REPRINT

risk & compliance

THIRD PARTY RISK MANAGEMENT IN SUPPLY CHAIN SECURITY

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2024 ISSUE

risk & compliance
APR-JUN 2024
www.riskandcompliancemagazine.com
Inside this issue:
FEATURE
Going global: navigating internationalisation
EXPERT FORUM
Managing and mitigating anti-cartel risk
HOT TOPIC
Conducting an effective and efficient internal investigation

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

THIRD PARTY RISK MANAGEMENT IN SUPPLY CHAIN SECURITY

PANEL EXPERTS

Corey Dunbar
Partner & Data Forensics Practice Leader
BDO
T: +1 (732) 621 5082
E: cdunbar@bdo.com

Corey Dunbar is a principal in the forensics practice and leader of data forensics at BDO. He specialises in data analytics pertaining to the detection of fraud, bribery, corruption, compliance risks and other forms of nefarious activity occurring within accounting, financial and communicational data. He also specialises in the operations and technology enablement of compliance programmes. With significant experience working with global companies in heavily regulated industries, he is often engaged to assist with designing, developing and implementing compliance monitoring solutions and platforms.

Adam Turteltaub
Chief Engagement & Strategy Officer
Society of Corporate Compliance and Ethics
& Health Care Compliance Association
T: +1 (952) 405 7922
E: adam.turteltaub@corporatecompliance.org

Adam Turteltaub is the chief engagement and strategy officer for the Society of Corporate Compliance and Ethics & Health Care Compliance Association. He joined SCCE & HCCA in 2008 with more than seven years of experience working with ethics and compliance professionals. He is a regular speaker at SCCE & HCCA events. He has also spoken at conferences of the Institute of Internal Auditors, the International Association of Privacy Professionals and the Association of Certified Fraud Examiners. He also hosts the Compliance Perspectives podcast, which spotlights current issues in compliance.

James MacDonnell
Principal
BDO
T: +1 (703) 245 0382
E: jmacdonnell@bdo.com

James MacDonnell is a risk management, business continuity and crisis management professional with over 20 years of experience helping clients prepare for and respond to crises and emerging risks. He has designed enterprise risk management, business continuity, disaster recovery, vendor risk and crisis management programmes in support of non-profit, commercial, national security and military clients. He also has experience providing crisis response support during real world events across multiple threat vectors including cyber attacks, product recall, extortion, workplace violence, natural disasters and corporate misconduct events.

R&C: Could you provide an overview of the key risks facing today's supply chains? To what extent are companies exposed to vulnerabilities arising from their third-party relationships?

Turteltaub: While to most organisations, outside suppliers are thought of as outside suppliers, to enforcement authorities, regulators, the public and investors they are seen as extensions of your organisation. Often from a legal and reputational risk perspective, anything your supply chain does on your behalf can have negative impacts on your organisation. For that reason, it is essential that organisations have a thorough understanding of not just who their suppliers are, but also how they operate and the risks they pose to their organisation.

Dunbar: Many businesses are focused on 'high profile' supply chain risks, such as geopolitical conflict. But the risks vendors may present to a business are highly contingent on the nature of goods and services provided, the business relationship and the brand of the purchasing party. Companies may also struggle to evaluate the risk presented by the extended supply chain. A supply chain risk management programme should address a series of simple questions. First, can suppliers consistently meet demand? Second, are the data, goods or services properly protected and managed? Third, do suppliers have appropriate controls to ensure sufficient quality? Fourth, are suppliers financially viable with an effective governance structure? Fifth, do suppliers meet all applicable local, federal and international regulations? Sixth, will a relationship with the supplier reflect poorly on our brand or reputation? And lastly, do suppliers meet green standards that align with expectations and industry standards?

R&C: Drilling down, what specific types of third-party risks are common throughout global supply chains?

MacDonnell: Global risks to the supply chain vary significantly depending on a company's industry and operating model. Some of the most pressing concerns to global supply chains are geopolitical risks, greenwashing and other environmental, social and governance (ESG) considerations, compliance with global regulations, risks to intellectual property, reliability of international infrastructure such as water or energy supplies, and the volatility of global transportation. As we have seen over the last several years, the materialisation of some of these risks can have cascading impacts into other areas. For example, geopolitical issues such as the conflicts in Ukraine or Israel can cause a series of sanctions or tariffs that can disrupt the global flow of money, goods and information.

Turteltaub: The list of risks is growing greatly. A few years ago, the conversation would have focused almost exclusively on anticorruption risks. Today, it includes human rights issues such as modern slavery and human trafficking, sustainability issues, data privacy, conflict minerals and economic sanctions. The list is large and continuing to grow both in depth and complexity. Standards keep rising and, notably, the number of countries with laws in these areas is also rising. As a result, we are seeing more and more issues that once were the purview of ESG or corporate social responsibility becoming actual compliance requirements.

R&C: In your opinion, how adept are companies at vetting their third parties and carrying out ongoing due diligence to monitor risk?

Turteltaub: Great progress has been made in vetting third parties and carrying out due diligence, but there still is a long way to go. A variety of challenges are facing organisations. For those that had not done much in the way of third-party vetting in the past, the road is obviously a long one. They must establish a programme and understand how it fits within their procurement operations. Companies that have been doing this for some time are in a much better place, not surprisingly, and many can rely upon well-established programmes for meeting their due diligence requirements. But two gaps remain. First, companies are better at initial due diligence than they are at ongoing auditing and monitoring. Some of that reflects old habits. Some may reflect suppliers' unwillingness to submit to ongoing audits of their operations. The second great challenge relates to rising expectations of the public and governments. If you had a good third party or supplier management programme three years ago and have not updated it, chances are you are not addressing some of the newer risk areas.

> "If you had a good third party or supplier management programme three years ago and have not updated it, chances are you are not addressing some of the newer risk areas."
>
> *Adam Turteltaub,*
> *Society of Corporate Compliance and Ethics & Health Care Compliance Association*

Dunbar: One consistent trend we have seen is a heavy reliance on vetting third parties at the onset of a relationship to understand their risk profile. All too often, these same risk mitigation processes are repeated after the onboarding process, once the relationship is underway. But it is not enough to recertify your diligence on a three-year cycle or simply scan third-party databases for risk signals. Companies should monitor their ongoing relationships with third-party suppliers by leveraging the supplier's own internal data. Similarly, we often see clients manage risk in silos. Third parties may appear to have manageable risk in isolation. However, when operational resiliency risk is overlayed with compliance and legal risk, companies may find that their risk appetite decreases and their approach to managing resilience requires more intervention.

R&C: How should companies go about implementing a third party risk management (TPRM) programme to highlight and reduce their exposures? What are the essential areas to address?

MacDonnell: Companies should design their risk management programmes based on the outcomes of a risk assessment. It sounds obvious, but it is surprising how often there is a rush to implement downstream controls without adequately evaluating risk exposure at the outset. This can lead to sunk investments in areas where risk is perceived to be high but in retrospect was manageable. We recommend quantifying risk exposure by leveraging available data rather than relying solely on market trends or industry markers. Similarly, we advocate removing laborious and time-consuming processes from the workflow. Using technology platforms to streamline third party risk management (TPRM) offers great efficiencies. Documenting risk decisions, observational data and compliance outcomes offers organisations a treasure trove of data to measure perceived risk versus actual risk. It is increasingly

> **"As generative AI takes root in the workplace, companies should be vigilant about its use, especially when relying on third parties."**
>
> *James MacDonnell, BDO*

challenging to do so without an underlying technology platform to document these outcomes and streamline the review pathways.

Turteltaub: The compliance team and business unit must work in partnership to address the full lifecycle of the supplier relationship. That means working together to understand not just the opportunity of using the third party, but also the risks that come with it. With those risks identified, it is important to have a thorough review of the third party's business practices to ensure that they are compliant, ethical and do not create unnecessary risks. Onboarding must emphasise your organisation's expectations of suppliers so that the new third party both understands your expectations and realises that you take them seriously. Finally, on an ongoing basis, there is the need to audit and monitor, and, from the start, your third parties need to be made aware that you expect that ongoing visibility into their business.

R&C: What are some of the common challenges companies can expect to face when implementing and maintaining a TPRM system for their supply chain? What advice would you offer on overcoming these challenges?

Turteltaub: One of the greatest challenges they are likely to face is pushback from suppliers that are uncomfortable with ongoing due diligence. It is understandable that companies may resist ongoing scrutiny. A customer is a customer and not an investor, after all. But a buyer cannot take 'no' for an answer if it is sourcing in a high-risk area. At the same time, companies need to recognise that one size does not fit all. The scrutiny of a vendor sourcing from a high-risk country is going to be very different than, say, one of the top cloud services providers.

> "As the world grows increasingly complex, divisive and disjointed, organisations must pay closer attention to third-party relationships, particularly as they relate to supply chains."
>
> *Corey Dunbar, BDO*

Dunbar: An effective TPRM system includes stakeholders from many different parts of the organisation. Thus, designing an effective process to plan procurement, select vendors, monitor contracts and offboard vendors with a diverse set of stakeholders can be challenging. In addition, aligning stakeholders on a risk-mitigation strategy for specific suppliers or services can be challenging. Often, the correct solution requires a more comprehensive perspective that integrates more risk mitigation measures than any single functional area can offer. Also an issue is leveraging different software applications for different components of TPRM, particularly if the applications do not speak to each other. This can lead to key aspects such as supplier performance not being collected at all. Procuring a software system before assessing overall need can leave significant gaps in the TPRM programme.

R&C: In what ways can technology assist with TPRM? How are innovative solutions being deployed and applied?

MacDonnell: Technology is the backbone of an effective TPRM programme. Software platforms can help generate onboarding questionnaires for third-party suppliers, facilitate review pathways between compliance, legal and other departments when assessing risk, and provide a reliable inventory by monitoring usage through data analytics and operational reporting. Among other things, technology is useful for tracking observational data like sales key performance indicators, usage and audit findings, as well as compliance and remediation items. New technologies can create new risks, too. As generative AI takes root in the workplace, companies should be vigilant about its use, especially when relying on third parties.

Turteltaub: Technology already plays an enormous part in TRPM. A number of vendors now offer the ability to conduct desktop inquiries into potential suppliers on an enormous range of measures. Tools have emerged to help organisations stay on top of changing legal and regulatory changes that can affect the relationship. But, as good as they are, there is still often a need to visit the vendor, actually see its plant or offices, and ensure that what looks good on paper smells good in real life.

R&C: What is the outlook for third-party relationships across supply chains? In your opinion, will the associated risks only intensify going forward?

Turteltaub: TPRM is only going to get more complex. These are turbulent times, with the public demanding greater accountability from business and legislators keenly attuned to them. Expanding global instability increases the risks of corruption and the need for companies to look for new suppliers, many of which are likely untested or from parts of the world with different standards. Successful companies will recognise this reality and work to create an approach that makes managing the risk an integral part of how they do business with their suppliers.

Dunbar: As the world grows increasingly complex, divisive and disjointed, organisations must pay closer attention to third-party relationships, particularly as they relate to supply chains. In recent times we have seen how geopolitical conflicts and climate events can combine to create unprecedented disruption, while cyber attacks continue to increase year on year. Increased regulatory activity and scrutiny – everything from the Uyghur Forced Labor Prevention Act in the US to Greenhouse Protocol in the European Union – can impact an organisation's bottom line. if the risks posed by third parties are not adequately assessed, there is no question that third-party risks will intensify in the future. The question is whether organisations are preparing for them now.