



Signals of change and the risk agenda

July 2022: Geopolitics and readiness for disruptive risks



Chief Audit Executives (CAEs) continuously assess how to deliver on their objectives to maintain trust of stakeholders. This includes considering signals of change in risks faced by their organization and, in turn, changing the focus of the Internal Audit (IA) plan needed. Our complementary series, “On the CAE agenda,” provides a full view of top risks highlighted this period.

Signals of change

Geopolitical risks have moved up the agenda as the world is going through a period of extreme political volatility. In a highly globalized business environment, these risks affect all companies regardless of where they operate because of the impact on the global economy, supply chains, cybersecurity, and business continuity, among others.

Only few could have predicted the recent turn of events. The World Economic Forum’s 2022 Global Risk Report¹ published in January 2022 did not even include political disruption or armed conflict in its top 10 risks. The assumption that there was no immediate threat or that exposure to geopolitical risk to an organization is far away simply as a function of where it is located, has proven false.

The importance of having a cohesive response strategy that integrates with resilience capabilities is now even more relevant. IA can help incorporate macroeconomic and geopolitical risks at an engagement level, outside of an annual audit, and support the improvement to both management systems and control processes.

Risk considerations

- Current geopolitical risks are not disappearing anytime soon and new ones will continue to appear. Organizations should be prepared for all scenarios, and IA is best equipped to provide assurance in crisis management and business continuity.
- Uncertainty in geopolitics can complicate ESG discussions. With an ongoing humanitarian crisis and shortage of labor and resources, organizations will reevaluate their prioritization of ESG targets and refocus attention to other immediate operational needs.
- There are challenges to understanding what and how to audit for a disruptive risk like geopolitics. Organizations struggle with understanding and defining these risks and falter without adequate controls and stress testing needed for decision-making.
- Monitoring and assessing the far-reaching implications of the broad suite of economic sanctions impacting supply chains is paramount for future planning activities.
- With geopolitical volatility comes a variety of financial risk implications for organizations, to assess whether certain financial positions are at higher risk.
- Customers are more closely monitoring the actions of organizations. Alongside complying with sanctions, corporations are expected to respond to calls to provide humanitarian support and disengage themselves from entities who are contributing to the crisis.

¹ War in Europe: Why Geopolitical Risks Should Always Be on Internal Audit’s Radar, Richard Chambers, Feb 27, 2022.

Questions to ask/actions to take

- Is there sufficient advisory support in the time of crisis? Chief audit executives and senior management need to be fully cognizant of pertinent risks to the organization. IA can also apply its transformative role as adviser to assess and inform on the scale of impact of geopolitical risks.
- Has the organization identified geopolitical disruption in its risk framework? Are macroeconomic and geopolitical risks being factored into the organization's business strategy and decision-making? Ignoring the far-reaching implications of political tensions in a connected global economy and enduring on without contingency plans can place the company in a difficult position.
- Is there a leader assigned to tackle such risk planning? Are there enough resources and analytical capabilities available to action on resilience, contingency, and/or exit planning? Do team members have expertise/knowledge in handling geopolitical crisis?
- Are board members of the organization well-briefed of the relevant geopolitical risks and prepared with adequate response strategies?
- Do all lines have established channels of communication for effective coordination? Engagement of second and third line are crucial to the stability of the business, with finance, legal, IT, compliance, and internal audit working together for crisis management.
- How is the organization's supply chain reviewed? Are there controls in place to test disruption to operations? While a company's direct exposure to geopolitical risk may be low, indirect exposure via the supply chains may be higher than anticipated.

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

kpmg.com/socialmedia



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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP342919-3B

Learn more by visiting:

- [Russia-Ukraine war: Scenario planning for an uncertain future](#)
- [Scenario planning and wargaming](#)
- [On the CAE Agenda](#)

Visit our Risk Assurance insights page by scanning our QR code:



Contact us

Michael Smith
Partner, Internal Audit &
Enterprise Risk, Internal
Audit Solution Leader
E: michaelasmith@kpmg.com

Richard Knight
Principal, Technology
Risk Management, IT Internal
Audit Solution Leader
E: raknight@kpmg.com