blue umbrella
making business better

Learn Five Third-Party Compliance Lessons From Fortune 500 Companies

Introduction

Over the last decade, we have had the pleasure of working with and supporting some of the biggest and most sophisticated third-party compliance programs on the planet. While we do consider these bragging rights to show our expertise, we also understand that not every company has the resources, program complexity or needs of some of the biggest global brands. Working with Fortune 500 clients has given us major insights into what best practices mid-size companies can take away and apply to their own programs and teams. We see firsthand what these companies are asking of their clients and partners, who are typically smaller and less compliance-sophisticated organizations. Overall, here are 5 important lessons we would like to share from working with Fortune 500 companies.

Lesson #1: Race to the Middle

The guidance from the US Department of Justice (DOJ) is for organizations to adopt a risk-based approach and do what is *appropriate* to identify and manage risk with third parties. The government falls short of providing specific guidelines and, as a result, companies are left to determine exactly what they should do. Although it can be frustrating to try to conceive of, adopt and implement a program from scratch without much guidance, each company has its own understanding of the risks inherit in its external relationships.

A good rule of thumb is that if you have more than 250 important external relationships, a technology enabled third-party compliance solution is a good idea to implement. Not sure where to get started with choosing a third-party compliance platform? Check out our white paper on the topic. This will allow you to evaluate third-party relationships around your own organization's risk parameters and then to apply different levels of on boarding, diligence and monitoring to ensure that your budget is spent in accordance with the risk presented.

Lesson #2: Right-Size Your Program

We have worked with large organizations who have ample internal resources and sophistication to manage their third-party compliance program and interact with their tens of thousands of third parties. Honestly, what works for them is probably not going to work for you. They tend to utilize advanced workflow workflow automation, taking into account several (or sometimes dozens) of criteria to allocate and assess risk profiles. What is important, however, is to take a close look at what resources you do have internally and then determine what is manageable and appropriate for your company. Consider:

- How big is your company? How many active third-party relationships do you have?
- Do you have internal resources dedicated (even partially) to compliance, vendor onboarding or managing third-party risk?
- Who oversees these risks? (Hint: If it is everybody, it is nobody).
- What budget do you have to manage this process?

Understanding the questions above as they apply to your company will help you determine how to develop and manage your third-party compliance and risk management program. Program design does not need to be complicated. In working with Fortune 500 companies, we have observed that the majority of program can be condensed to a number of key, easy to implement steps as outlined in our How to Launch a Third-Party Risk Management Program checklist. Preparing adequately before beginning will help to avoid building something that isn't manageable on an ongoing basis or, on the other hand, underestimate the size and scope of your program and not allocate resources accurately.

Lesson #3: No Need to Reinvent the Wheel

Fortune 500 companies have far more resources to dedicate to each area of compliance. Mid-size companies, on the other hand, typically have an individual in an in-house counsel role who, among literally dozens of other things, is tasked with determining the best approach to third-party risk management. These risks can include multiple compliance subjects, including anti-bribery and corruption, data privacy, IT security and more. As a result, many companies spin their wheels trying to determine what specific questions to ask their business partners, sometimes relying on outside counsel to develop questionnaires. This can take a lot of time and money.

Most specialized risk management questionnaires cover standard questions. We know this because we have literally seen them all! This means you probably want to know the same things about your business partners that Fortune 500 companies also want to know. There is no need to reinvent the wheel when it comes to developing questionnaires. There are affordable solutions in place that allow you to access and distribute gold standard risk assessment questionnaires. It is worth exploring these out of the box solutions before you spend valuable internal time and resources to build your own wheel, so to speak. (It just so happens we built one of these systems! It's called Blue Umbrella GRC.)

Lesson #4 – Target Due Diligence Spending & Follow-up

The basis of most third-party compliance programs involves the combination of risk assessment questionnaires and due diligence reports. Many mid-size companies don't regularly order due diligence reports and, as a result, may not know when one is advisable or how to interpret the data they find in one. The importance of identifying risks using a standardized questionnaire will allow you to determine when a due diligence report may be necessary to get a clearer picture of the risks associated with a third-party relationship. Many due diligence report providers offer different scopes and depth of analysis in their report offerings. Getting a clear picture of what is covered in each level of report will help you determine what level of report will be the best investment depending on the risk identified with the third party or how critical they are to your business operations.

Once an approach to the acquisition of diligence has been formulated, the next important step is to track remediation. Just because a third party presents a risk does not mean that you cannot necessarily do business with them. For instance, if a third party was previously indicted for a bribery offense, it is a major cause for concern. However, diligence may reveal that the offence was years before and resulted in the company implementing a world-class anti-bribery and corruption compliance program. In this case, identifying the risk is useful, but remediation, and accurately documenting that remediation (in this case by asking for program documentation), are key. On the other hand, some diligence will prove that the third party is extremely high risk and measures should be made to cut ties. Learn more about Blue Umbrella's due diligence research services here.

Lesson #5 – Recertification: The Importance of "Rinse and Repeat"

Most sophisticated third-party compliance programs at Fortune 500 companies involve some element of recertification. This means, in practice, that they will automate the distribution of a questionnaire or repeat a due diligence report on a

Most sophisticated third-party compliance programs at Fortune 500 companies involve some element of recertification. This means, in practice, that they will automate the distribution of a questionnaire or repeat a due diligence report on a given schedule (be it annually or every two to three years). The premise here is that even though a vendor, distributor or agent may be "squeaky clean" at one moment in time, it's critical to regularly evaluate their practices and if anything in their risk universe has changed. Now, for those of us who don't work at Fortune 500 companies, adding recertification as an aspect of your program may involve setting a calendar reminder for a year after you receive a completed questionnaire or putting in this diligence process at the time of contract renewal. If you're considering investing in a technology to help manage these interactions with third parties, it's important to look at what features they have to automatically repeat these activities on a scheduled cadence or implement a system of reminders to do so.

Summary: It's Easier Than You Think to Have a Program Like the Big 500

Our expertise in working with some of the biggest companies on the planet has given us insights into what best practices are easily transferable to smaller teams with less dedicated resources to manage third-party risk. The key is to consider the lessons we have described above and understand how technology can play a role in helping you streamline your processes in alignment with best practices. Taking the time to critically assess your company's needs and allocate the right resources will help everyone sleep better at night and know that your third-party risk program is in great shape. We would be more than happy to help along the way! Talk to us.

Is it time to consider upgrading your third-party compliance technology? Learn more about what we offer.

Blue Umbrella's Third-Party Compliance Technology Platforms

Status

- For companies with thousands to tens of thousands of third parties
- Due diligence reports and their flagged results populate automatically to the dashboard
- Unlimited options for custom workflows and automation to reduce manual burden

Learn more about Status

Blue Umbrella GRC

- Modular, plug and play software built specifically for mid-size companies
- Includes risk assessment modules for anti-bribery and corruption, data privacy, CCPA and IT security
- Offers a right-sized compliance screening and monitoring solution

Learn more about Blue Umbrella GRC