INVESTIGATION · BUSINESS AND CORPORATE INVESTIGATION

Investigating Supplier and Third-Party Risk

Much of the risk an organisation faces comes from the suppliers, agents, distributors and contractors it works with. This article explains why third parties are a major source of legal, financial and reputational harm, and how organisations investigate them before and during the relationship.

ModQu research article · 2,788 words · 24 references (APA 7th edition)

Most organisations depend on other businesses. They buy materials and components, outsource manufacturing and logistics, engage agents and distributors to reach new markets, and rely on software providers and data processors to run their systems. Each of these relationships brings benefits, and each brings risk. A supplier may use forced labour, an agent may pay bribes, a distributor may sell to sanctioned buyers, and a software provider may give attackers a route into the organisation's network. When this happens, the organisation is often held responsible, by the law, by regulators and by the public, for conduct it did not directly commit.

Investigating third parties has therefore become a core part of corporate risk management. This article explains where third-party risk comes from, what the law expects, how organisations assess and investigate third parties before engaging them and while working with them, and the limits of the methods most commonly used.

Why third parties matter

Bribery through intermediaries

Third parties are the most common channel for bribery in international business. An analysis of foreign bribery cases concluded by member countries of the Organisation for Economic Co-operation and Development found that intermediaries, including agents, distributors, consultants and subsidiaries, were involved in about three quarters of cases (Organisation for Economic Co-operation and Development [OECD], 2014). Payments to intermediaries can be dressed up as commissions, consultancy fees or marketing expenses, with part of the money passed on to officials.

The law reflects this. In the United States, the Foreign Corrupt Practices Act prohibits payments to third parties made while knowing that all or part will be passed on as a bribe, and enforcement authorities treat deliberate ignorance of obvious warning signs as knowledge (U.S. Department of Justice & U.S. Securities and Exchange Commission, 2020). In the United Kingdom, the Bribery Act 2010 makes a commercial organisation liable for bribery committed by any person associated with it, including agents and contractors, unless it can show that it had adequate procedures to prevent bribery. Official guidance identifies due diligence on associated persons as one of the core principles of adequate procedures (Ministry of Justice, 2011). The settlement by Siemens with United States authorities in 2008, which followed findings that the company had paid hundreds of millions of dollars in bribes, much of it through consultants and intermediaries, remains one of the largest examples (U.S. Securities and Exchange Commission, 2008).

Human rights and forced labour

Supply chains for many goods pass through factories, farms and mines where labour standards are weak. The collapse of the Rana Plaza building in Bangladesh in 2013, which killed more than a thousand garment workers, drew attention to the gap between the standards claimed by global brands and conditions in the factories that supplied them. Governments have since introduced laws requiring companies to report on or investigate risks in their supply chains. The United Kingdom's Modern Slavery Act 2015 requires large businesses to publish an annual statement on the steps they have taken to ensure that slavery and human trafficking are not taking place in their supply chains. Canada's Fighting Against Forced Labour and Child Labour in Supply Chains Act (2023) imposes similar reporting duties. In the United States, the Uyghur Forced Labor Prevention Act (2021) creates a presumption that goods produced wholly or partly in the Xinjiang region of China were made with forced labour and are barred from import unless the importer can show otherwise.

The European Union has gone further. The Corporate Sustainability Due Diligence Directive (Directive (EU) 2024/1760, 2024) will require large companies to identify, prevent and address actual and potential adverse human rights and environmental impacts in their own operations and in their chains of activities. These laws build on international frameworks such as the United Nations Guiding Principles on Business and Human Rights (United Nations, 2011) and the OECD's guidance on due diligence for responsible business conduct (OECD, 2018), which describe due diligence as an ongoing process of identifying, preventing, mitigating and accounting for adverse impacts.

Product integrity and fraud

Third parties can also introduce fraud into the products an organisation sells. In 2013, tests in Ireland and the United Kingdom found horse meat in products labelled as beef, revealing long and opaque supply chains in which meat passed through several traders and countries. The government review that followed called for stronger testing, audit and intelligence-sharing across the food industry (Elliott, 2014). Food fraud, the deliberate substitution, addition or misrepresentation of food for economic gain, can also create risks to public health (Spink & Moyer, 2011).

Cyber and data risks

Suppliers with access to an organisation's systems or data create cyber risks. In the 2013 data breach at the United States retailer Target, attackers first stole credentials from a heating, ventilation and air conditioning contractor and used them to gain access to the company's network, eventually stealing payment card data for tens of millions of customers (U.S. Senate Committee on Commerce, Science, and Transportation, 2014). Guidance on cybersecurity supply chain risk management now treats supplier assessment as a standard part of security programmes (National Institute of Standards and Technology [NIST], 2022).

Operational disruption

Finally, third parties create operational risks. If a critical supplier fails, the organisation may be unable to operate. Hendricks and Singhal (2005) found that companies announcing supply chain disruptions experienced significant falls in share price and increases in share price volatility that persisted for long periods. Sheffi (2005) and Chopra and Sodhi (2004) describe how organisations can map dependencies and build resilience, which begins with knowing who their suppliers are and how they could fail.

Assessing risk across the supplier base

Large organisations may have tens of thousands of suppliers, and they cannot investigate every one in depth. The starting point is therefore a risk assessment that sorts third parties according to the risks they present and the importance of the relationship.

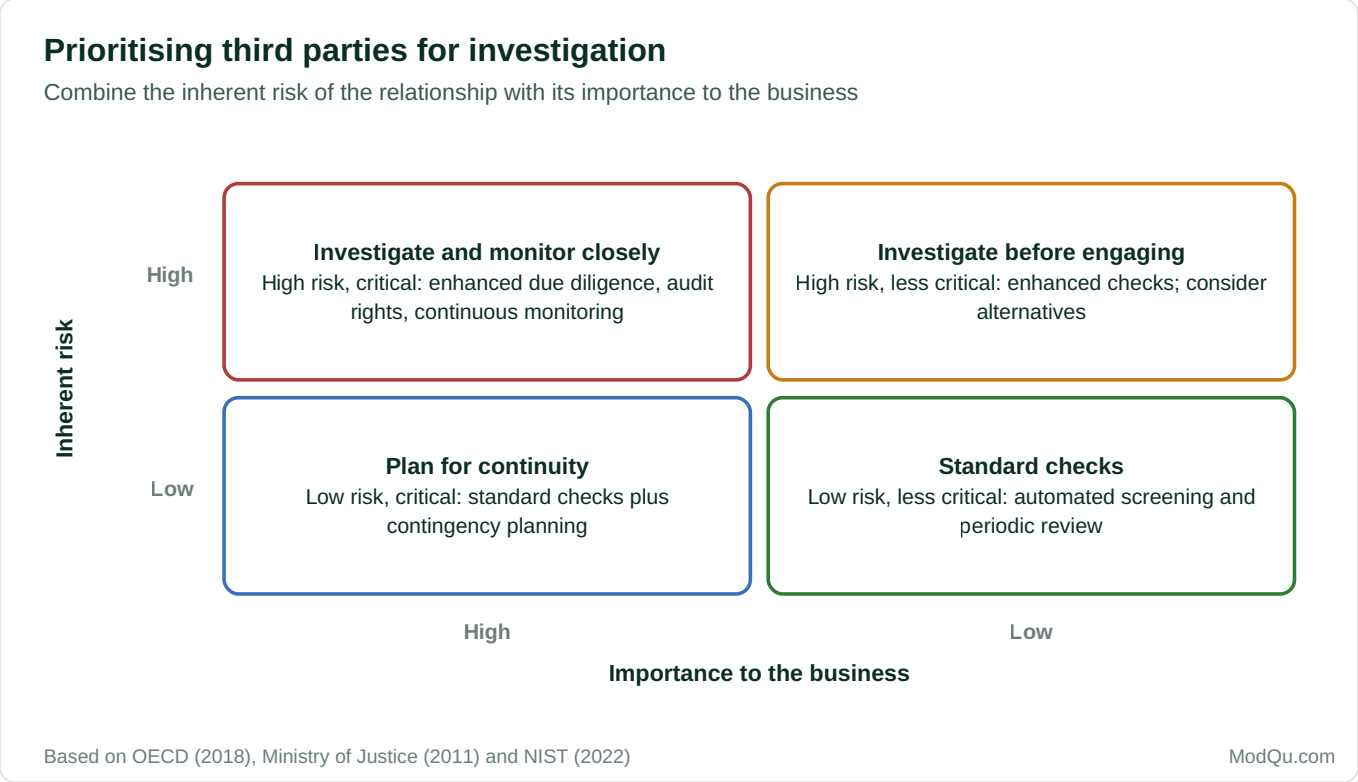


Figure 1. A simple way to decide how deeply to investigate each third party. Inherent risk depends on factors such as country, sector, the nature of the services and any interaction with public officials. Diagram by ModQu.

Inherent risk is assessed from factors such as:

- **Country.** Operations in countries with high perceived corruption, weak rule of law or known forced labour risks. Indices such as the Corruption Perceptions Index provide a starting point (Transparency International, 2024).
- **Sector.** Industries with known risks, such as extractives, construction, defence, garment manufacturing and agriculture.
- **Nature of the service.** Agents who deal with governments or obtain licences, permits or contracts on the organisation's behalf present much higher bribery risk than suppliers of office stationery.
- **Payment arrangements.** Success fees, unusually high commissions, payments to third countries or requests for cash are warning signs.
- **Access.** Suppliers with access to the organisation's systems, data or premises present cyber and security risks.

Investigating before engagement

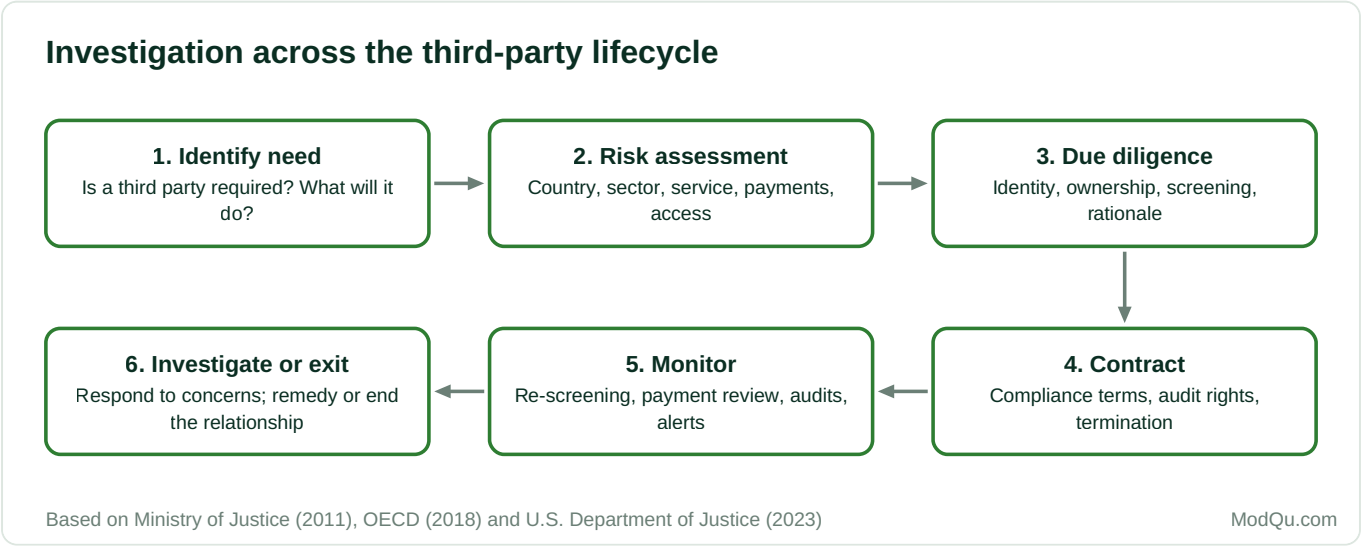


Figure 2. Investigation of a third party does not end when the contract is signed. Monitoring and the response to concerns are as important as the checks made before engagement. Diagram by ModQu.

Due diligence on a third party aims to establish who the party is, who owns and controls it, whether it is capable of doing what it says, and whether there are signs of risk. The depth of the inquiry depends on the risk assessment.

Identity and ownership

The first step is to establish that the third party exists and to identify its ultimate owners. Company registry records, financial statements and ownership documents are checked, and the third party is asked to declare its owners, directors and any links to public officials. Undisclosed ownership by an official, or by a relative of an official, is one of the most serious warning signs in bribery cases.

Screening

Third parties and their owners are screened against sanctions lists, lists of debarred contractors, enforcement records and politically exposed person databases. Media searches look for allegations of corruption, fraud, labour abuses, environmental harm or links to organised crime. As with any screening, name matches must be resolved carefully, and adverse media must be assessed for reliability: an unverified allegation in a single source is a lead, not a finding.

Questionnaires and interviews

Higher-risk third parties are asked to complete questionnaires about their business, ownership, compliance programmes and relationships with public officials. Their answers are tested against independent sources. For the highest-risk relationships, the organisation may interview the third party's management, request references from other clients and visit their premises.

Commercial rationale

One of the most useful questions is also one of the simplest: does the relationship make commercial sense? An agent with no relevant experience, no staff and no office, recommended by a government official and asking for a large success fee, does not make commercial sense, however clean the screening results. United States enforcement guidance specifically emphasises understanding the business rationale for using a third party and ensuring that payment terms are appropriate for the services provided (U.S. Department of Justice & U.S. Securities and Exchange Commission, 2020).

Contract terms

Due diligence findings feed into the contract. Contracts with higher-risk third parties typically include commitments to comply with anti-bribery and labour laws, rights for the organisation to audit books and records, obligations to report concerns, and rights to terminate if the third party breaches these commitments.

Sanctions and export controls

Sanctions add a further layer. Governments prohibit dealings with designated individuals, companies and, in some cases, whole countries or sectors, and many sanctions regimes extend to companies owned or controlled by designated persons even if those companies are not named on any list. Breaches can occur through third parties: a distributor may resell goods to a sanctioned buyer, or a supplier may be owned through intermediate companies by a designated person. Export control laws similarly restrict the transfer of certain goods, software and technology, and require exporters to understand who the end user is and how the goods will be used.

Investigating these risks means looking beyond the immediate counterparty. Investigators trace ownership through layers of companies to identify ultimate owners, compare shipping destinations and end-user declarations with what is known about the customer's business, and watch for warning signs such as requests to ship through third countries, reluctance to state the end use, or orders for products that do not fit the customer's stated activity. Because sanctions lists change frequently, often in response to international events, screening must be repeated, not performed only once.

Monitoring during the relationship

Due diligence at the start of a relationship provides a snapshot. Risks change: ownership changes, new allegations emerge, conditions in a factory deteriorate, or an agent's payment requests become unusual. Enforcement guidance expects organisations to monitor third parties throughout the relationship, not only at onboarding (U.S. Department of Justice, 2023; International Organization for Standardization [ISO], 2016).

Monitoring can include periodic re-screening, automated alerts for adverse media and sanctions changes, review of payments and invoices for unusual patterns, audit of the third party's books and records, and site visits. Payments deserve particular attention: requests to pay a different entity or a bank account in a third country, invoices with vague descriptions, and increases in commission without a corresponding change in services are all common warning signs.

The limits of supplier audits

Much supply chain due diligence relies on social audits, in which auditors visit factories to check working conditions against a code of conduct. Research has raised serious questions about how reliable these audits are. Locke (2013), studying the supply chains of several global brands over many years, found that private compliance programmes based on monitoring and audit produced limited and uneven improvements in working conditions, and that improvements were more likely where brands worked with suppliers to improve management systems and where local labour regulation was strong. LeBaron and Lister (2015) argue that the ethical audit system is structurally limited: audits are often announced in advance, short, paid for by the supplier or brand, and focused on documents that can be falsified, so that they can certify factories where abuses continue. LeBaron (2020) reports that forced labour persists in supply chains covered by audit and certification schemes.

The Rana Plaza building had been visited by social auditors before it collapsed, but structural safety was outside the scope of their checks. For investigators, the lesson is that an audit report is evidence of limited scope and reliability. It should be weighed alongside other sources, including worker interviews conducted away from management, grievance mechanisms that allow workers to report concerns safely, and independent information from trade unions, non-governmental organisations and journalists.

When something goes wrong

When a concern arises about a third party, the organisation must investigate it in much the same way as it would investigate internal misconduct. The investigation is usually harder, because the organisation has no direct authority over the third party's employees and limited access to its records. Audit rights in the contract become important, as does the organisation's leverage as a customer.

The investigation should establish what happened, whether the organisation's own employees knew or should have known, and whether the organisation's due diligence and monitoring were adequate. Enforcement authorities expect organisations to examine whether their controls failed and to remedy the failure, not simply to terminate the third party (U.S. Department of Justice, 2023). Where the concern involves harm to workers or communities, international guidance expects organisations to provide or cooperate in remedy for the people affected, rather than simply withdrawing from the relationship, which can leave workers worse off (United Nations, 2011; OECD, 2018).

Looking inward

Third-party investigations often reveal problems inside the organisation as well. A bribe paid through an agent usually requires someone inside the company to approve the agent, sign the contract and authorise the payments. A supplier using forced labour may have been chosen because purchasing staff were rewarded for cutting costs without regard to how the savings were achieved. An investigation that looks only at the third party, and not at the internal decisions that led to the relationship, will miss these causes and leave them in place. Investigators should therefore ask who proposed the relationship, who approved it, what warning signs were visible at the time, and whether incentives or pressures inside the organisation encouraged people to overlook them.

A short example

The following hypothetical case illustrates the process. A medical device company plans to enter a new market and is introduced to a local distributor by a hospital procurement official. The distributor would sell to public hospitals and receive a commission of 25 per cent, well above the 8 to 12 per cent the company pays elsewhere.

The compliance team classifies the relationship as high risk because the distributor will deal with public bodies, the country has a high perceived level of corruption and the commission is unusually high. Registry searches show that the distributor was formed eight months earlier, and its declared owner is a lawyer with no healthcare experience. A media search finds a local news report naming the lawyer's brother as the procurement official who made the introduction.

The company asks the distributor to explain its ownership and its proposed services. The answers are vague and the distributor declines to provide audited accounts. On this evidence, the company decides not to engage the distributor and records its reasons. It also reviews whether the procurement official's involvement should be reported to anyone, and looks for an alternative distributor through an open selection process.

Building a sound third-party investigation programme

The practices that distinguish effective third-party investigation programmes are consistent across bribery, human rights, cyber and operational risks:

1. **Know who your third parties are.** Maintain a complete and current inventory, including who owns them and what they do for you.
2. **Assess risk systematically.** Use consistent criteria to decide how deeply to investigate each relationship.
3. **Test the commercial rationale.** Ask why the relationship is needed and whether the terms make sense.
4. **Verify, do not just collect.** Test the third party's statements against independent sources.
5. **Monitor throughout the relationship.** Re-screen, review payments and act on alerts.
6. **Recognise the limits of audits.** Combine audits with worker voice, grievance mechanisms and external information.
7. **Investigate concerns properly.** Use audit rights, establish the facts and examine your own controls.
8. **Document decisions.** Record why each relationship was approved, conditioned or rejected.

Conclusion

Organisations cannot outsource responsibility along with their operations. Laws on bribery, forced labour, human rights, data protection and sanctions increasingly hold organisations to account for the conduct of the third parties they work with, and the public and investors do the same. Investigating third parties, before engaging them and throughout the relationship, is how organisations find out what they are exposed to. The most effective programmes match the depth of inquiry to the risk, test what they are told against independent evidence, and treat each warning sign as a question to be answered rather than a box to be ticked.

References

Bribery Act 2010, c. 23 (UK).

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53–61.

Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence. (2024). *Official Journal of the European Union, L 2024/1760*.

Elliott, C. (2014). *Elliott review into the integrity and assurance of food supply networks: Final report*. HM Government.

Fighting Against Forced Labour and Child Labour in Supply Chains Act, S.C. 2023, c. 9 (Canada).

Hendricks, K. B., & Singhal, V. R. (2005). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management, 14*(1), 35–52. https://doi.org/10.1111/j.1937-5956.2005.tb00008.x

International Organization for Standardization. (2016). *Anti-bribery management systems — Requirements with guidance for use* (ISO Standard No. 37001:2016).

LeBaron, G. (2020). *Combatting modern slavery: Why labour governance is failing and what we can do about it*. Polity.

LeBaron, G., & Lister, J. (2015). Benchmarking global supply chains: The power of the 'ethical audit' regime. *Review of International Studies, 41*(5), 905–924. https://doi.org/10.1017/S0260210515000388

Locke, R. M. (2013). *The promise and limits of private power: Promoting labor standards in a global economy*. Cambridge University Press.

Ministry of Justice. (2011). *The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing*.

Modern Slavery Act 2015, c. 30 (UK).

National Institute of Standards and Technology. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161r1). https://doi.org/10.6028/NIST.SP.800-161r1

Organisation for Economic Co-operation and Development. (2018). *OECD due diligence guidance for responsible business conduct*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2014). *OECD foreign bribery report: An analysis of the crime of bribery of foreign public officials*. OECD Publishing. https://doi.org/10.1787/9789264226616-en

Sheffi, Y. (2005). *The resilient enterprise: Overcoming vulnerability for competitive advantage*. MIT Press.

Spink, J., & Moyer, D. C. (2011). Defining the public health threat of food fraud. *Journal of Food Science, 76*(9), R157–R163. https://doi.org/10.1111/j.1750-3841.2011.02417.x

Transparency International. (2024). *Corruption perceptions index 2023*.

United Nations. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. Office of the United Nations High Commissioner for Human Rights.

U.S. Department of Justice. (2023). *Evaluation of corporate compliance programs*. Criminal Division.

U.S. Department of Justice, & U.S. Securities and Exchange Commission. (2020). *A resource guide to the U.S. Foreign Corrupt Practices Act* (2nd ed.).

U.S. Securities and Exchange Commission. (2008, December 15). *SEC charges Siemens AG for engaging in worldwide bribery* [Press release 2008-294].

U.S. Senate Committee on Commerce, Science, and Transportation. (2014). *A "kill chain" analysis of the 2013 Target data breach* [Majority staff report].

Uyghur Forced Labor Prevention Act, Pub. L. No. 117-78, 135 Stat. 1525 (2021).