

THE NEW ERA OF DUE DILIGENCE IN 2023

A guide for companies to survive—
and thrive—by managing third-party risk



Nexis[®] Solutions

Due diligence has changed beyond recognition in recent years and continues to evolve at pace. Traditionally, it involved a team of compliance officers manually searching through legal documents and financial accounts to detect risks of doing business with a third party. But in 2023, that model is far from sufficient for a company to mitigate rising legal, financial, reputational and strategic risks.

In this E-Book, we explore ten trends which have transformed what companies need to do around due diligence and regulatory compliance. This includes the explosion of new technologies; the need to understand corporate Environmental, Social and Governance (ESG) impacts; and the increase in enforcement action against due diligence failures. Then, we suggest ten steps companies should take to manage these emerging risks. Finally, we explain how Nexis Diligence+™, a new tool from Nexis® Solutions, can help make organizations' compliance processes more effective, more efficient, and more prepared for the new era of due diligence.

**TEN
DRIVERS
OF THE
NEW ERA
OF DUE
DILIGENCE**



1

Regulatory Expansion

For decades, the [US Foreign Corrupt Practices Act](#) (FCPA) of 1977 was the world's leading piece of legislation proscribing corporate involvement in foreign bribery and corruption. But in recent years, laws have been introduced around the world which make new and more stringent requirements on companies to tackle bribery, corruption and other crimes by carrying out due diligence on their activities—and those of their third parties and suppliers.

Laws covering bribery, corruption, and financial crime including money laundering and terrorist financing continue to be introduced and updated. But the most striking legislative trend at present is that new regulations are mandating companies to carry out due diligence to understand ESG factors like their impact on the environment and human rights. Here are some of the main regulatory developments of recent years:

US and North America

- The US updated its [Corporate Enforcement Policy](#) in January 2023 to strengthen the incentives offered to companies to voluntarily self-disclose evidence of wrongdoing and improve their compliance. Companies which do this can now receive up to 75% off the recommended fine—an increase on 50% previously.
- The [Uyghur Forced Labour Prevention Act](#), which was enacted in December 2021, 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 can prove through due diligence that forced labor was not involved.
- The [Slave-Free Business Certification Act](#) (introduced in the US Senate in 2022) would, if passed, require many large companies to audit their supply chain for evidence of forced labor. Companies would need to publish the results and document their efforts.
- The proposed [Fighting Against Forced Labour and Child Labour in Supply Chains Act](#) is in its final stages of passing through Canada's parliament, and is expected to take effect at the start of 2024. It would require businesses to report annually on evidence of forced labor in their activities and their supply chains.

European Union

- The European Commission has adopted a proposal for a [Corporate Sustainability Due Diligence Directive](#). This would mandate 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 member state will need to ensure its regulatory and legislative framework is compliant.
- The EU has introduced a series of Anti-Money Laundering (AML) Directives in recent years, under which member states must meet certain standards in their regulations against money laundering and terrorist financing. For example, the [Sixth Directive \(6AMLD\)](#), which was proposed in 2021, expanded the definition of a money laundering offence and placed more responsibility on companies for failing to prevent this crime.

France

- France's [Sapin II law](#) requires certain companies to put in place a corporate compliance program to prevent and detect corruption or trafficking of influence in France and abroad. The 2017 law allows companies to enter a judicial settlement of public interest (CJIP) under certain circumstances, as an incentive to companies to comply.
- Updated [guidance](#) subsequently released by the French anti-corruption agency (AFA) in late 2020 states that mapping bribery risk must be adapted to each company according to its activities, size and structure, and it defines the role of compliance and risk officers.

UK

- The UK's [Modern Slavery Act](#) of 2015 was the world's early leader in human rights due diligence legislation, requiring large UK companies to publish an annual statement on steps taken against human trafficking or modern slavery within their organization or supply chain.
- But it had limitations, including not penalizing companies whose statement does not demonstrate taking action, and allowing firms to decide whether to publish their statement on a public registry. So in summer 2022, the UK government proposed an updated [Modern Slavery Bill](#) which would require statements to address firms' due diligence processes and spell out their assessment of risks and the steps taken to mitigate them.
- The UK's capacity to tackle financial crime (including bribery) was strengthened with the passage of the [Economic Crime \(Transparency and Enforcement\) Act](#) in 2022.

Germany

- One of the first examples of legislation to comply with the EU's forthcoming due diligence Directive is Germany's [Supply Chain Due Diligence Act](#), which came into force in January 2023.
- The Act requires regulated companies in the country 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.

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.
- 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 at a wide range of sources, including media, not just legal sources.

Asia Pacific

- Singapore’s [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 had already been adopted in countries including the US, UK and France to incentivize companies to self-disclose any evidence of wrongdoing surfaced during due diligence.
- Banks in Hong Kong must ensure they meet certain requirements for managing climate risk and make appropriate disclosures on their activity to the regulators, following a regulation which came into force in December 2022.
- Australia has introduced new legislation which compels businesses to provide documents related to alleged workplace sexual harassment. The [Fair Work Act](#) came into effect in March this year.

Nordic countries

- The Nordic countries have an outstanding reputation for a lack of corruption in various global rankings. But they are now making efforts to improve their record of enforcing their anti-bribery and corruption laws, which has not always been at the same level. For example, Finland recently introduced new commitments to enforce its bribery laws after a warning by the [OECD’s Working Group on Bribery](#) in 2020.
- New regulations mandating supply chain due diligence are expected in the Nordic countries when the EU Directive comes into force. While only Denmark, Finland and Sweden are EU member states, in practice Iceland and Norway tend to align their regulations in areas like this.

Brazil

- Brazil’s [Clean Company Act](#) of 2014 aimed to transform the country’s ability to hold companies to account for bribery and corruption, following a long-running investigation into alleged bribery involving a state-owned oil company and senior public officials. The Act introduced corporate liability, whereas previously only individuals could be liable for bribery, which raised the risk for companies of engaging in bribery and corruption.
- The Brazilian government published a [new decree in 2022](#) to improve enforcement of the Act. It outlined new ways to measure companies’ compliance programs including due diligence for Politically-Exposed Persons (PEPs) and other risk factors.

2

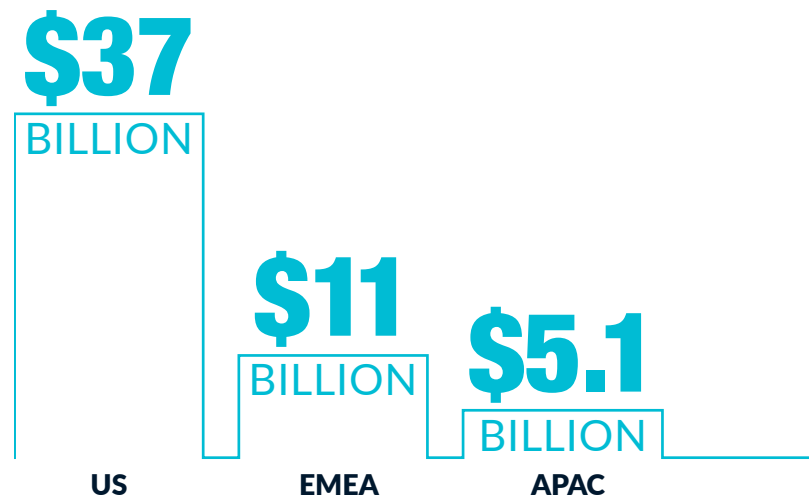
Heavier Enforcement from Regulatory Agencies

Having legislation in place does not guarantee that it will be enforced by a country's regulators. Nonetheless, in the case of anti-bribery and corruption and human rights due diligence legislation, there has been a massive rise in enforcement action and penalty fines against companies over the past decade. The US enforcement agencies have long had a reputation for enforcing the FCPA, and their pace of enforcement elsewhere is increasing with billions of dollars in corporate fines in the last few years alone. Regulators in Europe, South America and Asia are also showing sharper teeth around enforcement. Reading the regulatory judgments accompanying corporate fines reveals that simple failures of due diligence are often a primary cause of enforcement action.

The statistics bear this out. Global fines for corporate failures to prevent money laundering and other financial crimes surged more than 50% in 2022. The US was the most aggressive enforcer, accounting for \$37 billion of the fines. Europe, the Middle East and Africa accounted for \$11 billion of fines, and Asia-Pacific represented over \$5.1 billion—according to [data](#) from Fenergo.

A notable trend is that some of the largest fines were the result of a joint investigation involving enforcement agencies across multiple countries.

Mutual legal assistance is now the norm, so a regulator investigating a company headquartered in their country is more likely than ever to discover wrongdoing by one of their suppliers on another continent. Companies therefore need to carry out due diligence across all countries (and in multiple languages) in which they and their third parties are doing business. In the last six months alone, major enforcement actions have reflected the rising regulatory risks in the main areas of due diligence legislation.



Global fines for financial crimes in 2022



Bribery and corruption:

- A multinational telecommunications company based in Sweden pleaded guilty in March 2023 to breaching the anti-bribery provisions of the US FCPA and must pay a \$206 million penalty. This came after it allegedly failed to meet the conditions of a DPA over alleged bribery of government officials and falsification of records in China, Vietnam, Indonesia, Kuwait and Djibouti.
- A multinational conglomerate agreed to pay over \$160 million in December 2022 to resolve bribery investigations by regulators in the US and Brazil. The company was accused of paying a multi-million pound bribe to a senior official in a Brazilian state-owned oil company in an attempt to win a lucrative building contract.
- A multinational mining firm was fined over £280 million in November 2022 after a UK investigation into suspected bribery in exchange for preferential access to oil in five countries in West Africa. The investigation was pursued in parallel with regulators in the US, Netherlands and Switzerland.



Financial crime:

- A fintech firm was fined \$360,000 by the United Arab Emirates' regulator in August 2022 over alleged due diligence failures in its AML approach. The regulator said the firm had failed to carry out enhanced due diligence on high-risk customers after a business relationship had started. The firm was also alleged to have failed to properly assess the risk of customers according to their nationality and geography.
- A UK regulator fined a bank over £4 million earlier this year for allegedly failing to put in place adequate AML controls, citing deficiencies in its enhanced due diligence checks for higher risk customers.
- A company based in Hong Kong settled with a US regulator in 2022 for allegedly breaching sanctions around trade involving Iran.



ESG:

- In November 2022, it was announced that a financial services company in the US would pay \$4 million to settle claims that it did not sufficiently assess ESG factors in some of the investment products it offered.
- In February 2023, a gaming company was fined \$35 million in the US for allegedly failing to disclose investigations into sexual harassment and misconduct by employees to investors.
- Further enforcement actions are expected after the US Securities and Exchange Commission created a [Climate and ESG Task Force](#) within its enforcement division to identify ESG-related misconduct by companies.
- A mining company in Australia was charged by an investigative body in the country in February 2023 for allegedly failing to supply documents relating to more than 30 cases of alleged sexual harassment at mining sites.

On top of the obvious legal and financial costs of these alleged due diligence failures, the companies involved also suffered reputational risk of global media coverage of their cases and strategic risk of interruption to business during the investigations.



3

The Explosion of ESG

Many of the new laws we explored earlier make it mandatory for companies to understand the environmental and human rights impacts of their activities and those of prospective third parties. But legal risk is not the only reason companies today should carry out ESG due diligence. Surveys show that consumers, investors and employees increasingly want to buy from, invest in and work for companies that can demonstrate a positive impact on society. There is growing evidence that responsible and ethical businesses are attracting custom and enjoying profits. For example:

- Over 5,000 companies have certified as B Corporations with a commitment to benefiting society. From 2017 to 2020 B Corporations in the UK enjoyed an [average](#) turnover growth of 26% from 2017 to 2020, against the UK average of 5%.
- ESG investment funds have outperformed the market in recent years, particularly in the first year of the pandemic. A [survey](#) by PwC in September 2021 found that 79% of investors consider ESG as an important factor in their investment decisions, while 50% are willing to move money away from companies that fail to take sufficient action on ESG issues.
- Another [survey](#) of 1,300 executives (this time by Workiva) found that, when companies carried out ESG reporting, 72% saw better customer retention and acquisition, 69% noticed better employee recruitment, and 70% observed improved investor and stakeholder relations.

Compliance teams face a substantial challenge of finding accurate information on ESG and assessing third parties' claims around the topic. In the Workiva survey, more than 70% of executives said they lacked confidence in their own organization's reporting of ESG impact. While in the PwC survey, 87% of investors said they "suspect that corporate disclosures contain some greenwashing".

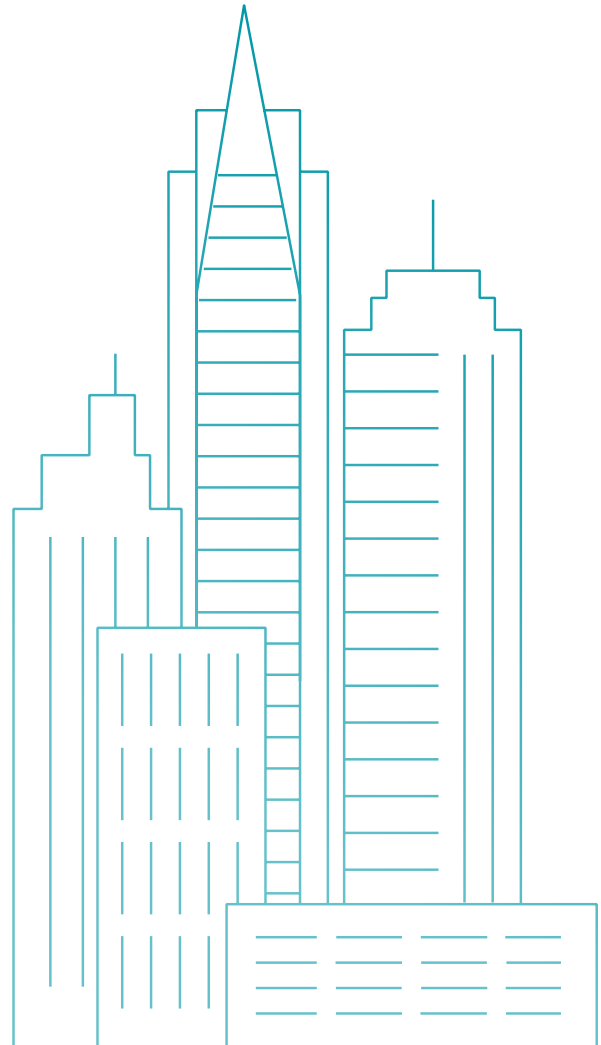
Companies therefore need access to authoritative and relevant sources which capture the true ESG record of a company. This includes alternative sources—for example, recent and historic news coverage from licensed outlets is particularly useful for identifying any potential reputational issues around ESG.

4

Due Diligence as an Opportunity

The success of B Corporations and ESG investment funds demonstrates that compliance is increasingly being recognized by companies as a driver of responsible profits and a sustainable long-term future. As young people are particularly committed to ESG and ethics, this trend is only likely to accelerate. By contrast, growing numbers of consumers, investors and employees have shown that they will end their involvement with a company associated with a breach of regulations around financial crime, bribery or corruption, or ESG.

ESG due diligence is now being demanded and used by sales teams and the C-suite to drive profit, not just manage risk. A company's due diligence process therefore needs to adapt by covering a much wider range of sources than before to accurately establish ESG impact.



5

'Black Swan' Events Have Become the Norm

The business world has always experienced changes, but the period since 2020 has brought a series of external shocks which have forced companies to shut down products and services, and even their offices. The Covid-19 pandemic, European heatwaves, blockage of the Suez Canal and Ukraine war were so unexpected and consequential that they would ordinarily be regarded as 'black swan' events. Such events are supposed to be extremely rare—but they seem to have become the new normal.

External shocks bring severe financial and strategic risks to companies. For example:

- The supply chains of 75% of US companies were disrupted in the first year of Covid-19, according to the [Institute of Supply Chain Management](#).
- Natural disasters such as Hurricane Irma and Hurricane Maria inflicted nearly \$350 billion of losses in 2017, according to McKinsey's [calculation](#).
- The blockage of the Suez Canal by a container ship in 2021 was [estimated](#) by insurance firm Allianz to be costing global trade up to \$10 billion a week.

Compliance officers are often expected by management to play a role in preparing for black swan events. They might be asked to identify any suppliers who are key to their business operations, but who might be vulnerable to bankruptcy in the event of a shock. A better understanding of the financial health of a supplier can help to spot supply chain problems before they occur. Relevant data sources for this include business data and risk scores and a company's beneficial ownership and structure.

Compliance's work in scanning the horizon for risk might also include flagging emerging events or trends which could impact the company—such as the first news stories in China about the emergence of the Covid-19 virus. While, shortly after the conflict in Ukraine started, compliance officers would have been asked to rapidly identify any exposure to Russia among their third parties.



The pandemic has highlighted the importance of planning for extreme disruptions of business, and the very real fact that emerging risks can become active threats much faster than many businesses anticipated.”

- Deloitte Enterprise Risk Management UK survey, 2021.

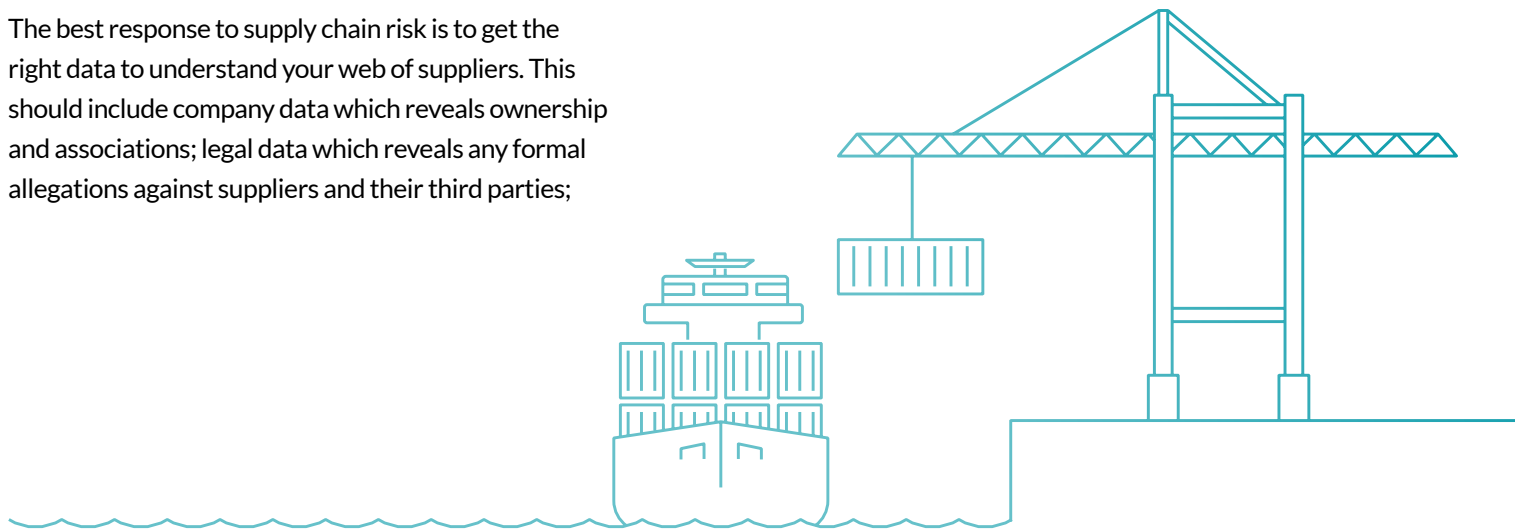
6

Rising Supply Chain Risks

Supply chains have clearly been affected by these disruptions. But even if they hadn't happened, supply chains have become more difficult for compliance teams to monitor. The chains are getting ever longer, more complex, and more global. It is not uncommon for hundreds of entities to be involved in supplying a single product for a company. That gives compliance officers a tough task to monitor a vast number of entities for risk. Compliance teams are also put under pressure to facilitate a quick onboarding process to bring on new suppliers to re-establish business operations after an external shock.

The best response to supply chain risk is to get the right data to understand your web of suppliers. This should include company data which reveals ownership and associations; legal data which reveals any formal allegations against suppliers and their third parties;

and news data across multiple languages which gives insights into rumors to be followed up. This investment will likely be worth it as a 2022 [Gartner](#) survey of 262 supply chain leaders found that those who reduced risks in their supply chain saw disruption to their business fall by two-thirds. It concluded that managing supply chain risk is key to "enhancing resilience and improving competitiveness".



7

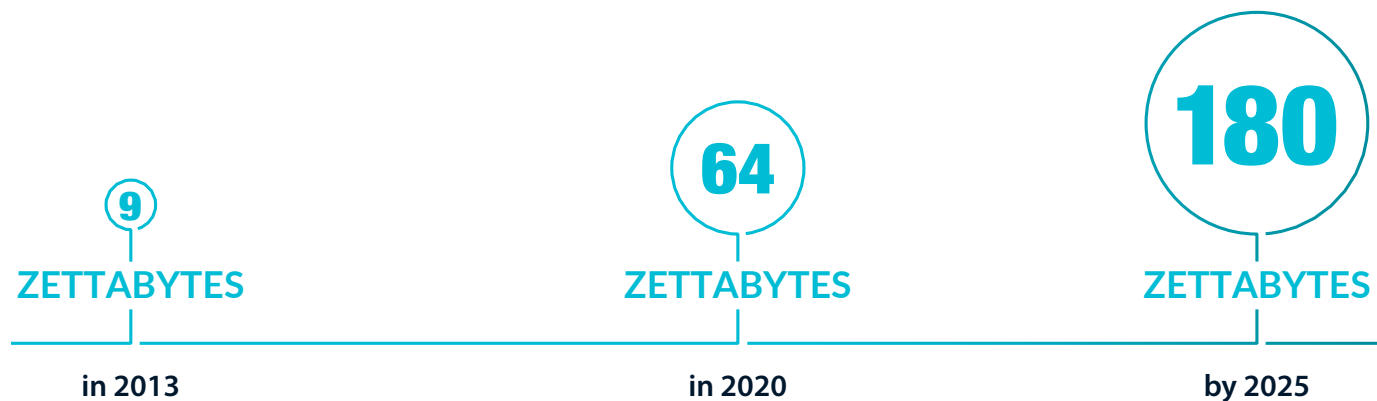
Misinformation and Noise

We live in "the age of noise", as Norwegian author and explorer [Erling Kagge](#) wrote. As our lives move online, we generate more data. [Statista](#) charts the amount of data created and consumed online, which is growing exponentially. It was at 9 zettabytes ten years ago, 64 zettabytes by 2020, and projected to exceed 180 zettabytes by 2025. This is not a new development, but it was accelerated by the pandemic. It brings a significant challenge for compliance officers who are tasked with wading through data to find relevant mentions of their company and third parties.

An additional complication is the proliferation of misinformation, and unsubstantiated claims made

in sources with dubious origins. Social media posts can publicly make allegations about an individual or a company without offering evidence or provenance. While so much data is ephemeral and disappears overnight—Statista found that only 2% of the newly-created data in 2020 still existed the following year.

Compliance officers need to be able to identify and buy in high-quality data from authoritative sources as the basis for decisions on risk. Relying on unsourced or ephemeral data could lead to risk indicators being missed, and as a result legal, financial, reputational and strategic costs to the business.



Amount of data created and consumed online

8

A Shifting Sanctions Landscape

The conflict in Ukraine was swiftly followed by a raft of sanctions by many countries against companies and individuals in Russia and Belarus, as well as sanctions by Russia against foreign entities in retaliation. New entities continue to be regularly added to these lists at an unprecedented rate—for example, the EU published its [tenth package](#) of sanctions against Russia in February 2023, only a year after the start of the conflict.

Regulators expect companies to stay on top of these changes and ensure they are not doing business with a sanctioned entity. In early 2023, the US government launched an [inter-agency initiative](#) to enforce sanctions and export controls targeting Russia and Belarus. The regulator warned that some companies had used intermediaries to evade sanctions. The Assistant Attorney General for National Security said “companies are our first line of defense” around “national-security related corporate compliance”, and another official warned “it is incumbent upon industry to maintain effective, risk-based compliance programs”.

Enforcement agencies will take action against companies implicated in an apparent sanctions breach. For example, a UK company with strong links to Hong Kong was fined £30,000 in 2022 for allegedly breaching European sanctions related to the conflict in Ukraine by doing business with a firm that was subject to an asset freezing order.

Sanctions lists can appear to be a tangled web, ranging from lists maintained by individual national agencies (such as the US OFAC list) to supranational sanctions lists (like the European Union’s). Compliance officers can effectively manage by risk by using a technology platform which automatically flags changes in all relevant sanctions lists in relation to their company’s third parties.

9

The Acceleration of Technology

The best compliance operations are taking advantage of new and longstanding technologies to make efficiency savings and surface risks that would not have been possible to capture under the traditional and inefficient model of manual due diligence searches. For example:

- Technology platforms allow companies to screen multiple entities against a wide range of data sources; carry out risk scoring of these entities; and alert the user to new information or changes to risk levels.
- Artificial Intelligence and Machine Learning technologies can search across high volumes of datasets to offer insights around risk which would not have been possible in a manual search.
- Robotics can be employed to automate a large chunk of the compliance workflow.
- Cloud computing technologies can store data virtually, while APIs can deliver data in an optimized way to power technological applications—without the need for heavy manual involvement in cleaning and optimizing datasets.

In an [Accenture survey](#) of 860 compliance leaders in 2022, 93% of respondents said they believe that advanced technologies will streamline their compliance process. Yet 37% of respondents said their company invests too little in technology, and 72% said their tech budget did not change in the past year. Those companies who can harness technology in their compliance process could therefore gain a competitive advantage.

But technology is not a magic bullet, and its insights around due diligence are only as good as the data which AI and other technologies rely on. So compliance officers should start by acquiring high-quality and relevant data, and if possible seek this data in a format that can easily power technology applications. This might involve using enriched data, and ingesting it via an API.

10

New Pressures on Compliance

The nine drivers above have added new requirements, risks and pressures that typically fall on a company's compliance team. The asks on them now include:

- Reviewing a much broader range of sources to capture ESG risk.
- Surfacing risks before they even emerge, such as alerting management to a key supplier who might go out of business if an external shock occurs.
- Advising the C-suite on risk management, including reputational risk management.
- Contributing to their company's revenue and responsible profit by providing evidence of ethical practices and positive ESG impacts.
- Understanding and adopting new and fast-emerging technologies to streamline the compliance process.

All of this converges to pose the very real risk that something gets missed by a stretched compliance team. In the [Accenture survey](#) of compliance leaders, nine out of ten forecast the costs of compliance operations to surge as much as 30% by 2024. But only six out of those ten expected to receive an increase to their budget.

Insufficiently resourcing compliance is a false economy. The costs of a regulatory fine, or the loss of trust and business associated with a poor reputation, will far outweigh any savings from cutting a compliance budget. The recent economic downturn and movement towards recession in many countries will force CEOs to take tough financial decisions. But they should think carefully before decreasing compliance budgets or headcounts. Effective due diligence can not only save them enormous fines and business interruption, but drive new and responsible profits.



Compliance executives are facing a dual challenge of needing to invest in people, processes and tools while evolving in an ever-increasing, cost-pressure environment. The cost equation is a growing challenge for the compliance function.”

– Accenture Compliance Risk Study 2022 Report.

HOW TO RESPOND

Checklist

How companies can survive—and thrive—in the new era of due diligence

The best way for companies to respond to the emerging challenges explored in this E-Book is to upgrade their compliance program by leveraging the best available data and technology to carry out risk-based due diligence on third parties. Here are ten areas to consider to help upgrade your approach:

1

Expand your data coverage

Legal and financial data are still necessary, but they are no longer sufficient for effective due diligence. Companies need to bring in data which surfaces ESG risks and opportunities. News data is particularly important for reputation risk management.

2

Embrace technology

An entirely manual due diligence process will not satisfy regulators' requirements that companies should carry out ongoing due diligence. Technology platforms allow you to upload large volumes of entities from an Excel spreadsheet and screen them immediately, then alert you to relevant changes in risk level over time. This leads to greater efficiency and accuracy.

3

Put compliance on the C-suite's agenda

A due diligence failure can be an existential threat to a company, while responsible profit can be a driver of long-term success. Compliance must not be ignored or sidelined, even (or especially) at a time of economic downturn. A company's leaders should take responsibility for promoting compliance, and set the right tone across the business.

4

Embed compliance across your business

Any changes to a company's business or strategy should build in due diligence from the start. For example, if you are planning to expand into a new continent, your compliance director should be alerted so they can prepare the right screening and systems to assess risk in these markets.

5

Work closely with your external due diligence provider

External platforms can distil high volumes of data and provide you with relevant insights. These insights can be even more targeted if you maintain an open dialogue with your provider to ensure their solution continues to meet your needs. If you share your ambitions for the service with them, they can help you with a tool that is flexible and scalable.

6

Set your objectives for compliance

You should clearly identify your aims from compliance—typically this will include mitigating regulatory, financial, reputational and strategic risk; and supporting responsible profit. This will help you to define your return on investment when you bring in due diligence technology.

7

Aggregate your data sources

The new era of due diligence means being on top of legal data, sanctions data, news data, ESG data, company data, and more. Searching through these sources individually is inefficient and time-consuming. You should bring them together in a solution—so that a single search pulls relevant information from all sources—or better yet, outsource to an external system which does that for you in one place, and updates the sources constantly.

8

Set expectations of suppliers

It's all very well ensuring your company is not directly involved in bribery, or ESG failures—but if wrongdoing is uncovered in one of your suppliers, you will still be reputationally (and often legally) liable. You should set clear ethical expectations of all third parties during onboarding and throughout the relationship, and scrutinize their due diligence processes so that you are confident in their ability to surface wrongdoing.

9

Beware greenwashing

Understanding ESG risk is made harder by the fact that many claims to ESG compliance have been shown to be false. You should approach ESG due diligence with a critical mind and an awareness of 'greenwashing', and don't just rely on claims in a company's annual report. Test these claims against external sources like news and social media data.

10

Prioritize data quality

Given the proliferation of data, and the frequency of misinformation, companies should only base due diligence decisions on reliable and authoritative data. Legal data, company data, sanctions and watch lists and PEP data should be drawn from official sources. While only the most reputable and licensed news outlets should be used.

Nexis® Solutions:

Helping organizations to step into the new era of due diligence with confidence

This report has explored the myriad factors which have raised companies' due diligence requirements in an increasingly complex regulatory environment—not to mention an increasingly complex world. In response, we have introduced a new and improved solution to help companies to retool and upgrade their compliance program in this new era of due diligence. Nexis Diligence+™ is setting a totally 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 company or individual and be assured the results cover all the bases. No other company can match the quantity and quality of our data, 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 50,000 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.

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

LexisNexis.com/DueDiligence | 1-888-466-3947

LexisNexis, Nexis and the Knowledge Burst logo are registered trademarks and Nexis Diligence+™ is a trademark of RELX Inc, used with permission. Other products or services may be trademarks or registered trademarks of their respective companies. © 2023 LexisNexis. All rights reserved. US-EDDM-Diligence-New-Era-of-Due-Diligence 0523

