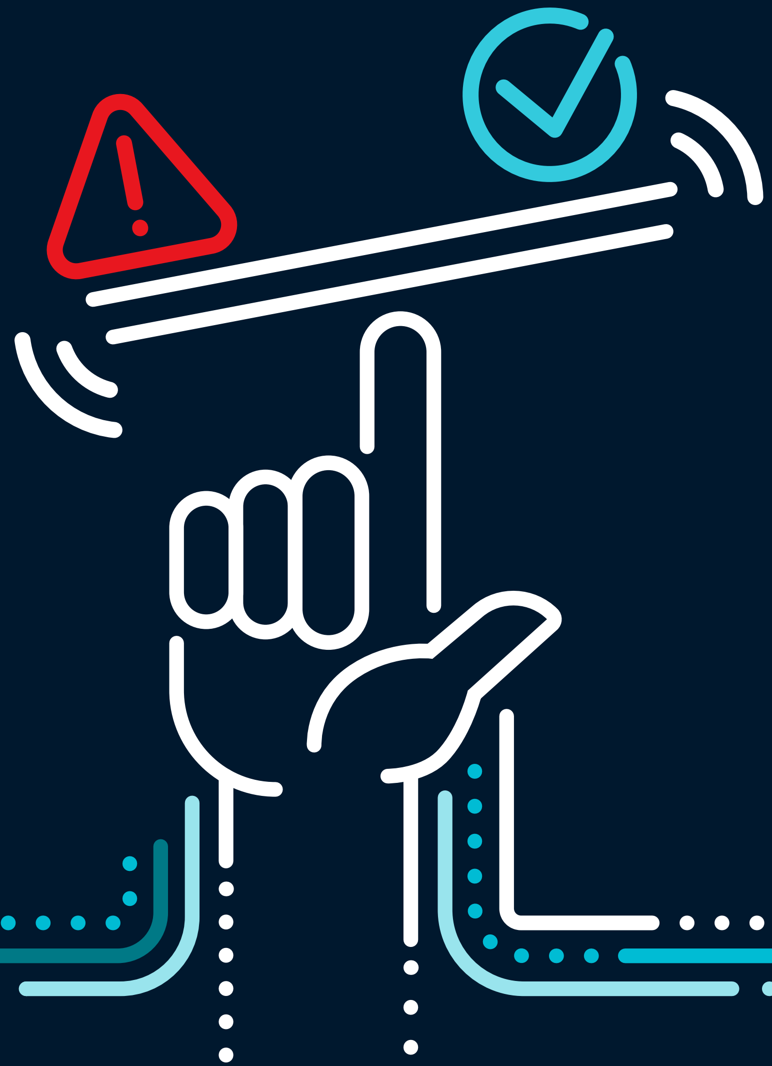
LexisNexis®

Nexis® Solutions

Tipping Point

Ten Trends in Third Party Risk and How to Manage Them Effectively



Relationships with third parties and suppliers are vital to any business. They are also a major source of risk. Our ebook analyses the urgent third party risks facing your business, and how you can overcome them.

Managing risk is the most important task of any CEO. Every CEO prioritizes—or should prioritize—ensuring their company's activities are free from bribery, corruption, human rights abuses or other ESG failures. But in the modern, globalized world of business, this is no longer enough to effectively manage risk.

Companies rely on third parties and suppliers around the world to deliver their products and services, and these third parties are increasingly becoming their main exposure to risk. In a 2023 survey by Compliance Week, 82% of company executives said indirect bribery by third parties is a greater risk than bribery from their own personnel.

Why is third party risk now at the top of a company's agenda? Ten trends have come together to bring third party risk management to a tipping point. Seven of them are already in effect, such as global legislation requiring companies to take additional steps to monitor their third parties for bribery, corruption and human rights abuses. Three are predicted to impact companies soon, including a seismic shift in the way supply chains are expected to operate in the future.

In this ebook, we dive deeper into these ten trends, then offer practical suggestions for companies to mitigate the risks each poses. Finally, we explain how LexisNexis can help your firm to surface third-party risks more effectively and efficiently than ever by using the right data and technology.

7 TRENDS FOR TODAY

Why has third party risk reached a tipping point in 2023–24? Seven main trends have reshaped the risk landscape and, as a result, the way companies must identify and manage these risks.

1 Tougher Anti-Bribery and Corruption (ABC) legislation

Regulators in many countries have strengthened the obligations on companies to manage ABC risk in recent years—and increased the punishments if they fail. Many of these laws and regulations specify the steps companies must take to identify and manage third party risks. Regulators have also expanded the type of bribery and corruption risks companies need to screen for; and given enforcement agencies more powers to take action against alleged breaches. For example:

FRANCE

Guidance released by the anti-corruption agency (AFA) in late 2020 states that companies must map the bribery risk of third parties according to each company's activities, size and structure. It also defines the role of compliance and risk officers.

BRAZIL

The government published a new decree in 2022 to improve enforcement of the Clean Company Act of 2014, which aims to tackle corporate bribery and corruption. It outlined new ways to measure companies' compliance programs, including requirements around due diligence for Politically-Exposed Persons (PEPs) and other risk factors.

SAUDI ARABIA

Since 2021, the Kingdom has expanded its Anti-Bribery Law to cover private companies, and set up an Oversight and Anti-Corruption Authority to investigate corruption allegations and refer companies to a criminal court. This reflects a wider trend in other Middle Eastern countries, including the United Arab Emirates and Bahrain, who are seeking to demonstrate a focus on compliance to help attract foreign investment.

Another regulatory trend is to incentivize companies to improve their management of third party risk by using the carrot as well as the stick. For example:

US

The landmark Corporate Enforcement Policy was updated in 2023 to strengthen the incentives offered to companies to voluntary-self disclose evidence of wrongdoing and improve their compliance. Companies that self-report can now receive up to 75% off the recommended fine—an increase on 50% previously.

SINGAPORE

The Criminal Justice Reform Act (2018) introduced Deferred Prosecution Agreements (DPAs), which allow prosecutors to agree not to prosecute a company if it meets conditions like implementing adequate compliance and remediation processes. DPAs have already been adopted in countries including the US, UK and France to encourage companies to self-disclose third party violations which were detected during due diligence.

2 Mandatory human rights and environmental due diligence

The dominant legislative trend of the last three years is that regulators are mandating companies not just to monitor third parties for bribery and corruption risk, but also for Environmental, Social and Governance (ESG) risks. The first to adopt these requirements include:

GERMANY

The Supply Chain Due Diligence Act, which came into force in January 2023, mandates regulated companies to carry out due diligence and risk management to mitigate human rights violations in their supply chains. Failure to comply could incur fines of up to 2% of global revenue and temporary exclusion from public contracts. The Act's scope will widen in January 2024 so that it applies to even more companies.

EU

The Corporate Sustainability Due Diligence Directive is now in its final stages of negotiation and expected to take effect next year. It will require regulated companies operating in EU member states to ensure activities by the business and its suppliers comply with strict human rights and environmental sustainability criteria. Every EU country will need to ensure its regulatory and legislative framework is compliant, which is expected to precipitate a new raft of legislation.

NETHERLANDS

The Child Labour Due Diligence Act 2019 mandates any company selling or supplying to consumers in the Netherlands to investigate whether child labor has been involved in the production process throughout the supply chain. The Act requires companies to assess whether there can be a "reasonable suspicion" of involvement of child labor. This suggests an expectation to screen third parties against a wide range of sources, including media, not just legal sources.

USA

The Uyghur Forced Labor Prevention Act presumes that all goods produced in Xinjiang, China, came from forced labor. As a result, companies cannot import these goods to the US unless they prove through due diligence that forced labor was not involved. The US Securities and Exchange Commission has also created a Climate and ESG Task Force within its enforcement division to identify ESG-related misconduct by companies.

HONG KONG

In December 2022, new requirements were introduced for banks to meet standards for managing climate risk, and make appropriate disclosures to the regulators on this activity.

What will this trend mean for companies in practice? The Institute of the German Economy polled firms on the impact of Germany's legislation in 2023 and found it was already changing companies' behavior:

- **18%** of companies said they would change their sourcing practices so that they only use third parties in countries with high standards on human rights, compliance and the environment.
- **12%** of companies indicated they would withdraw from supplier and third party relationships in jurisdictions with a high risk of environmental or human rights abuses.
- The CEO of a company in Bangladesh said that human rights due diligence legislation such as Germany's leads to major companies requiring their third parties to have "invested heavily in ESG issues".

The results from the survey indicate that the introduction of a due diligence regulation is costly."

— The Institute of the Germany Economy, *following a survey of the impact of mandatory human rights due diligence legislation*

3 Harsher enforcement against third party regulatory failures

When companies find themselves in breach of regulations, it is often because of the activity of their third parties—for which the original company remains liable. This is borne out by some of the major enforcement actions against companies in 2023. For example:

A multinational telecommunications company based in Sweden pleaded guilty in March 2023 to violating the anti-bribery provisions of the US Foreign Corrupt Practices Act and must pay a $206 million penalty. This came after it allegedly failed to meet the conditions of a Deferred Prosecution Agreement over alleged bribery of government officials and falsification of records in China, Vietnam, Indonesia, Kuwait and Djibouti. The regulator singled out the use of third parties to allegedly facilitate bribery payments and hold “slush funds”.

A mining company in Australia was charged by an investigative body in the country in February 2023 for failing to supply documents relating to more than 30 cases of alleged sexual harassment at mining sites. Activities taking place off-site from a company’s headquarters, whether that’s by a third party or a subsidiary, are more difficult for the parent company to monitor.

A chemicals firm was fined $218 million by US regulators in September 2023 over its alleged use of third parties to bribe government officials in Vietnam, Indonesia and India.

One of the first cases under Germany’s Supply Chain Due Diligence Act was brought against several major car companies in mid-2023 for alleged force labor in their supply chains in China. No convictions have followed to date, but the investigation indicates that enforcement agencies are ready and willing to take action against alleged ESG failures in the supply chain.

Screening third parties for ESG risk is not only important for avoiding enforcement action. Companies that can demonstrate a transparent and positive ESG record have found that this can drive commercial success.

This was reinforced by a paper in the Harvard Business Review in 2023 on the "rapid and dramatic transformation" of the role of the Chief Sustainability Officer (CSO). Until recently, the role typically focused on communicating about their firm's corporate social responsibility activities. Now, the Harvard report has found that many CSOs sit on a company's board and are charged with integrating ESG into the business' core strategy. As the authors wrote: "They once focused on optics and reputation. Today many are interacting with investors and helping set strategy.

This development reflects what surveys have been telling us for the last few years: that customers, investors and employees want to buy from, invest in and work for firms that can demonstrate they make a positive impact on the world. Significantly, younger people tend to be particularly concerned about ESG, so companies should take action or risk becoming losing the next generation. A survey by Harris Poll in summer 2023 found that young people expect to see "meaningful evidence of business ethics" by a company, and only 6% considered statements from the CEO to count as meaningful evidence.

A firm's laudable ambitions on ESG can be undermined if it is revealed to be doing business with a third party with a negative ESG record. By contrast, companies can demonstrate strong ESG standards by being transparent about their third party due diligence and supply chains. For that reason, every company should carry out third party due diligence for ESG risk.

Some CSOs have moved away from a role centered on messaging and instead are spearheading the true integration of material ESG issues into corporate strategy."

—Professors Bob Eccles and Alison Taylor,
Harvard Business Review 2023

5 New third-party risks for banks

In 2023, the Wolfsberg Principles were updated for the first time in six years. While not official regulations, the Principles are developed by an association of 13 global banks and regarded as influential guidelines of best practices for anti-bribery and corruption processes and ethical business.

The latest iteration singled out activities by a third party as a "potential liability" for financial institutions. It identified "red flags" which banks should screen third parties for, which could warrant enhanced due diligence.

These include:

- A third party making "unreasonable" or "unsupported objections" to ABC due diligence being included in a contract or transaction agreement.
- Use of a shell company or other non-transparent corporate structure.
- A company with a "flawed background or reputation".
- The "unusual involvement of Public Officials in commercial matters".
- A third party's jurisdiction; customer base; industry; and type of products of services.

The guidance concludes that, once companies have identified the level of risk posed by a third party, they should apply proportionate due diligence and ABC controls. Crucially, they should also "periodically assess" whether they are capturing new and emerging risks.

6 Unprecedented sanctions changes

A hallmark of the conflict in Ukraine has been the extensive use of sanctions by all sides as a means to persuade, threaten or reprimand other countries.

Numerous iterations of sanctions have been imposed by the US, UK, EU and other countries against Russian and Belarusian entities, which have been met with a series of sanctions by Russia. In the meantime, sanctions regimes unconnected to Russia continue to change constantly. For example:

The US Treasury eased sanctions on Venezuela's oil sector in October 2023 after apparent moves towards democratic elections in the country.

The US introduced new sanctions in August 2023 against entities tied to arms deals between Russia and North Korea. It notes that these sanctions applied to any third parties that are at least 50% owned (directly or indirectly) by sanctioned individuals or entities.

If a company is found to be doing business with a sanctioned entity, it could incur significant legal, financial, reputational and strategic costs. In the last year alone, heavy fines have been imposed against global companies for allegedly using third parties to breach sanctions against Russia, North Korea, Iran and Venezuela, and others. For example:

UK tobacco firm agreed to pay more than $635 million in April 2023 after its subsidiary admitted to violating US sanctions by reportedly selling products to North Korea.

A Beverage Company with connections to Hong Kong and the UK was fined by UK regulators in April 2022 for accepting a payment from a third party which appeared to violate sanctions related to the conflict in Ukraine.

An export firm with dealings with multiple third parties agreed to pay £1 million in August 2023 to settle alleged breaches of sanctions imposed by the UK on Russia.

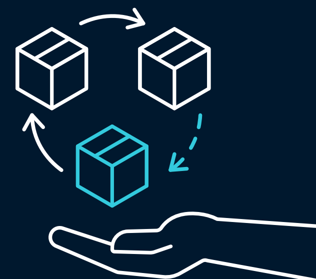
More serious implications for sanctions could follow in European countries, after the EU Council has proposed a Directive to introduce new criminal offenses and penalties for violating sanctions, which will require member states to do more to tackle breaches.

The pace with which sanctions regimes change makes it more likely that companies are doing business with third parties who are on a sanctions list, or doing business in jurisdictions or industries which are sanctioned. Even if a named third party is not directly implicated, it could have a subsidiary or beneficial owner that is—which would still leave the original company liable. It is therefore critical that firms screen all third parties against sanctions, and refresh this due diligence regularly.

“This case and others like it do serve as a warning shot to companies.”

— Matthew Olsen, *US Justice Department, on a record fine for a company breaching sanctions against North Korea*

7 Disrupted supply chains



The supply chain is where companies are most exposed to, and reliant on, third parties for the effective running of business operations, products and services.

If a third party goes out of business, or fails to deliver its promised service because it is dealing with bribery, corruption or human rights allegations, the original company is exposed to reputational risk among its clients and customers, or even to having to cease its operations altogether.

Unforeseen events in recent years, such as the COVID-19 pandemic, the conflict in Ukraine and the blockage of the Suez Canal, have wreaked havoc on supply chains. These events have cumulatively hit corporate bottom lines to the tune of billions of dollars. Disruptions on this scale were once considered 'black swan' events, but they appear to have become the norm. For example, technology and retail firms are currently experiencing delays due to the conflict in the Middle East. While extreme weather events regularly bring supply chains to a halt. The European heatwave in summer 2022 led to a number of data centers going offline, including Google's and Oracle's which power a significant proportion of global businesses.

All the while, a backdrop of rising inflation and energy prices and a cost-of-living crisis has dampened consumer spending and raised the risk that third parties and suppliers go bankrupt. It is therefore unsurprising that BDO's recent poll of 500 medium-sized businesses found supply chain disruption was their primary concern heading into winter 2023.

It is not easy for firms to prepare for the unexpected. But that does not mean they should do nothing. Carrying out effective due diligence on third parties and suppliers can help to establish whether these third parties are in jurisdictions with a likelihood of conflict, human rights violations, bribery and corruption, or extreme weather. Understanding third parties' financial health can also predict how resilient they would be to economic shocks.

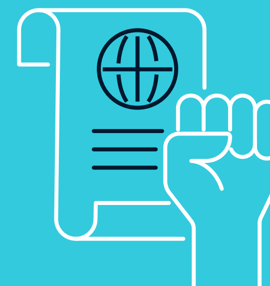
Covid wasn't the cause of the problems with the supply chain, it was a trigger to show how bad it was."

—Jack Buffington, *assistant professor of supply chain management, University of Denver*

3 TRENDS FOR TOMORROW

Third party risks do not stand still, and a trio of trends are expected to force companies to change the way they manage and monitor their third parties and suppliers in the coming years.

1 Replication of human rights due diligence laws



We have already covered the emergence of regulation mandating companies to screen third parties against ESG factors such as human rights and environmental abuses. But this trend is still only in its infancy. While Germany and the EU have already passed rigorous legislation, much more is expected across the world in the coming years. For example:

CANADA

The Fighting Against Forced Labour and Child Labour in Supply Chains Act passed through Canada's parliament in May 2023 and comes into force in early 2024. It requires businesses to report annually on evidence of forced labor in their supply chains.

UK

The government has proposed an updated Modern Slavery Bill which would require firms to publish statements which outline their due diligence process and spell out their assessment of risks from and the steps taken to mitigate them. This would strengthen the Modern Slavery Act of 2015, which already requires large companies to publish an annual statement on their efforts to tackle human trafficking or modern slavery in their supply chain.

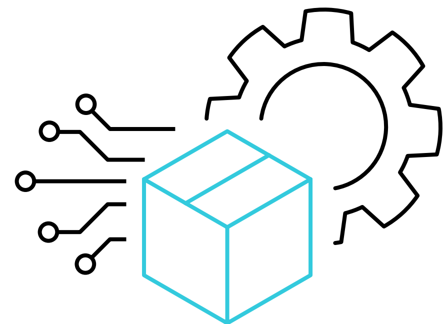
In the next five years, we expect to see a domino effect where, as each law is introduced, other countries respond with their own regulations. The US Treasury Secretary Janet Yellen has expressed concern about the extra-territorial application of the EU's Corporate Sustainability Directive on US firms. While Scévole de Cazotte of the US Chamber Institute for Legal Reform predicts "the US and other foreign countries may retaliate or implement rules of their own" after the Directive is implemented. It is too soon to tell how this will play out—but it seems inevitable the outcome for companies will be more requirements to improve their human rights and environmental due diligence.

2 Intelligent supply chains

For a company to understand third-party risk, it needs visibility over the entire supply chain that goes into making its products and services.

This is not easy to achieve—and impending changes to how supply chains operate could complicate it further. AI and technologies like blockchain are increasingly being used to power supply chains. Shipping giant Maersk predicts generative AI will cause a "once in a lifetime kind of disruption" to supply chains, while Morgan Stanley forecasts that "autonomous vehicles, drones and blockchain could make supply chains fully automated in the future.

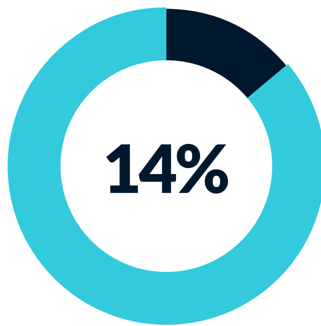
Automated supply chains could remove the potential for bribery by humans and provide a digital footprint (often over the blockchain) of each chain in the link. But the reliance on technology could also create a gray area where companies cannot demonstrate an absence of forced labor in the early stages of the supply chain. While the potential for corruption remains in the people and third parties overseeing the use of technology.



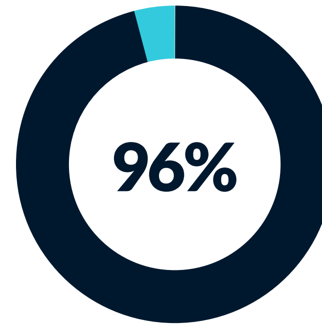
IN FIGURES

THE COMING REVOLUTION IN SUPPLY CHAINS

— Survey by Freightos, August 2023



of supply chain professionals are using AI technology in 2023



plan to implement AI technology soon

3 More complex financial crimes

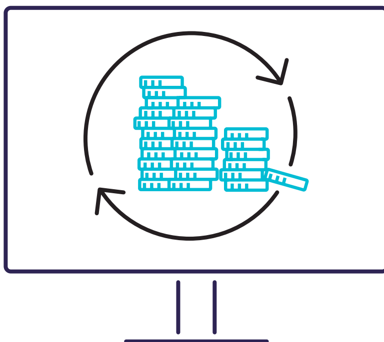
The way financial crime happens is evolving, and criminals are finding ever more sophisticated ways to conceal their illicit activities.

The acceleration of digital banking and remote working after the pandemic has created vulnerabilities for firms seeking to manage third party risks. In the past, if a firm's compliance team flagged a third party as high risk, inspectors could visit their offices to investigate as a form of enhanced due diligence.

But today, it has become common for companies to rely on third parties whose staff they never actually meet in person. This creates a gray area which criminals seek to target. Recent surveys of companies across various sectors suggest these trends are increasing the risk of financial crimes affecting third parties:

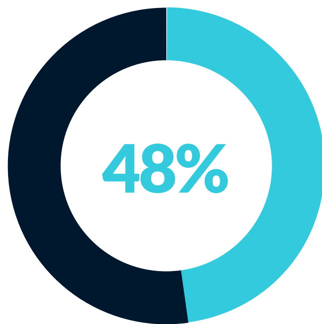
A survey by Compliance Week and Morgan Lewis found that 48% of respondents anticipate an increase to bribery and corruption risks to their company in the next two to three years, and 39% think the risks will stay the same.

Kroll's 2023 Financial Crime Report interviewed 400 senior executives over three continents and found that 67% predict an increase in financial crime over the next year, while 57% said third-party gatekeepers in particular increase financial crime risk.

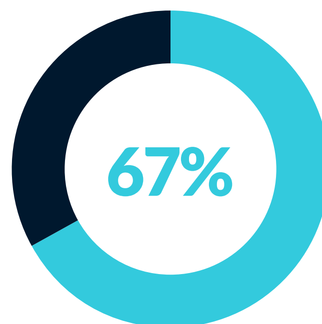


IN FIGURES

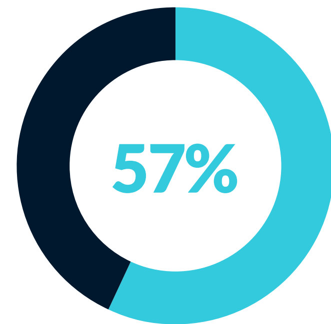
RISING RISKS OF THIRD PARTY CORRUPTION



expect an increase in bribery and corruption risks in the coming years*



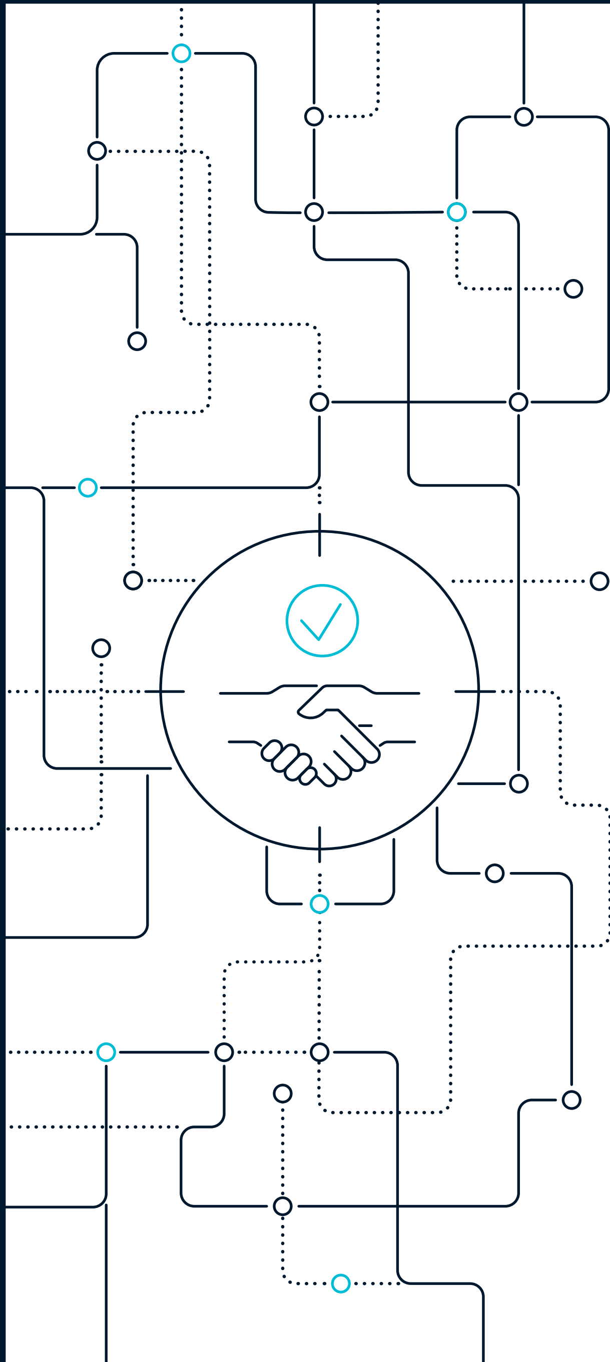
predict an increase in financial crime over the next year**



believe third-party gatekeepers increase financial crime risk**

* Compliance Week/Morgan Lewis Anti-Bribery and Corruption Survey Report, 2023

** Kroll Financial Crime Report, 2023



Survive and thrive in the era of third party risk by powering your due diligence with data and technology.

These ten trends demonstrate the scale of the challenge which third parties pose to companies. Namely, that third party risk is rising, yet it has become more difficult to establish oversight and understanding of third parties' activities and risks. Every trend outlined above requires companies to respond:

TREND		RESPONSE
1	TOUGHER ABC LEGISLATION	Ensure that you comply with all relevant regulatory requirements by implementing an effective due diligence process which monitors third parties for bribery and corruption risk using legal data, company data, media data and more.
2	MANDATORY HUMAN RIGHTS AND ENVIRONMENTAL DUE DILIGENCE	Expand your due diligence approach to go beyond an assessment of a third party's legal and financial risk by establishing indicators of ESG performance. This could involve media and social media searches, and setting clear ethical expectations in any contracts signed with third parties.
3	HARSHER ENFORCEMENT AGAINST THIRD PARTY REGULATORY FAILURES	The best way to avoid enforcement action from the regulators is to root out suspected bribery, corruption and human rights abuses in your supply chain; report any suspicions; and cut ties with a third party which is in breach of regulations.
4	ESG AT THE CORE OF A COMPANY'S STRATEGY	Approach ESG due diligence with skepticism—don't just swallow the bold claims made in a company's annual report. ESG claims should be tested against external sources like news and social media data, and questionnaires of—or visits to—suppliers and third parties when more information is needed.
5	NEW THIRD PARTY RISKS FOR BANKS	Banks should embed a risk-based approach to due diligence which assesses the likelihood that a bank's third party or customer is from a jurisdiction or sector with higher risk, then applies enhanced due diligence when required.

TREND		RESPONSE
6	UNPRECEDENTED SANCTIONS CHANGES	Use near-real-time information on sanctions regimes at national and supranational level to ensure your third parties and suppliers are not subject to ever-changing sanctions—and leverage technology which updates you automatically with any relevant changes.
7	DISRUPTED SUPPLY CHAINS	Acquire and use company data to assess your third parties' financial health, and media and legal data to expose any reputational or legal risks. This will help to determine the likelihood that a disruption could stop a third party from operating, thereby blocking your supply chain.
8	REPLICATION OF HUMAN RIGHTS DUE DILIGENCE LAWS	Stay up-to-date with developing legislation which affects you and your third parties, including HRDD laws around the world because many apply extraterritorially. But the pace of change will be fast, so companies are advised to use a technology solution which flags new and emerging regulations and trends.
9	INTELLIGENT SUPPLY CHAINS	Automated supply chains could make it harder to keep track of the role of individual third parties in the development of products and services. Your firm therefore needs to carry out due diligence on each of their suppliers, and be prepared to report to the regulator on your supply chain with transparency.
10	MORE COMPLEX FINANCIAL CRIMES	As criminals are using technology to carry out bribery and corruption and other financial crimes, so companies must use technology to detect suspected wrongdoing within their third parties. This ranges from using AI and Machine Learning to monitor transactions and deals, to bringing in technology platforms that leverage data to provide risk scores on individual third parties.

Ultimately, companies' best defense against third party risk is to put in place an effective compliance program underpinned by risk-based due diligence. This means screening every current and prospective third party against relevant data sources which can surface risk, then assessing the level of this risk. Higher-risk third parties should be subjected to enhanced due diligence, then a decision made about whether to continue doing business with them. As risks change constantly, this activity should be refreshed periodically.

Thankfully for companies, technology can make this process more efficient and effective than the traditional approach which involved compliance officers spending vast amounts of time making manual searches. Platforms such as Nexis Diligence+™ allow compliance officers to upload spreadsheets of all their third parties, then produces risk scores are provided based on a search of our comprehensive data sources. It delivers these assessments in a way that makes it easy to report to the board, or the regulators.

LexisNexis: Helping companies to detect and manage third party risk

Nexis Diligence+™ is setting a new standard in due diligence, allowing your team to vet and monitor third parties, map relationships, identify red flags and deliver actionable insights—at scale.

Nexis Diligence+™ can help your team to perform due diligence research on a third party company or individual and be confident the results help cover all bases. Our unrivaled data universe provides global perspective, which covers:

An unrivaled collection of reputational, legal and financial content, including sanctions, blacklists, Interpol watch lists, and more.

A global news archive that draws from more than 38,000 sources, some dating back 40 years.

A trove of legal documents, including cases, dockets, verdicts and more.

ESG ratings and news so you can determine who is (and isn't) living up to their commitments.

The ability to maintain an auditable trail of your searches and findings.

Nexis Diligence+™ can help you to leveraging data and technology to take your due diligence to the next level. Its features include:

- **Conduct due diligence at scale.** Nexis Diligence+™ offers high-volume, scalable searching capabilities to streamline your process and save you time.
- **Get results faster.** Nexis Diligence+™ enables you to launch a search and derive results at high speeds.
- **Take advantage of visual, at-a-glance risk information.** Sometimes you need the quick take. Nexis Diligence+™ offers this snapshot in-product, for downloading and in-report delivery.
- **Customize your dashboard and risk scoring.** With Nexis Diligence+™, you can tailor your dashboard and adjust the risk-scoring methodology to reflect your company's unique needs.
- **Add people and entities for analysis with ease.** Nexis Diligence+™ allows you to upload entities at volume via a spreadsheet.
- **Appreciate easier data manipulation.** For example, with Nexis Diligence+™, you can access a condensed view of all saved entities, annotate results, and export them into an Excel spreadsheet.

Do you want your due diligence solution to be:

1 THOROUGH AND TRUSTWORTHY?

2 SCALABLE AND STREAMLINED?

3 EFFICIENT AND EASY?

Why not have all three? Nexis Diligence+™. A higher standard in due diligence.

Enhance Third-Party Risk Management with Nexis Data+. Seamlessly integrate consistently formatted data through a single API source, so you can spend less time wrangling data and more time uncovering valuable insights. Nexis Data+ offers direct access to the critical data required to elevate your risk management strategies and outcomes.

See how Nexis Diligence+™ can take your due diligence to the next level.

LexisNexis.com/**DiligencePlus** | **1-888-466-3947**

LexisNexis, Nexis and the Knowledge Burst logo are registered trademarks and Nexis Diligence+™ is a trademark of RELX Inc. Other products or services may be trademarks or registered trademarks of their respective companies.
© 2024 LexisNexis. All rights reserved US-EDDM-eBook-Tipping-Point-Ten-Trends-TPRM 0324

LexisNexis®