

**General**

05 February 2025

## Legal and Compliance Unleashed: What should be on your agenda for 2025?

## **Disclaimer – Please Read**

---

The information contained in this document does not constitute any guarantee or warranty by Control Risks Group Holdings Limited, its subsidiaries, its branches and/or its affiliates ("Control Risks") as to the future commercial success of the client/reader or as to the (non-)realisation of any risk. It cannot be ruled out that the information contained herein has not covered all conceivable aspects and possible assessments with regard to its subject.

Nothing in this document - whether text or illustration - constitutes advice of a legal, economic or factual nature. All information is for illustrative purposes only. Control Risks shall not be liable for any damages caused to third parties nor for any damages suffered by yourself should the contents of this document be referred to or relied upon. Breach of sanctions may result in your criminal prosecution and loss of business - always seek professional guidance.

Control Risks assumes no obligation to report on any changes in circumstances or new events after the date of presentation or to adjust any estimates made. All work results and findings do not in any way and under no circumstances constitute a recommendation or advise regarding a business decision by the client/readership. This is always the responsibility of the customer/reader. This document may not be communicated to any third party without the express written permission of Control Risks.

Copyright © Control Risks. All rights reserved. This document may not be reproduced without the (prior) express written permission of Control Risks. Reproduction without the permission of Control Risks will be considered an infringement of Control Risks' copyright.

---

## Geopolitics and compliance

---

- ▶ Global trade will continue to grow, but trade controls and regulatory risks will also increase in the coming years. Changing underlying geopolitical dynamics will likely impact regulatory trends, such as sustainability and supply chains, having sweeping impacts on businesses across various sectors..
- ▶ The Trump administration will accelerate the trend of protectionism globally. Powerful states may increasingly withhold access to resources, partnership, territory or goods unless specific interests or requests are addressed.
- ▶ In recent years, supply chain elongation and the rising number of geopolitical shocks has increased both the regulatory and compliance burdens, but also the risk of operational and geopolitical disruption.
- ▶ Tariff threats by the US will continue to be a bargaining chip in negotiations with rivals and allies alike, including the EU, China, Mexico and Canada. Trump's snap tariffs, and quick reversal, highlights the unpredictability of US trade policy. While it underscores that the Trump administration is one of dealmaking, it also illustrated the targeted countries willingness to apply reciprocal measures.
- ▶ Critically, China will likely wield its own expanding trade restrictions as well as increasingly prioritise localisation. Ongoing localisation in many of these industries will also weaken the impact of foreign trade and technology restrictions over time, but progress will not be uniform across these sectors, given China's own global supply chain dependencies.
- ▶ International institutions and international alliances will be increasingly undermined as Trump pivots to isolationism and transactional relations. This further weakens forums of negotiations amid heightened tensions.
- ▶ Middle power countries will benefit from supply chain diversification, however. Geopolitical competition is increasing the importance and influence of a new set of countries in strategic locations, critical supply chains or new industries.

### What does that mean for companies?

- ▶ Regulation may become more politicised in a polarised and hostile geopolitical environment, with companies subject to evolving pressures from host and home governments.
  - ▶ Geopolitical competition and protectionism will establish an increasingly complex regulatory environment for business, especially those operating across a wide range of jurisdictions.
  - ▶ Middle power countries, including those with strategic sectors and/or critical transit hubs, will be increasingly viewed as key opportunities for companies in the coming years.
-

## Technology and cyber

---

- ▶ 2025 will be characterized by a marked increase in the volume and sophistication of cyberattacks, fuelled by the rapid advancement of AI-powered tools.
  - ◆ AI tools are enabling threat actors to improve their attack volumes, success rates and to evolve attacks that are usually well mitigated by advanced companies, such as the use of deepfakes of executives to enable fraud.
  - ◆ AI tools themselves are increasingly being targeted, presenting confidentiality, availability risks, as well as newer integrity risks for providers and users of those tools requiring implementation and compliance with AI risk management frameworks (e.g. ISO 42001 and NIST).
- ▶ Concentration risks are underscored by the persistent vulnerabilities within legacy and shared infrastructure systems.
  - ◆ Supply chain and third-party vulnerabilities are a growing concern, with such compromises accounting for 25% of identified attacks in 2024 compared to 11% in 2021.
  - ◆ Proactive third party risk management, resilience and crisis preparedness will be increasingly important in 2025, including a more in-depth assurance that third parties are complying with required frameworks and onboarding submissions, while also ensuring that third party incidents are considered as part of resilience, response playbooks and crisis exercising.
- ▶ 2025's geopolitical climate, marked by shifts in global leadership and a rise in isolationist policies, will contribute to an increase in hostile state-sponsored cyber activity.
  - ◆ Much of this activity will be centred on Europe as the security situation comes under strain from emboldened nation state threat actors looking to retaliate to sanctions and other economic measures, while NIS Directive 2.0, DORA, CER and other regulations are likely to increasingly draw regulatory attention to strong proactive compliance measures leading to significant corrective and punitive actions.

## Third-party risk management

---

Heightened geopolitical tensions and frequent regulatory shifts mean ongoing unpredictability for global supply chains. The ability to absorb and adapt to shocks is increasingly vital. Rapidly changing conditions – geopolitical flashpoints, trade wars, and regulatory revisions) demand flexibility and agility from legal and compliance teams across policy development, processes, and personnel.

### What that means for companies?

- ▶ **Stay Informed & Agile** - Track geopolitical developments, legislative changes and potential regulatory streamlining initiatives (eg. EU's Competitiveness Compass). Maintain flexibility in compliance programs to adapt swiftly.
  - ▶ **Map Your Supply Chain** - Conduct thorough, ongoing assessments to understand who your critical suppliers and partners are. Identify potential bottlenecks or single points of failure.
  - ▶ **Strengthen Due Diligence & Monitoring** – Procure holistic TPRM solutions that integrate traditional integrity risks (ABAC, AML, sanctions) with ESG obligations (sustainability, human rights, climate metrics).
  - ▶ **Scenario Planning & Contingency** - Develop backup supplier networks and alternative logistics routes to quickly shift if disruptions arise. Conduct periodic tabletop exercises to test resilience in crisis scenarios.
  - ▶ **Invest in Cross-Functional Expertise** - Build internal teams with specialised knowledge of key jurisdictions, ESG standards, and operational risk. Encourage collaboration among legal, procurement, compliance, and sustainability functions.
  - ▶ **Engage with Stakeholders** - Proactively communicate with suppliers about new regulations and expectations. Join industry groups or alliances that share best practices and offer early warning on upcoming compliance shifts.
-

## Failure to Prevent Fraud

---

- ▶ The Economic Crime and Corporate Transparency Act (ECCTA), came into force in December 2023, focused on widening the remit and effect of corporate criminal liability on large corporates with UK operations. ECCTA introduced a Failure to Prevent Fraud offence unless reasonable fraud prevention procedures are in place.
  - ▶ The UK government released guidance in November 2024 which sets out the six principles under which large organisations should consider when implementing reasonable fraud prevention policies and procedures. The guidance is relatively detailed and includes numerous references to the use of data analytics and the consideration of artificial intelligence in an organisation's fraud prevention framework.
  - ▶ Large organisations affected by ECCTA need to ensure that fraud policies, processes and compliance frameworks are reviewed and risk assessed by 1 September 2025. This includes revisiting existing controls, together with training and communication for staff. Businesses will need to consider the likelihood and impact of risks with respect to fraud offences such as mis-selling, misleading statements and false accounting.
-

## Get in touch

---



**Business intelligence and due diligence**

[Hannah.Lilley@controlrisks.com](mailto:Hannah.Lilley@controlrisks.com)



**Geopolitical and security analysis**

[Serena.Pilkington@controlrisks.com](mailto:Serena.Pilkington@controlrisks.com)



**Geopolitical and security analysis**

[Alexandra.Kellert@controlrisks.com](mailto:Alexandra.Kellert@controlrisks.com)



**Digital risks**

[Joseph.Buckley@controlrisks.com](mailto:Joseph.Buckley@controlrisks.com)



**Third party risk management**

[Charles.Brown@controlrisks.com](mailto:Charles.Brown@controlrisks.com)



**Investigations and forensic accounting**

[Adam.Garside@controlrisks.com](mailto:Adam.Garside@controlrisks.com)

---