Using Technology to Comply with the UK Economic Crime and Corporate Transparency Act 2023

Case IQ

Introduction

The Economic Crime and Corporate Transparency Act 2023 subjects companies to new areas of liability for failing to prevent fraud that can arise from corruption, sanctions evasion, and inaccurate financial or ESG reporting. Under the Act's failure to prevent fraud offense, large entities can be prosecuted for certain actions, unless they can tangibly demonstrate reasonable controls to prevent fraud.

Companies today, however, face incredible challenges in demonstrating such controls due to the lack of centralized compliance processes and the inability to easily access the data needed to assess fraud risk. The volume and global dispersion of employees and counterparties, the presence of data across numerous systems, and the shift to using mobile devices in the workplace make it crucial for a company to adopt a new approach to managing these risks. This white paper explores practical guidance for compliance organizations seeking to implement such controls using purpose-built compliance technology that meets the needs of their company's broader business and IT teams.

Compliance Approvals & Sanctions Risks

Compliance approval processes are a crucial step to mitigate the risk that a company does business with, or otherwise engages with, a sanctioned person or entity. Compliance approval processes related to providing or receiving gifts, hospitality or travel can vet whether the recipient or provider of such gifts raises any sanctions risks for the company. Approval processes for similar engagements like charitable contributions, donations, and sponsorships can determine whether providing such benefits to the recipient entity also poses any sanctions risks.

When it comes to engaging with third parties, such as vendors, suppliers, customers, sales agents, and distributors, end-to-end third-party risk management (TPRM) is a holistic process to identify and manage sanctions risks. End-to-end TPRM refers to identifying, assessing, mitigating, and monitoring many areas of potential third-party risks in a comprehensive approach across departments and functions, with compliance approvals playing a central role in the overall process.

Approvals & Disclosure and Third-Party Management tools manage compliance approval workflows across varied use cases from gifts and hospitality to sponsorships and donations, conflicts of interest, and third party due diligence. Through those workflows, company employees as well as third parties may provide information related to counterparties (i.e., gift and hospitality recipients, charities, trade associations, and vendors, suppliers, customers, sales agents, and distributors) who may be sanctioned or may be otherwise related to a sanctioned party.

These workflows can also embed real-time reputational risk data into compliance approval processes to help ensure that any counterparties, individuals affiliated with them, and beneficial owners thereof, are not on any government sanctions or other watchlists, not related to PEPs or state-owned entities, and do not have other adverse media that might increase their risk.

A robust workflow software should aggregate all the relevant data around any engagement, help assess the underlying risks, provide an automated risk score for sanctions risk, and escalate the workflow for heightened approval as required. The software should also make it easy to manage hundreds of these diligence processes without losing track of all the required steps, while also ensuring compliance inquiries are continuously documented and preserved to support audit and investigation functions.

Compliance Ongoing Monitoring & Sanctions Risk

Once compliance review and approval is received, ongoing monitoring is essential to ensure that the counterparty does not become subject to sanctions post-diligence. Workflow tools should allow you to monitor external reputational risk data and receive alerts if any new adverse information is available. New information might lead to termination of the third party or new mitigation measures.

In addition to ongoing reputational monitoring, the company should also monitor the actual financial transactions related to the counterparty. A Compliance Monitoring tool can proactively perform various analytics on vendor payments, customer revenue transactions, and travel and expense reimbursements to help detect sanctions risk. Relevant analytics that can be applied to financial data include

- **Sanctioned Name Matching** to look for matches between sanctions lists and the names and addresses, or combinations thereof, of vendors, customers, or individuals identified in T&E reports.
- **High-Risk Country Association** to look for sanctioned jurisdictions within vendor and customer financial transactions, including their address, delivery destinations and end-recipient countries for customers, sold-to-party information, and vendor or customer bank account countries.
- **Cross-border Transactions** to look for suspicious transactions where a company's shipments go to a country which does not correspond to the customer's location, particularly where that ship-to country is a common country used to evade sanctions. In such cases, products may end up in sanctioned jurisdictions via that country, potentially exposing the company to liability.

By utilizing compliance analytics, a company can mine large amounts of data quickly and efficiently and mitigate organizational sanctions risks.

Financial Reporting Risk

The Economic Crime and Corporate Transparency Act also requires corporations to carefully consider their responsibilities in presenting accurate financial statements.

Fraudulent manipulation of financial statement results could include inflating revenue or minimizing expenses. In a scheme to inflate revenue, a company may falsely record the amount of revenue in a quarter-end closing period. For example, a salesperson could feel pressure to meet sales targets in order to receive a bonus or achieve a promotion and may engage in a scheme known as "channel stuffing." This occurs when unnecessary and excessive sales are made to customers at a quarter or fiscal year-end which makes it appear that sales targets have been met or exceeded. However, because the customer did not need the products in that timeframe, the excessive products are returned to the company shortly thereafter. This creates a compounding effect for sales personnel, with additional manipulation continuing to be necessary to meet targets at future period ends.

A company can use analytics in a Compliance Monitoring tool to identify abnormal returns near financial closing periods. This analytic could be helpful in identifying potential financial manipulation and unethical business practices, particularly in the context of revenue recognition and returns management. By focusing on customer returns linked to abnormal revenue bookings near the close of financial periods, it helps in identifying patterns that may indicate efforts to inflate sales figures artificially. A company can configure the timeframe for review as well as indicate the percentage of deviation that would be considered abnormal. For example, a company may want to review revenue that is close to a financial closing period and is also 50% greater than an average of prior periods.

ESG Reporting Risk

Companies also face mounting Environmental, Social and Governance ("ESG") reporting requirements. Scrutiny regarding sustainable practices by investors and consumers has focused on "greenwashing," or falsely making positive environmental claims. In addition, many companies find it very cumbersome to prepare, review, and assess information regarding their ESG performance, given the large and disparate volumes of data involved. Providing misleading ESG reporting to benefit the company could run afoul of the Economic Crime and Corporate Transparency Act.

By leveraging an automated Approvals & Disclosure workflow tool, the nature and purpose of proposed sustainability initiatives can be verified in advance and reported accurately after the fact. For example, a company may use such a tool to ensure that donations go to organizations that align with its sustainability goals. Due diligence, screening, and investigative diligence reports built directly into the workflow can further help ensure that such ESG expenditures are going to bona fide entities with legitimate impact. In addition, a robust workflow tool will include functionality to manage such ESG-related projects by, for example, requiring recipient entities to provide documentation around the use of the funding and impact. With a full audit trail tracking the life cycle of such ESG expenditures, an organization can ensure its ESG reporting is accurate and respond timely and completely to audits or other stakeholder inquiries.

Finally, a Compliance Monitoring tool can enable your company to see the financial data related to ESG expenditures and subject them to advanced risk analysis to ensure they are not being misspent or are otherwise problematic. Such a tool can also provide end-to-end risk coverage by confirming the amount requested and approved in the Approvals & Disclosure tool correlates to the actual amount paid, or if the amount was paid to a different entity than the one approved and authorized. By using this detective control, an organization can mitigate risks from bad actors seeking to mislead the company and taint its ESG program and reporting efforts.

Conclusion

Through implementing proactive compliance program elements which are monitored and tested for effectiveness, an organization can demonstrate its effectiveness at preventing fraud and remain in compliance with the Economic Crime and Corporate Transparency Act.

Using purpose-built compliance technology that incorporates end-to-end compliance risk assessments, controls, and monitoring is the best way to implement these controls in a scalable and cost-effective manner.

One-on-One Advice

Our team of experts has implemented Case IQ for compliance teams around the world.

They are available - free of charge - to speak with you and share the best practices we've learned. No pushy salespeople, just a chance for you to learn from our experts.

With our suite of compliance tools, reporting hotline, and case management software, plus a 25-year track record of successful implementations, Case IQ is the global leader for end-to-end compliance risk management. To get a demo please visit www.caseiq.com/request-a-demo.

To book your one-on-one, please contact:

(800) 465-6089

sales@caseiq.com
media@caseiq.com
support@caseiq.com

300 March Road
Suite 501 Ottawa,
Ontario K2K 2E2
Canada

DON'T MISS OUT

Visit CaseIQ.com for more great investigation resources.