



DOJ CORPORATE COMPLIANCE GUIDANCE AND CS3D – ACHIEVING DUE DILIGENCE COMPLIANCE

BY DERMOT CORRIGAN

In its updated ECCP (Evaluation of Corporate Compliance Programmes) guidance of September 23, the US Department of Justice has placed much greater emphasis on third-party risk management, with significant implications for supply chain risk management:

- “A well-designed compliance program should apply risk-based due diligence to its third-party relationships”
- “Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships”
- “How is the company leveraging available data to evaluate vendor risk during the course of the relationship with the vendor?”

These requirements are similar to those of the EU’s Corporate Sustainability Due Diligence Directive (CS3D), albeit looked at through a different risk lens. While CS3D’s focus is more on ESG rectitude, both regulations send a clear message: revolutionise your approach to third-party risk management or face severe consequences. No longer will it be considered adequate risk mitigation to rely on third-party disclosures alone. Your third-party risks are now *your* risks.

Here, smartKYC’s CEO, Dermot Corrigan identifies the challenges to third-party due diligence compliance and argues how technology is key to a robust, systematic and sustainable third-party due diligence programme.

The Monumental Challenge of Regulatory Compliance for Global Organisations

Recent conversations with CPOs, heads of supply chain and third-party due diligence specialists of multinational corporations has revealed that they are asking the same three questions. In light of these new requirements, how do we:

1. Efficiently identify legacy risks in current supplier base?
2. Ensure due diligence on new suppliers is comprehensive?
3. Monitor suppliers for new risks as they emerge during the relationship?

The scale of the challenge is significant.

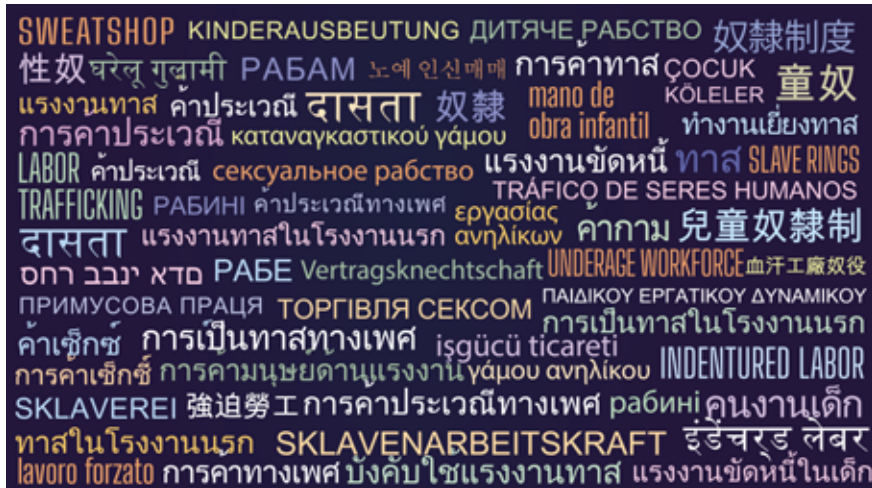
The size of the supplier base: For a large multinational the number of suppliers can run into the many thousands, sometimes the many hundreds of thousands and that is before one considers the possibility of vetting associated parties such as beneficial owners, directors, significant shareholders and subsidiaries. How can they be all screened promptly and cost-efficiently?

The extent of risks that need to be considered: Bribery, sanctions, other financial and non-financial criminality, ESG failings, security breaches, exposure



to risky countries, questionable integrity. These might all be risk factors that require assessment. Our ESG risk framework extends to over 100 concepts and while governance does not fall within the scope of the CS3D, the environmental and social misdemeanours we identify are sufficiently fine-grained that companies can know what 'bad' looks like in their screening due diligence.

The geographic distribution of supply chains: If your suppliers operate in emerging and frontier markets, how can you ensure you elicit local risk intelligence written in the local language or script?



Minimising noise and maximising insight: The investigative work of third-party due diligence, particularly when dealing with unstructured information like web content and news items is overwhelming. The sheer volume, repetition and ambiguity inherent in such data is daunting.

AI: The Only Viable Solution to the Compliance Challenge

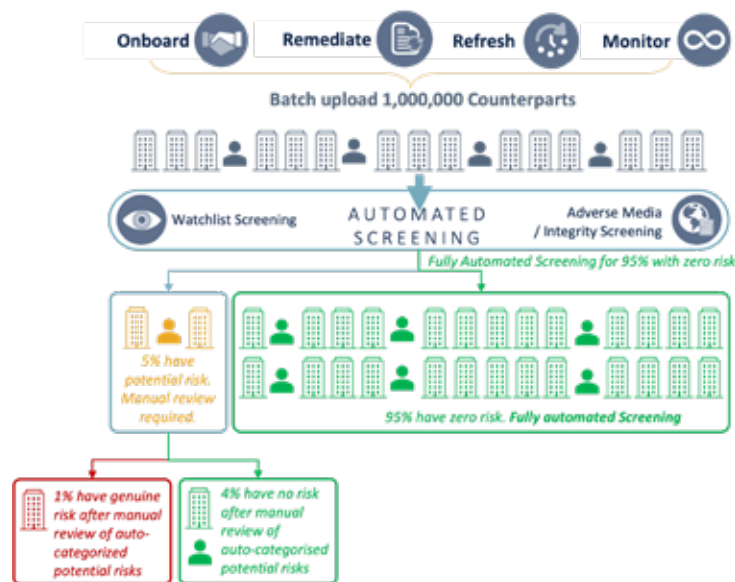
In this new regulatory era, Artificial Intelligence is the only realistic solution to these overwhelming challenges. Here's how it can answer the three questions raised, above:

1. Efficiently identify legacy risks in current supplier base

Our tools can dovetail with your procurement and supply chain applications so that your entire supplier base can be batch processed for risk assessment. The outcome would typically be that the majority will have zero legacy risk and a small minority will be judged by the system to require triage for human review, thus saving time and money looking for risks where none exist.

2. Ensure due diligence on new suppliers is comprehensive

Not only can our software integrate and harmonise a broad spectrum of sources ranging from sanctions lists, watchlists, web search engines, corporate databases and sources of specialist ratings, but it also specialises in reading documents such as news items and web pages. So instead of the analyst having to read lots of documents, analysts see the 'so what' first. And with our new generative AI integration, that 'so what' can be summarised automatically, succinctly and with a high degree of accuracy. Ironically, note, while this ECCP guidance highlights the compliance implications of using AI, smartKYC's implementation of it addresses all the potential risks, including traceability and human oversight.



3. Monitor suppliers for new risks as they emerge during the relationship

a. Periodic Refresh

Once any initial screening has been completed on a third party, a subsequent review on the entity can be run after a specified period has lapsed since the previous screening event. Only net new information since the last review (deltas) are presented to the user for review. Periodic Refreshes can be scheduled or launched manually.

b. Continuous Monitoring

This necessitates 24/7 risk vigilance with real-time, event-driven refresh triggers to the systems or people responsible for risk assessment. smartKYC's product, smartEYE, enables this, offering the ultimate defence against ESG, supply chain, financial criminality and reputational risk associated with third parties not only at the beginning of a relationship but throughout its entirety.

Empowering a Risk-Based Approach to Compliance

The DOJ's 2024 guidance, along with the EU's CS3D, signals a new era in corporate compliance and third-party risk management, reflecting the evolving landscape of global business, where emerging technologies and complex supply chains present both opportunities and risks.

For multinational corporations, the message is clear: compliance programmes must be dynamic, data-driven, and deeply integrated into business operations. The emphasis on continuous monitoring, risk-based approaches, and the management of emerging technological risks underscores the need for sophisticated, AI-driven solutions in third-party risk screening as using a human-led approach to achieve compliance is no longer feasible, let alone affordable.

In order to harness AI's immense benefits while mitigating any of its associated risks, organisations must adopt a controlled AI framework. This involves collaborating with AI experts to refine models, conducting ongoing research and testing, and maintaining a balance between AI efficiency and human oversight. Through this controlled use, organisations can ensure full traceability back to original sources, mitigate AI-related risks and potentially reduce research and reporting time by a substantial margin.

As regulatory frameworks evolve, those who successfully integrate AI into their compliance programmes will be better positioned to succeed in the complex landscape of global business operations and third-party risk management.

[Find out more about smartKYC.](#)



International House,
36-38 Cornhill,
London,
EC3V 3NG,
United Kingdom

Get in touch:
www.smartkyc.com
info@smartkyc.com