a single point of failure?

03
How many days can we operate if that dependency disappears?

04
What happens to EBITDA if energy and logistics stay elevated for six months?

05
How much additional working capital would we require?

06
Which contracts don't protect us against cost escalation or disruption?

07
Can we trace sanctions and beneficial-ownership exposure across our transaction chain?

08
What happens if a critical technology provider becomes unavailable?

09
Can our critical people keep operating if travel or access is disrupted?

10
What decision should we make before the next disruption, not during it?

These questions deliberately move the discussion from geopolitics to enterprise consequences, from “What is happening?” to “What does it mean for us?”.

If the board cannot answer these questions with evidence, ownership and numbers, geopolitical resilience has not yet become an operating capability.

MGC GLOBAL RISK ADVISORY LLP

Knowing the questions are not enough. The organization must act on them.

Three phases can turn awareness into an operating capability.

The answer is not another 40-page geopolitical report. The answer is a practical mechanism that identifies dependencies, quantifies consequences, defines triggers and assigns accountability. That is why we propose a simple 90-day progression: Identify → Stress-test → Act.

The 90-day agenda provides a disciplined sequence from diagnosis to stress-testing to action.

DAYS 0-30

First, understand where the enterprise is actually dependent.

Identify

– Critical suppliers & customers
– Energy & financial dependencies
– Sanctions exposure
– Critical routes
– Technology dependencies
– Critical people

Output: Enterprise geopolitical dependency map

DAYS 31-60

Then quantify what happens if those dependencies fail for 30 days, 90 days or longer.

Stress-Test

– Scenario A: 30-day disruption
– Scenario B: 90-day disruption
– Scenario C: Prolonged instability

Measures: Revenue · EBITDA · Cash flow · Inventory · Working capital · Customer SLA · Liquidity · Cyber resilience

DAYS 61-90

Finally, convert the findings into owners, actions, deadlines and triggers.

Act

- Red: Immediate single points of failure
- Amber: Manageable, needs mitigation
- Green: Diversified / resilient

Owner → Action → Deadline → Trigger → Board reporting

The objective is not a better risk report. It is a faster management response.

Geopolitical risk needs a dashboard that changes decisions - not a report that merely records them.

Management does not need more information. It needs the right information early enough to act.
A useful dashboard therefore has to shorten the distance between **external change and internal decision**.

MONITOR

Oil	**FX**	**Freight**
Insurance	**Shipping**	**Sanctions**
Supplier lead time	**Inventory**	**Cyber incidents**

INTERPRET

What changed?

ASSESS

What does it mean for us?

DECIDE

What action is required?

ESCALATE

What requires the Board's attention?

Every indicator should answer a management question: **What changed? What does it mean for us? What should we do? Who needs to know?**

The value of a dashboard is not what it tells you. It is what it makes you do.

From risk register to resilience register

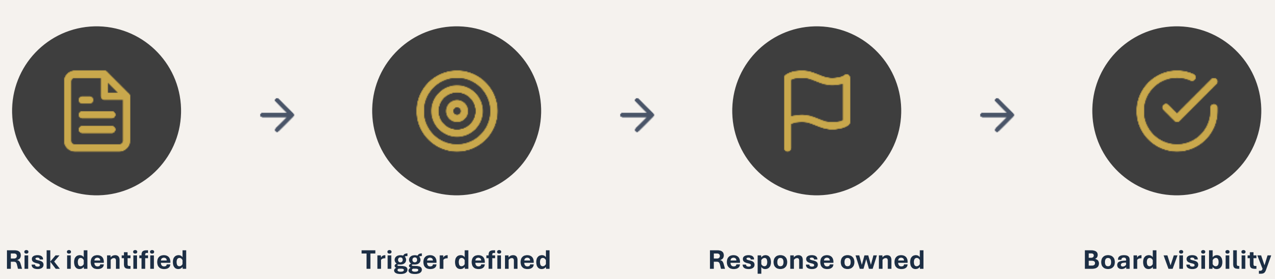
Traditional risk management is often strongest at identification.

The harder question is what happens next.

A resilience register closes that gap by connecting the risk to a dependency, a measurable trigger, an impact, a response and an accountable owner.

Risk	Dependency	Trigger	Impact	Response	Owner	Design
Hormuz disruption	Gulf Supply	Shipping below threshold	High	Alternate sourcing	COO	Activate alternate route
Oil Spike	Energy	Brent > defined threshold	High	Pricing / hedge	CFO	Review pricing
Sanctions	Counterparty	New designation	High	Suspend / replace	Compliance	Escalate immediately
Cyberattack	Critical vendor	Service unavailable	High	Failover	CIO	Activate continuity
Travel disruption	Key personnel	Airspace closure	Medium / High	Remote continuity	HR / COO	Activate contingency

This changes the conversation from: **“Are we monitoring this risk?”** to **“What trigger will make us act and who has the authority to act?”**



Resilience begins when risk has an owner, a trigger and a response.

Prediction is no longer the finish line.

The journey is from prediction → adaptation → advantage.

The first phase of this crisis was about prediction: **Which scenario will materialize?**

We now know enough to ask a different question.

How effectively can an organization operate when uncertainty persists?

And beyond that:

Can the organization adapt faster than its competitors?

Prediction → **Adaptation** → **Advantage**

Prediction informs. Adaptation protects. Advantage compounds.

Resilience cannot remain a contingency plan. It has to become part of strategy.

So, what should management do now?

Five imperatives for operating through persistent uncertainty.

01

Know your dependencies

Know which suppliers, routes, technologies, counterparties and people could materially disrupt the business.

02

Quantify the financial impact

Translate geopolitical exposure into revenue, EBITDA, cash flow, working capital and liquidity.

03

Build alternatives before you need them

The worst time to design an alternative is after the original system has already failed.

04

Create early-warning triggers

Decide in advance which indicators should trigger management action.

05

Turn resilience into competitive advantage

The objective is not simply to survive disruption. It is to adapt faster and emerge stronger than competitors.

The organizations that win in prolonged uncertainty will not necessarily be those with the best forecasts. They will be those with the clearest dependencies, fastest decisions and greatest ability to adapt.

MGC
GLOBAL RISK ADVISORY LLP

From risk identification to competitive advantage.

The world does not need to become predictable for businesses to become resilient. What matters is whether an organization can understand its dependencies, quantify the consequences of disruption, act on early signals and adapt before the impact compounds.

- From risk identification to resilience.
- From resilience to readiness.
- From readiness to competitive advantage.

MGC Global Risk Advisory helps organizations translate uncertainty into decisions - connecting geopolitical, financial, operational, technology and compliance risk to enterprise resilience.

Start a conversation →

Specialists in Risk. Partners in Trust.

Bengaluru · Mumbai · New Delhi
www.mgcglobal.co.in

Allinial Independent Member of GLOBAL®