GROUND TRUTH
INTELLIGENCE

MEETING THE NEW CHALLENGES OF DUE DILIGENCE





MEETING THE NEW CHALLENGES OF DUE DILIGENCE



By **Matt Kelly**

Every compliance professional today understands that due diligence is a critical capability for effective compliance programs. The challenge for too many, however, is that your need for better due diligence — more accurate information, delivered more quickly, on more risk areas — is expanding and accelerating faster than the actual capabilities you have.

That is, for many years compliance programs have focused on anti-corruption due diligence, a task already difficult enough. Now regulators are requiring due diligence on additional business risks: cybersecurity, sanctions, and human rights, to name just a few. At the same time, compliance programs need to deliver better-quality due diligence information, on an ongoing basis.

What's really happening is that **due diligence is evolving into a larger program of third-party risk management.** At a long-term, strategic level that's good for the compliance officer: it means you'll play a more important role in the business to help senior management use third parties wisely.

In the immediate term, however, this shift is forcing compliance programs to develop new due diligence capabilities, both technical and organizational. Let's explore what those are.

> *"At a long-term, strategic level that's good for the compliance officer: it means you'll play a more important role in the business to help senior management use third parties wisely."*

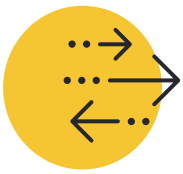
THE DRIVERS OF MORE DUE DILIGENCE

Before compliance officers contemplate how they should revitalize their due diligence capabilities, it's important to understand where this need for greater due diligence comes from. We can identify several distinct drivers.



COMPANIES ARE RELYING UPON MORE THIRD PARTIES GENERALLY

Large corporations now routinely have thousands of third parties providing various services, and even small or mid-sized businesses might have hundreds of third parties doing the same. Moreover, the range of services those third parties provide has expanded as well. Many companies now rely on third parties for mission-critical services such as outsourced accounting functions or shipping services. As those relationships proliferate and deepen, so does the level of oversight you must exercise.



NEW REGULATIONS HAVE PUSHED THIRD-PARTY RISK INTO NEW FIELDS

For example, regulators have adopted a host of privacy and cybersecurity rules meant to protect personal or confidential data — and as a practical matter, that means you must now review your third parties for potential security risks. We can say the same for forced labor; the United States adopted the Uyghur Forced Labor Prevention Act in 2021, and now businesses must assure that their goods aren't sourced from Uyghur forced labor in China. Economic sanctions, ESG regulations, and other measures are also expanding the range of due diligence companies must perform.



THE ENFORCEMENT CLIMATE IS CHANGING

Yes, regulators are pushing to hold companies more accountable for compliance violations — but that change is unfolding on two fronts. First, we see continued enforcement of anti-corruption, sanctions, and data privacy rules, where third parties almost always play a starring role in how the violation happened. At the same time, regulators are also trying to be more lenient with companies that voluntarily self-report their violations. (For example, consider the Justice Department's new policy for more leniency for violations discovered at acquisition targets, if a company promptly self-reports and remediates the trouble.) Taken together, these two enforcement pressures ratchet up the need for strong third-party oversight.



STAKEHOLDER SCRUTINY IS RISING

Even more threatening than greater regulatory enforcement is the prospect of various stakeholder groups holding your company more accountable for third-party misconduct. For example, non-governmental organizations might blindside your company with forced-labor allegations on social media, and quickly form alliances with unhappy customers and disaffected employees. You could be encircled by the opposition before you even fully understand the allegations against you.

WHY *'TRADITIONAL'* DUE DILIGENCE NO LONGER WORKS

Given all the new pressures discussed above, it's little surprise that traditional approaches to due diligence — manual workflows developed in response to specific regulatory requirements, and typically executed in separate silos of the enterprise — no longer suffice. For far too long, many companies invested in due diligence capabilities only because regulatory pressures demanded it: *"We have this regulatory compliance obligation telling us to worry about third parties in this way, so those are the due diligence practices we'll adopt, and nothing more."* That approach is no longer feasible, for three principal reasons:

01.

It places too much emphasis on onboarding due diligence at the start of a business relationship, rather than ongoing monitoring throughout the relationship.

02.

It allows each silo of your business to dwell on its own due diligence needs: IT security focused on cyber risks, compliance on corruption risk, procurement on human trafficking risk, and so forth. Nobody has any sense of the total third-party risk for the enterprise.

03.

It approaches the entire question of third-party oversight as a compliance burden to fulfill, not a business risk to be managed thoughtfully and consistently over time.

Remember what we said earlier: third parties are now enmeshed in modern business operations, across the whole enterprise; and they pose a wide range of risks — with potentially dire consequences for mishandling those risks.

This means that traditional due diligence programs, where each business function implements its own procedures for the risk it worries about, is no longer tenable. It won't scale to keep pace with the expanding number of third parties you have, nor the expanding range of third-party risks marching into your enterprise. It allows for inconsistencies in due diligence across your enterprise, which will give senior managers an imprecise understanding of the risks they have and leave you facing uncomfortable questions from regulators should a violation happen.

To meet the compliance and risk management challenges of today — challenges that are here to stay; that won't recede any time soon — companies need a better approach.



WHAT A MORE COMPREHENSIVE DUE DILIGENCE PROGRAM MUST ACCOMPLISH

Fundamentally, modern due diligence must provide better analysis of all a third party's risks, so that you can understand which laws and regulations might apply to that business relationship. Armed with that insight, the compliance officer can then assign a proper level of oversight to the third party throughout its business relationship with your enterprise.

From those requirements, we can derive several capabilities that your due diligence solution will need to have:

- An ability to **integrate data from multiple sources** and in multiple formats, since you're likely to take in data from a wide range of sources. (Specifically, the solution should use APIs and artificial intelligence to sort that first intake of data and begin triage.)
- **Strong data analytics and risk scoring,** so you can identify high-risk third parties more quickly for enhanced due diligence or other precautionary measures.
- **Due diligence and monitoring procedures** that fit seamlessly with other parts of the enterprise, so that operating units (and even your third parties themselves) suffer minimal disruption from your due diligence program.
- **Automated due diligence workflows** based on certain rules developed by you and other executives at your enterprise. Essentially, your due diligence solution should be able to anticipate, *"If the third party falls into category X, the following happens."*
- **Better holistic reporting,** so that the compliance officer can see the entire picture of third-party risk, and provide better briefings to senior management about how the company's use of third parties affects its overall level of risk.

Your due diligence program also needs to support the broader goal of ongoing monitoring, so that your third party data doesn't go stale. For example, if your overseas real estate consultant goes from scouting office locations to negotiating leases and securing operating permits, you'll need to re-perform a potentially higher level of due diligence on that agent. Can your solution and due diligence partners pivot into that expanded scope? Can you capture that new data quickly, and integrate it into existing due diligence profiles for a fresh risk score?

In short, your due diligence program will need to keep the company's use of third parties aligned with your risk model. That will require technology that is both sophisticated and versatile.

HOW TO GET STARTED

The first step in strengthening your compliance program is convincing the rest of the enterprise that better compliance serves their interests, so start there. Show senior management how better due diligence capabilities (in whatever form that may take: more knowledge about your third parties, better processes, a more integrated approach to onboarding and monitoring) isn't just about meeting new compliance demands. It's about harnessing your supply chain in a risk-aware manner, so your third parties deliver the most performance for the least risk. Moreover, an effective due diligence program should alleviate burdensome compliance procedures along the way.

You'll also need to work with operating business units to understand the risks they are bringing to your enterprise by their use of third parties. From there, you can next develop the due diligence and monitoring capabilities your compliance program will need; and then keep working with the business units to craft sensible, effective onboarding, monitoring, and termination procedures that reflect those risks.

Obviously technology will play a critical role. You will need to find the right technology partners and due diligence vendors to fit your needs, and that search requires careful consideration. That may mean you still need multiple vendors, each one best-in-class for its specific solution (data management, due diligence research, monitoring, and so forth), but thanks to API connections, managing multiple vendors can now be done more easily than in the past.

And while technology integration can be a tedious or painstaking journey, ideally it should be a straightforward process that flows from all the planning and consensus building you've already done. Your due diligence technology should fit your risks, procedures, and objectives — not vice-versa.

For better or worse, external circumstances are making the need for better due diligence quite clear. Develop a clear understanding of how those pressures affect your own organization, find the right technology and due diligence partners, and then bring your compliance program into the modern age.

> *"Moreover, an effective due diligence program should alleviate burdensome compliance procedures along the way."*



MATT KELLY

Editor & CEO

Radical Compliance

Matt Kelly is editor and CEO of RadicalCompliance.com, a blog and newsletter that follows corporate governance, risk, and compliance issues at large organizations; it includes the Compliance Jobs Report, a weekly update on compliance professionals moving around the industry. He also speaks on compliance, governance, and risk topics frequently.

Kelly was named as *'Rising Star of Corporate Governance'* by Millstein Center for Corporate Governance in inaugural class of 2008; and named to Ethisphere's 'Most Influential in Business Ethics' list in 2011 (no. 91) and 2013 (no. 77). In 2018 he won a Reader's Choice award from JD Supra as one of the Top 10 authors on corporate compliance.

Kelly previously was editor of Compliance Week, a newsletter on corporate compliance, from 2006 through 2015. He lives in Boston, Massachusetts, and can be reached at mkelly@RadicalCompliance.com

GROUND TRUTH
INTELLIGENCE

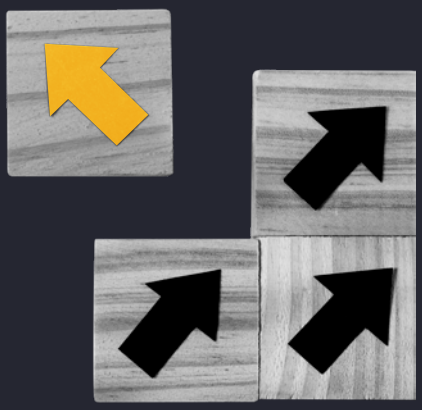
Due Diligence | Document Retrievals |
Site Visits | Human Source Enquiries

250+ Jurisdictions

2000+ Investigators

80+ Languages

API Capabilities



www.gtintel.io

Get in touch for further information:

info@gtintel.io

+44 203 773 6509

GROUND TRUTH INTELLIGENCE

Telephone House

7th Floor, 69 Paul Street

London EC2A 4NQ

United Kingdom