COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2021
Knowing when your firm should take action against third-party risk

By Allan Matheson

Allan Matheson (allan@blueumbrella.com) is the CEO of Blue Umbrella in Vancouver, British Columbia, Canada.

Typically, working with higher-risk third parties can creep up on a company that is either high growth or in a more regulated industry. For instance, bribery and corruption risk can easily find its way into technology or life sciences organizations as they evolve globally. As these companies grow, the sales side of the organization will look to different models to get their product to market, specifically working with agents, distributors, and channel partners to help push more product. Typically, the sales side will consult with legal on matters they are well versed in, like commercial risks and legal contracting issues. However, when they lift their heads, they will find that many of these relationships put them at a very high risk of corruption and bribery, and it is usually left to an enterprising general counsel who understands both the risks and how the new model is being pushed into new markets to help protect the organization.

In the earlier part of their growth stories, most companies essentially wing it when it comes to managing the compliance risks inherent in their third-party vendors and agents. Their compliance processes tend to be inconsistent and diffuse, lacking tools that give their leadership true visibility into the landscape of risks faced by the company.

And that can work just fine…until it doesn't. When a company's revenue grows past about $50 million, the increasing complexity of its third-party universe starts to make that sort of ad hoc system unsustainable. It's this critical mid-market period that is the most challenging for companies. Those with revenue above $1 billion mostly have systematic compliance solutions in place, while the third-party ecosystems of companies under $50 million generally haven't reached critical size or complexity.

A survey we conducted last year of more than 230 compliance professionals at medium-sized firms found that many of these companies still use the equivalent of duct tape and a few blunt tools to manage their third-party risks.[1] Compliance processes tend to be patchy, with companies using an average of 3.6 different tools, such as emails, questionnaires, and response tracking.

How can mid-sized companies like these know when it's worth investing in a more systematic solution to manage third-party compliance?

There's no one-size-fits-all answer to that question, though size is certainly one factor. The $200–$600 million range is where companies will inevitably start to realize they have a problem as their old ways of managing risk start to buckle under the growing volume and complexity of external relationships.

Time to face the risks

But the reckoning may come sooner, like when the CEO or board requests a more systematic approach to compliance. Or it may bubble up from within as staff become overwhelmed by the number, complexity, or risk levels of relationships with external vendors and sales agents. In the worst-case scenario, it happens when a company gets hit by a compliance-related crisis, creating urgent pressure to implement a new system of

controls.

And much depends on the industry and the kind of global footprint a company has. One compliance fault line runs through the company's exposure to foreign partners. Another crack is widened by the risk level of the industries these firms serve. A tech company relying on hundreds of reseller agents in Asia, for example, would have a bigger, earlier need for a sophisticated compliance system than a company whose customers and suppliers are mostly from the US.

The exact type of risk varies widely. Bribery and corruption risks will be prominent for firms with big sales distribution networks outside the US. Data privacy risks will be a top concern for companies with partners that hold information about their customers. Information technology security should be a priority for companies with third-party partners that have access to their data or systems.

The unfortunate general counsel

When companies finally get serious about putting new controls in place, it often falls to the unfortunate general counsel to spearhead the efforts. Unfortunate because the first thing general counsels learn is how hard it is to get a grip on the company's real third-party risks. Different departments, subsidiaries, and individuals often keep their own lists of vendors and agents, making a single source of truth on third parties hard to come by.

For example, here's how a company can suddenly find itself exposed. Imagine a life sciences company looking to grow globally. This firm's sales side will naturally look to work with non-US agents, distributors, and channel partners to get its product to market.

Though sales will consult with legal on matters such as commercial risks and legal contracting issues, they may not be aware of how many of these relationships put the company at high risk of corruption and bribery. A sales software tool may help, but it can also add to the confusion, because the data it contains can be inaccurate. Company names are often entered incorrectly or inconsistently, making it hard to know whom you're actually dealing with. A salesperson, for example, might enter the name of a partner company as they know it, which may be very different from its formal, legal corporate identity.

Getting a grip on the full spectrum of compliance risks quickly leads to mid-sized firms being overwhelmed. After all, a general counsel might have only a small team already burdened with other responsibilities.

No more fat checks

A common knee-jerk reaction is to write a fat check to a law firm that offers consultancy services on managing compliance risk. But the truth is that getting a handle on your third parties doesn't have to be as difficult or expensive as most businesses assume. It can be handled in a way that won't interrupt operations and will allow you to sleep at night without worrying about breaking the budget.

The trick: take a risk-based approach to third parties, focusing on the parts of your ecosystem that are most likely to create problems. If you can set up effective, ongoing controls around third parties, you've already gone a long way to matching the systems that Fortune 500 companies have in place. Most mid-market companies won't need the level of sophistication that the biggest firms have. A Fortune 500 firm might have an ecosystem of more than 10,000 third parties, requiring a much different level of nuance than a mid-sized firm with just a few hundred.

Start laying the groundwork

Unfortunately, it's common for mid-sized organizations to lack risk-mitigation programs, leaving these

companies open to data privacy lapses or even bribery and corruption risks. Once the crisis has occurred, it's too late to implement a system of controls.

There is some good news, however. Getting 90% of the way there is likely to be good enough for most medium-sized firms, and that can be achieved in a pretty painless, cheap, and templated way. The information you need is out there. It's just a case of finding it and developing workflows around it that enable you to manage the risks efficiently.

Takeaways

- Addressing the full spectrum of compliance risk may be daunting, but it can be managed without interrupting operations or breaking the budget.
- To mitigate risk, leaders should focus on the parts of their business ecosystems that are most likely to create problems.
- The type of risk varies widely. Bribery and corruption risks will be prominent for firms with big sales distribution networks outside the US.
- Data privacy risks are a top concern for companies with partners who hold information about their customers.
- Often general counsel teams are tapped to spearhead compliance efforts, but general counsels fall short because they generally aren't equipped for the complexity.

1 Quadra Research and Blue Umbrella, "Quantitative Study Among Compliance Professionals in the U.S.," June 2019.