

## Step-by-Step Guide: How to Launch a Third-Party Risk Management Program

You are probably one of the many hardworking professionals at mid-size organizations who are unsure of how to get started with building a program to manage third-party risk. Lucky for you, we built this handy checklist to help guide your important internal conversations and activities around where to begin.

Steps	Approach	Next steps? Done?
<b>Step 1:</b>  <b>Pick a compliance area of concern.</b>	<p>Generally, if you are reading this, you have an area in mind already. Many companies will focus on the most immediate risk to the business, typically starting with data privacy, bribery or corruption, sanctions compliance or IT security. To launch a meaningful compliance program within budget, it is advisable to start with one area before trying to implement across multiple compliance subjects.</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>
<b>Step 2:</b>  <b>Get a list of your third-party vendors.</b>	<p>This can be a pain point for some companies as sometimes there is no centralized list of agents, distributors, channel partners and vendors. Each of these will have varying risk profiles with regards to each different risk. For instance, a vendor of a payroll system has significantly higher IT security risks than does a sales agent in China. The inverse is true when considering bribery and corruption risk. Retrieving this data may be complicated depending if you have a more centralized or decentralized compliance program.</p> <p>Make sure that your list includes all third parties as well as relevant data required to contact them and assess the relationship. Some key fields to collect would be; name, address, country of operations, countries served, industry, nature of relationship, contact person, contact email, internal contact person.</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>

<p><b>Step 3:</b></p> <p><b>Identify relevant third parties.</b></p>	<p>This is where it starts to get tricky. Depending on how rich your data fields are in your list of third parties, you should be able to identify which populations should be covered by your different compliance areas. For example, there may be a data privacy risk with a payroll provider, but there may be a lower risk with a manufacturing relationship. Usually this is accomplished with a broad stroke as identifying who may present a vulnerability is enough of a threshold at this point. The idea here is not to conduct a risk assessment, it is merely to identify who may have risk vs. who has virtually no risk at all. There is no point sending a parts manufacturer through a data privacy process if they don't have access to your data.</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>
<p><b>Step 4 [Optional]:</b></p> <p><b>Conduct an internal review of the third party.</b></p>	<p>Sometimes an organization will first identify which third parties are active, adding value and should be evaluated before beginning the process. This would involve collecting information about the third party from those responsible for setting up and maintaining these relationships. For example, if a sales agent is being used in Vietnam, before engaging that agent in a compliance process, it may be pertinent to ask your head of sales for Asia or your finance department whether this agent is being used - and if so, how much and would they like to retain the relationship? More times than not, this step can shrink the total size of the third-party ecosystem by 20%-30%.</p> <p>A drawback is that it involves active participation of other parts of the company. That participation is not always well-received or reciprocated with vigor. (Basically, some people just won't help much...)</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>
<p><b>Step 5:</b></p> <p><b>Send questionnaire to relevant third parties.</b></p>	<p>Typically, a questionnaire process enables you to decide more accurately who is a risk for your organization and who is not. Crafting a questionnaire that is relevant to your own company risk profile is a service that many law firms and the 'Big 4' will be happy to charge you for... <i>ahem</i>, we mean provide. That said, as an organization that has seen hundreds, maybe thousands, of such custom-made questionnaires in the field, they do not vary greatly. So long as relevant questions are being asked, spending less time on the precise wording and more time on the results is highly recommended.</p> <p>To that point, ensure that your questionnaire is written clearly, succinctly and is in a machine-readable format. A free text answer that takes 30 seconds to read and is sent to 1,000 third parties will take <b>8 hrs. and 20 minutes just</b> to read all the responses. That doesn't even include making sense of it all and remediating where required. This is where pain of the process creeps in and swallows your time.</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>

<p><b>Step 6:</b></p> <p><b>Identify risks.</b></p>	<p>Crafting an approach to the answers is generally straightforward. If a foreign sales agent says they are in fact selling to government authorities on your behalf, that is a bribery risk.</p> <p>However, when you have many questions being answered across many third parties, using a technology to scan these responses and understand where your risks lie (and the magnitude of each of those risks) can save an enormous amount of administrative effort and prevent errors.</p>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>
<p><b>Step 7:</b></p> <p><b>Remediate.</b></p>	<p>Once you have identified where risks exist, you must do something to address them. Sometimes this is obvious. For example, if the risk is very large and your relationship is very small, it may be prudent and easiest to simply end the relationship.</p> <p>However, most remediation action is more nuanced. This is where you have quite a few different options: research further, involve frontline colleagues, change contract language, interact with the third party directly to get comfort, provide understanding of your expectations on this area of compliance to the third party.</p> <p>Most important at this stage is to ensure that you have provided some action for the various exposed risks. The kinds of risks presented are too numerous to identify and communicate within this checklist, if at all. Often, some type of remediation framework helps.</p> <p>For example, walking through the below:</p> <ul style="list-style-type: none"> <li>• What is the problem? Further research may be required to fully understand this, but an assessment should be made as to what precise risk this issue poses to your organization.</li> <li>• Who is responsible for managing this risk within your organization?</li> <li>• What should the end state look like? How can we reach a level of comfort that this risk has been addressed?</li> <li>• What are the steps needed to get there?</li> <li>• Track/document the steps and progress of achieving the steps.</li> <li>• Recertify and potentially monitor the third party every year to ensure that they continue to be compliant.</li> </ul>	<p>Action:</p> <p>Responsible:</p> <p>Target date for completion:</p>



Step 10:		
Monitor the relationship.	Wasn't that fun!?!? Now that you have a full third-party compliance program in place, it has already expired. Darn! Just because a third party with a high risk of data privacy leakage is OK today, doesn't mean they won't have a massive data breach tomorrow. For high-risk parties, some type of monitoring (against databases) and recertification process is prudent.	Action:  Responsible:  Target date for completion:
Step 11:		
Wash and repeat.	Once the above steps have been completed, a couple of key steps should be employed. First, take a bit of time and speak to your team about what went well and which steps could be improved. One take-away that is frequently observed is that the amount of administration in a program like this can be notable. The fact remains that when we spend time sending emails, following up questionnaire completion requests, reading responses to identify flags and manually remediating and documenting all of the above, we are getting away from the parts of the process where we add the most value. One solution to this problem is to <b>USE TECHNOLOGY</b> . <i>Blue Umbrella</i> has an affordable, modularized GRC technology that can help you manage many different facets of your compliance program. Have a quick look at a video to show how our product can manage the entire above process for you. Data Privacy, Data Security, Anti-Bribery and Corruption.	Action:  Responsible:  Target date for completion:

## In Conclusion...

Once step 11 is completed and we understand how the process can be improved, it is time to begin thinking about what other compliance issues would be worth managing through the same process. Part of the complication arises when trying to overlap these risks to get a true view of the third-party risk. Again, technology can help. When you began this checklist, did you ever imagine that a vendor of third-party compliance technology would end up trying to convince you that technology can help...? You must be shocked. If you are new to *Blue Umbrella*, feel free to check out [Who We Are](#).