Legal and Compliance Unleashed: What should be on your agenda for 2024?

Geopolitics and compliance

- The global sanctions landscape in 2024 poses a dilemma. Western efforts to counter sanctions circumvention could stoke further opposition to sanctions among Middle Powers and the Global South.
- The G7 will focus its sanctions politics on enforcement, which bears opportunities for the EU in particular. The bloc can move away from internal disputes over sanction expansion and focus on developing the institutional capabilities of member states (more government powers, intelligence, jobs).
- The US will be keen to expand secondary sanctions, but the EU will fear diplomatic backlash.
- The international enforcement of G7 sanctions in relation to Russia and the US' increasing usage of secondary sanctions will add to geopolitical tensions in 2024.
- There is growing opposition between Middle Powers and Global South towards internationalisation of sanctions. Middle Powers such as Brazil and South Africa continue to oppose economic sanctions as coercive, and criticise Western financial dominance. This will add further promotion of de-dollarisation discussions within BRICS.
- Both Russia and China will use this opposition as a way to weaken the western-led international trade system.
- What that means for companies?
  - Companies will need to pay close attention not just to which entities are designated and penalised but to trade flows, diplomatic pressure, and other informal indicators of sanctions enforcement.
  - Stronger sanctions enforcement will increase demand for robust sanctions and trade compliance teams, including around end use certification.
  - Companies should assess if compliance with sanctions will pose political or reputational risks in local markets.

Technology and cyber

- The regulatory landscape is changing quickly and is increasingly fragmented.
- Attacks are diversifying – we still see a huge amount of cyber extortion and business email compromise but also the use of novel tactics in extortions and fraud such as deep fake videos, audio etc. demonstrate how threat actors are adjusting their approach.
- Integrity is becoming a bigger issue than normal as AI is starting to be leveraged within company data and as part of customer engagement.
  - Legal teams need to question the validity of data/and insights given AI biases. We need to question what our insights are based upon and what behaviour that could lead to.
- We used to talk re: data protection but now data sovereignty, data security and regulator-led engagement requires legal and compliance teams to have a more global outlook on understanding risks.
- NIS2 and DORA are examples of two new frameworks/regulations that are of increasing importance to our clients
- While these are legal/regulatory issues, their impact is far reaching and requires technical and non-technical teams to work even closer together to ensure that tech strategy reflects the legal/regulatory requirements – if they are an afterthought it can be very costly. E.g. data residency, process requirements, personal data storage, new procurement systems to manage vendor risk etc.
- From an implementation perspective, responding to issues in one jurisdiction can look very different to one jurisdiction to another; requiring more up-front preparation to ensure an effective and efficient incident management, if the worst should happen.

Third-party risk management

- Pressures on those working in third-party risk management are rising due to a convergence of challenges – increasing global regulations, data privacy laws, the rise of ESG and related challenges, reshaping of supply chains driven by post-Covid dynamics, commercial pressures, and rapidly changing geopolitical norms.
- The recent Economic Crime and Corporate Transparency Act also widens yet further the risks and challenges third party compliance managers need to manage across their third-party networks and supply chains, as arguably fraud is a more recurrent issue than bribery.
- The result of these rising challenges is that compliance teams are increasingly stretched in having all the inputs and expertise necessary to ensure consistency in decision making within their compliance programmes.
- Policies and procedures need to be updated to reflect new local markets, along with sensitivities to traditional markets such as China and India. Risk models need to be revised, with a focus on more nuanced data inputs such as regional and industry, rather than just national governance and social risk indicators. Training also needs to be continually reviewed to ensure it is fit for purpose,
- Technology is a critically important element to achieve this, with high quality automation and data inflows.

Third-party risk management (cont.)

- But increasingly clients are talking about a need to achieve a broader level of third party peace of mind – looking for a wider range of inputs than traditionally sought to help make sound decisions, such as geopolitical insights to help determine supply risks such as occurring in the Red Sea currently, or ESG insights to understand nuances of carbon and labour risk and how to measure, to consultative support in understanding shifting regulations and implications, to in-country local insights to ensure quality decision making on issues in jurisdictions they are unfamiliar with.

ESG

- High volume of supply chain sustainability due diligence regulation has emerged around the world over the last two years. This includes everything from the German Supply Chain Act, the Norwegian Transparency Act, the EU Deforestation Due Diligence and the recent Canadian Forced Labour Act, to name just a few.
- At the EU level, the Corporate Sustainability Due Diligence Directive (CSDDD) was informally agreed by the EU Council and Parliament late last year, and is expected to be signed off in 2024, at which point it will move to implementation by EU member states.
- As with other regulations, the EU CSDDD brings with it a far-reaching set of supply chain operational requirements which (in the case of the CSDDD, if approved) will be backed by financial penalties through a European Supervising Authority.
- Clear operational requirements underpinning all legislations include the need to identify, prevent, manage and mitigate sustainability risk and impact in the supply chain.
- Requirements apply not just to direct business relationships (Tier One suppliers), but also to indirect business relationships (Nth tier suppliers). This will require companies to have much more visibility of their upstream supply chains, from raw material origin through processing, distribution, sale, use and end of life. This will drive a step-change in supply chain transparency and accountability.
- Companies are advised to upgrade and enhance their existing supplier management systems and controls as well as their existing policies and risk management procedures

Corporate transparency

- The Economic Crime and Corporate Transparency Act (ECCTA), which came into force in December 2023, focuses on widening the remit and effect of corporate criminal liability on large corporates with UK operations. ECCTA provides:
  - Reform of Companies House so there is a more reliable companies register to prevent opaque holding structures being formed and to increase transparency.
  - Greater power for enforcement agencies – for example, the Serious Fraud Office has powers to ensure that individuals and companies hand over information pre-investigation, to fast track matters including those relating to fraud, domestic bribery, and corruption; together with an extension of powers for The National Crime Agency.
  - The introduction of a Failure to Prevent Fraud offence, especially in terms of who it applies to with “Senior Managers” falling under the remit of the legislation, unless reasonable fraud prevention procedures are in place.
- The means that companies need to ensure that fraud policies, processes and compliance frameworks are reviewed and risk assessed; existing controls are revisited; 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.
- The UK government should be releasing statutory guidance by March 2024. In summary, there is an increased risk for corporates being held liable for financial crime committed by their employees, subsidiaries and agents and which will lead to a greater compliance focus for affected organisations.

Business intelligence and due diligence

Hannah.Lilley@controlrisks.com

Sanctions and political risk consulting

Tobias.Wellner@controlrisks.com

Cyber security

Jayan.Perera@controlrisks.com

Third party risk management

Hugo.Williamson@controlrisks.com

Sustainable supply chains and ESG

Robert.Bailes@controlrisks.com

Investigations and forensic accounting

Ramon.Ghosh@controlrisks.com