YOUR COMPLETE GUIDE TO

Third Party Risk Rating

GAN INTEGRITY

Table of Contents

Introduction 1

A need for a renewed approach 2

Asking the right questions 3

Taking a risk-based approach to third party due diligence 4

Risk rating your third parties 5

Building your third party risk profile 6

1. Identify the types of third parties you work with 6
2. Screening 7
3. Assess your business' degree of exposure 8
4. Assess what you know about the third party 12

Conducting risk-based due diligence 14

Failure to adopt a risk-based approach 15

Adopting a connected approach to third party risk rating 16

Introduction

Third party risks are unavoidable but manageable for almost any business out there. Working with third parties is necessary, and often advantageous, however, due to the high risks that these relationships might expose your company to, the related risks must be carefully assessed and contained to allow you to confidently enter third party agreements.

The increasingly long arm of regulators is no longer just cracking down on bribery and corruption, but regulating an array of other areas that relate to third party risks; including, but not limited to, tax evasion, modern slavery, trade sanctions, human rights and enhanced anti-trust laws, setting higher expectations for business, and compliance teams in particular, to meet these renewed requirements. Likewise, the array of risks associated with third parties has exploded even more over the past few years, moving into cyber and data security risks with the global pandemic magnifying the ways in which third parties can expose companies.

Aggressive enforcement of legislation around the world as well as tighter cross-border collaboration between national regulatory agencies attests to the increasing persistence on upholding competitive business practices around the world.

But compliance with regulations are not the only risks compliance practitioners should worry about, the omnipresent reputational risk of working with third parties has become as damaging — if not more — than financial damages companies might incur from legal settlements and litigation.

Companies today recognize the importance of costs associated with managing third parties, partly due to significant fines and unsavory headlines, but also due to the inherent way of doing business in today's global, ultra-digitized economy inherently linking business to third parties. Nonetheless, compliance practitioners still report insufficient resources and budgets allocated to their third party risk management programs.

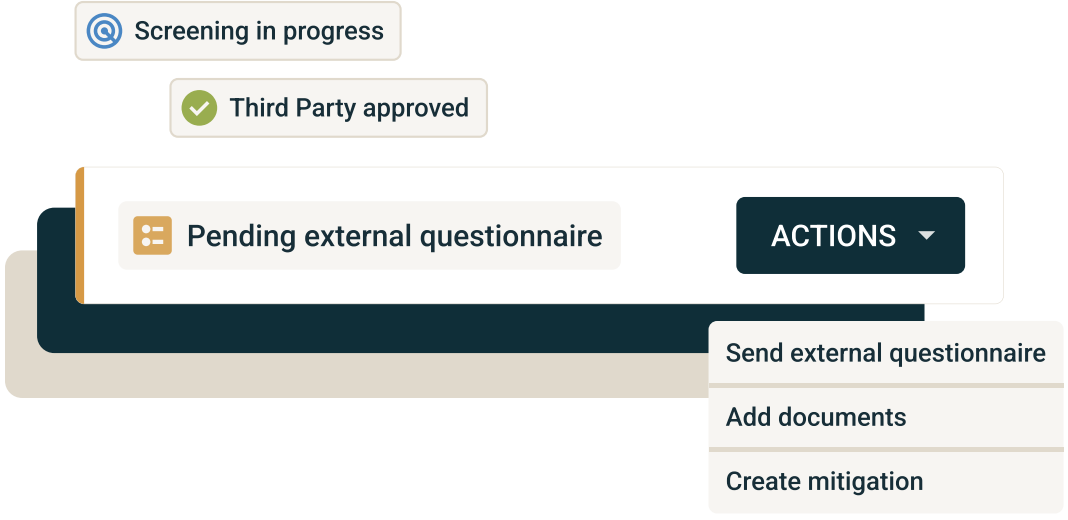
With budgets and resources lagging behind the expanding third party risks, adopting a risk-based approach to due diligence is imperative for businesses around the world.

A need for a renewed approach

Managing third parties properly is a large and complex undertaking. Third party risk management programs can be costly and require a lot of change management. While poorly executed third party management programs can lead to frustrating processes, inefficiencies, and legal risk.

Given the variety and number of third parties that many corporations deal with, managing third party risk is a complex challenge and can feel hugely daunting especially when often faced with limited resources, time and budget. It can also be overwhelming just knowing where to start and knowing which measures are suitable for the different types of third parties; Many companies work with thousands of third parties of all different types operating in different parts around the world and with different parts of their business. This is why a risk-based approach is vital.

This eBook serves as a robust guide to understanding how to effectively manage third party risks by creating a systematic and scalable due diligence approach and effectively mitigating the challenges that come with resetting your business' third party risk management program. In this eBook we will outline a few simple steps any business can take to accommodate their unique third party risk management program.



Asking the right questions

All along the value creation chain, third parties put organizations at risk. Ask yourself and your business all the right questions and make sure that the program you set up can help you answer them. Having information and insights accessible and handy at all times will give you the confidence you need to enter third party agreements without exposing your company to unmanageable risk. In order to best protect your organization, let's look at the fundamental questions you should be asking before initiating a third party relationship:

1. Am I allowed to do business with that third party? Are they on a sanctions list that would prohibit us from doing business together?

2. Am I confident that this third party is in good standing and will not create a legal or reputation liability? What would it mean to our organization if this third party was found engaging in unethical or illegal conduct? Could their conduct pose a legal liability? (Also known as "The Front Page Newspaper Test")

3. Can I explain and document my decisions if something unideal happens? This is all about taking reasonable and appropriate measures to successfully defend the organization to regulators in the face of any alleged breach.

While the safest approach would be to do a deep dive on every third party your company works with, this simply isn't feasible. The resources to make this happen are likely not available and it would be costly, inefficient, and slow down business. On the other hand, you don't want to do the minimum check for all third parties because that would leave your highest risk third parties without sufficient due diligence, exposing your organization to risk.

Take a risk-based approach to third party due diligence

Taking a risk-based approach to third party due diligence is vital. Given the sheer number and variety of third parties most organizations work with, answering every question about every third party can be nearly impossible at worst and an uphill battle at best.

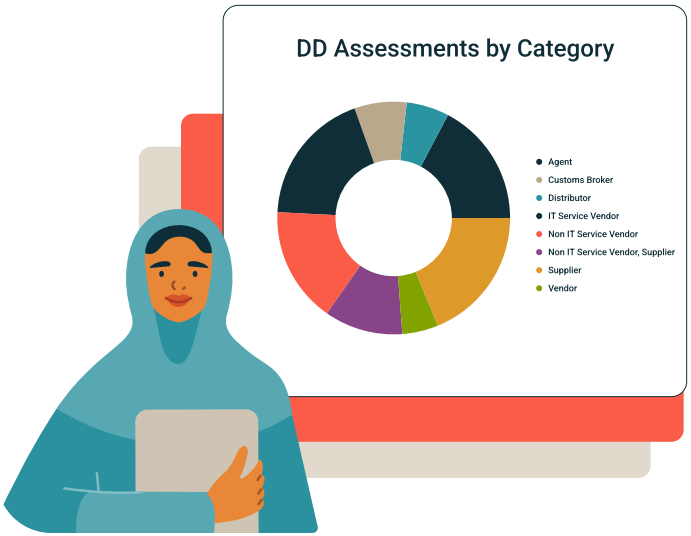
A risk-based approach will help you determine what measures are suitable for each third party and to apply different levels of due diligence to your third party population based on the level of risk they pose. This approach enables you to identify the third parties that represent the greatest risk to your organization and focus your limited time and resources on mitigating those risks, thereby creating an efficient, cost-effective due diligence process. This is where developing a risk rating methodology comes into play.

The method by which compliance professionals can determine what level of due diligence to complete and how many resources to commit should be based upon the level of risk posed by a third party. But how do you efficiently categorize third parties? How do you determine which ones are low risk and which ones are high risk? How do you allocate appropriate compliance resources for the number and variety of third parties you work with?

We lay out a step-by-step approach to third party risk rating to show you how to easily and efficiently adopt a risk-based approach to your third party due diligence program.

Risk rating your third parties

In order to risk rate a third party, you really need to look at it from two angles. First, the degree of your risk exposure as a result of your relationship with the third party. Think: what services is the third party providing to your business? Where is the work being carried out? Second, you need to examine the profile of the third party. No matter what your relationship is with them, you need to know who they are, what their reputation is, what risks, if any, are associated with the third party, and where in the world they are operating. When this information is gathered and put together it forms a risk profile for a third party. The risk profile will give you an understanding of the level of risk your company faces when entering an agreement with the third party in question, which, in turn, will help you determine the levels of due diligence and potential mitigation you need to establish to protect your company from exposure.



> “Assessing the degree of your risk exposure as a result of your relationship with the third party combined with an assessment of the third party profile and who they are will help you determine the third party’s *risk* profile.”

Building your third party risk profile

1. Identify the types of third parties you work with

Understanding the universe and the scope of third parties is crucial. Not all types of third parties undergo the same types of assessments, and each third party may carry a different level of risk to the company. Categorize third parties to achieve a high level of accuracy when conducting your due diligence process. Let's look at a few examples:

Local Venture Partner: A venture partner is a person who a VC firm brings on board to help them do investments and manage them, but is not a full and permanent member of the partnership.

Joint Venture Partner: A joint venture partner may be a person or an organization which has agreed with another person or organization (and possibly other parties) to establish a new business entity and to manage its assets.

Consortium: A consortium partner is a person or an organization which is pooling its resources with another organization (and/or other parties) to attain a common goal. Each participant in a consortium retains its separate legal status.

Sales Agents: One who is authorized or appointed by a manufacturer to sell or distribute his/her products within a given territory, but who is self-employed, takes titles to the goods, and does not act as agent for a principle.

Custom Clearing Agent: A party authorized by international customs authorities to certify and manage consignments between countries, also called customs, forwarding agents, or custom brokers.

Customer: The recipient of a product, service or idea bought from another organization/ business. Customers can be grouped into two categories (1) An intermediate customer who is a dealer that purchases goods for resale. (2) An ultimate customer is one who does not in turn resell the goods purchased but is the end user.

Contractor and Subcontractor: A contractor is a non-controlled individual or organization that provides goods or services to an organization under a contract. A subcontractor is an individual or organization that is hired by a contractor to perform a specific task as part of the overall project.

Event Agency: The event manager is the person who plans and executes the event, taking responsibility for the creative, technical and logistical elements.

Global Supplier: A supplier is a person or entity that is the source for goods or services. A company that provides microprocessors to a major computer business is an example of a supplier.

Distributor: A person or organization that buys products from another organization, warehouses them and resells them to retailers or directly to end-users.

Service Provider: A person or entity that provides another organization with functional support (e.g. logistics, processing services, etc.).

Marketing Consultants: consultants provide their advice to their clients in a variety of forms.

2. Screening

Screening is the most basic form of due diligence which seeks to answer: can we do business with this third party? It's highly advised to perform initial due diligence by screening all existing and potential clients, agents, and business partners. Check all third parties against key risk categories such as:

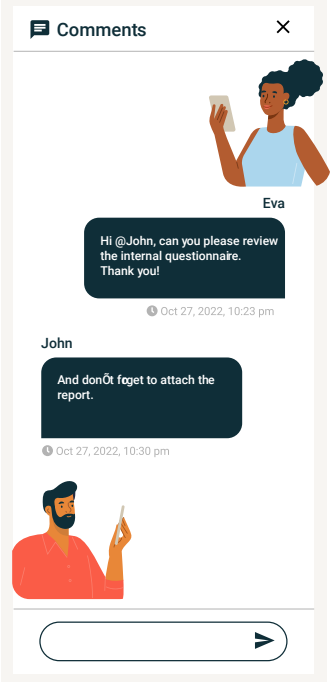
- **Government, Regulatory, Disciplinary Lists:** Screen your whole third party population against high quality and comprehensive sanctions data; this includes global sanctions, securities exchange actions, fugitives, exclusions, fraud warnings, debarment, disciplinary actions, and law enforcement.

- **Adverse Media and Press Coverage:** Your corporate reputation is invaluable. Screening and monitoring your third parties for adverse media coverage is an essential part of protecting it. Databases can provide over 100K sources and 2.5B articles through the daily media scanning of newspapers, magazines, TV, radio, and transcripts.

- **Politically Exposed Persons (PEP):** Understand your third parties' relationships with any government officials, military or judicial figures, state-controlled businesses and key executives, ambassadors and top diplomatic officials, family, associates or advisors, multinational organizations, and associated leadership. Make sure to refine your PEP screening by geographical specification, and international and regional PEPs.

- **Associated Entities:** Screen against third parties with known connections to sanctioned entities or individuals and uncover hidden risks.

- **State-owned Enterprises:** Ensure that you uncover state-owned and state invested stakes in entities with state owned enterprise data.



You can choose to not subject your third parties to a full screening and only a sanctions screening. If your sanctions screening returns a true match i.e. your company is not allowed to do business with this third party, then your due diligence journey should end at this stage and the third party relationship should be terminated.

3. Assess your business' degree of exposure

If your third party has passed the sanctions screening test and you know that your company — based on this initial assessment — is allowed to do business with the third party in question, you can progress the due diligence process to the next stage: Assessing the degree of exposure. When seeking to understand your degree of exposure you want to involve the business team requesting to initiate the relationship in this process as much as possible as they are ultimately the relationship holder. This information gathering process will typically be in the form of an internal questionnaire that the business team completes. Below are some of the key considerations that your questionnaire should address.

Country Risk

It is extremely important to identify the levels of risk in the country where the work will be carried out to ultimately help you determine the third party risk profile. Find answers for questions such as; where is the third party company located? Where will the third party operate in relation to our business? Make sure you dive into not only where they are headquartered but also into where they actually operate and/or where services are being performed. Once you have identified the country in which the third party is operating, you attribute a country risk as a first step towards forming your risk profile. If the country is very high risk your third party risk profile will skew toward being a high risk profile for your business, if the third party is operating in a very low risk country, then the country score will weigh down the risks of the third party profile. You can find a full list of country list rankings in the latest edition of Transparency International's Corruption Perception Index 2022.

Role of Third Party

You also need to understand the role the third party will play in relation to your business. Ask questions such as; what will the third party do for you? What services or products are being rendered? In which capacity will they be representing your organization? For instance, an agent representing your company in procurement negotiations should be carefully scrutinized while a catering company providing lunch to the office is a much less risky agreement requiring very little scrutiny.

Liaising with Government Bodies

Look at any connections or relationships with government officials both from a third party profile perspective (see politically exposed persons (PEPs) screenings above) or from a business exposure perspective i.e. does the nature of the services provided involve interaction with government officials such as bidding on government contracts. Ask questions such as; will the third party be exposed to or be interacting with government officials on your behalf? Does the third party have any connections to government officials that could potentially give rise to additional risks.

Criticality of Relationship

Assess the criticality of the relationship. Ask questions such as; how important is this relationship? What happens to your business if you don't work with this third party? If for example the third party is the only available distributor in a key market for your business, then the criticality of the relationship is high and it thus becomes crucial for the business to balance the risk and the business need.

Transactional Red Flags

When assessing the nature of the transactions, it's essential to identify red flags. A red flag is a fact or set of circumstances that may indicate a potential risk, but cannot be considered as evidence for the actual existence of a risk. That said, if your assessment renders one or more red flags, the task of compliance teams is to support the business in making all the right further inquiries to understand whether there are additional red flags and whether the red flags already identified do in fact indicate potential impropriety. Red flags can also help you make informed decisions around the types of mitigations that need to be established once the agreement with a third party is established. This will allow you to keep the potential risks contained and protect your business. Questions you need to ask to identify transactional red flags will vary based on the unique factors of your organization but as a general rule there are six main types of transactional red flags you should be paying attention to.

Types of Transactional Red Flags

1. **Reputational Risk:** To what extent has an entity or individual been subject to criminal enforcement actions, civil actions, or litigation for acts suggesting unethical or improper conduct?

2. **Absence of an Ethics or Integrity Program:** Find out if the third party has a compliance program in place; a good indicator of the way the third party chooses to do business is to assess whether or not they follow compliance regulations that apply to business conduct.

3. **Links to the Government:** Are government officials recommending you work with this organization? Are there any existing close relationships or ties to governing bodies?

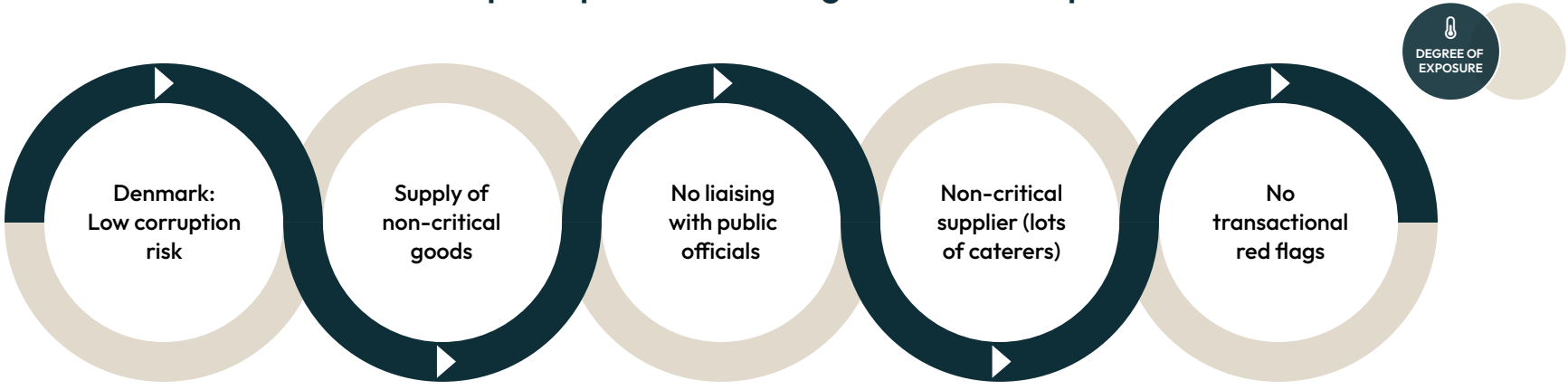
4. **Unusual Circumstances:** Is there anything peculiar about the relationship? Did the third party become part of the process late in the game? Are they uncooperative? Are they reluctant to provide the assurances that should be pretty straightforward? Does the third party want to have their involvement be anonymous?

5. **Compensation:** Look at the nature of compensation. Look at questions that account to invoicing; are they requesting upfront payments or increased commissions? Are they requesting inflated commissions? Are their payments being requested to be made through third parties or accounts in third world countries?

6. **Business Rationale:** What is the business justification? To what extent is the third party really qualified to do the job? Why can we not do the work provided by the third party internally?

Example of potential high degree business exposure

Example of potential low degree business exposure



4. Assess what you know about the third party

While the degree of exposure takes into account how you will be interacting with a third party, the third party profile consists of information that is static about the organization or person. This could be information that you gather internally, but if the risk is higher, you might want to reach out to the third party directly to request further information. The information collected in regards to your business exposure combined with data on the third party will give you a view of the third party's risk profile. Below are some factors that you should take into consideration.

Country Risk

It's important to not only look at where the third party is operating in relation to your company, but to identify where they are based and registered? Where do they operate? Keep in mind: You might only be working with the third party in a low-risk jurisdiction but they may have other operations in a high-risk jurisdiction that could still expose your company to certain risks which you need to be aware of.

Ownership and Governance

Essentially, this is about identifying who is behind the company. If you are not able to identify the ultimate beneficial owners or have trouble accessing that information, then that might be a red flag in and of itself. Look at potential concerns related to any of the individuals or persons of interest. Investigate how the company is run and managed and look at the third party's internal compliance procedures that can give you assurance that the company is protected against corruption.

Political Exposure

This is not only about whether or not a third party is liaising with government officials on your behalf but also if they have any exposure to government entities. Do any government officials have stakes in the company, even if small? Are there any public officials with significant influence over the organization? All of these factors could increase the likelihood of bribery and corruption.

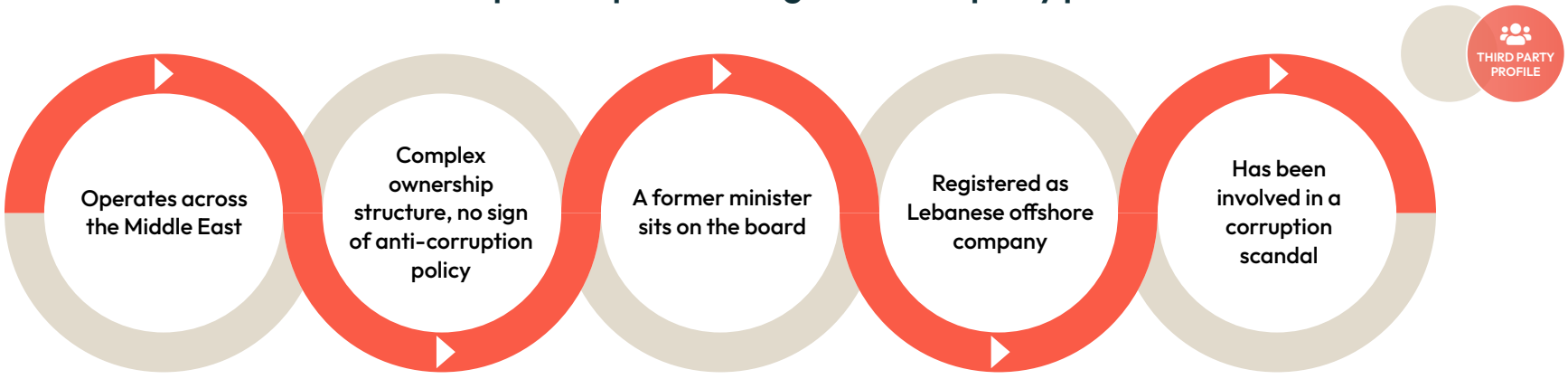
Entity Type

You will also need to look at the entity type. Find out if the company is publicly listed as that can be an indicator of transparency in operations. On the other hand, if the company is registered in a low disclosure jurisdiction or even a tax haven, you could be exposing your company to high risks.

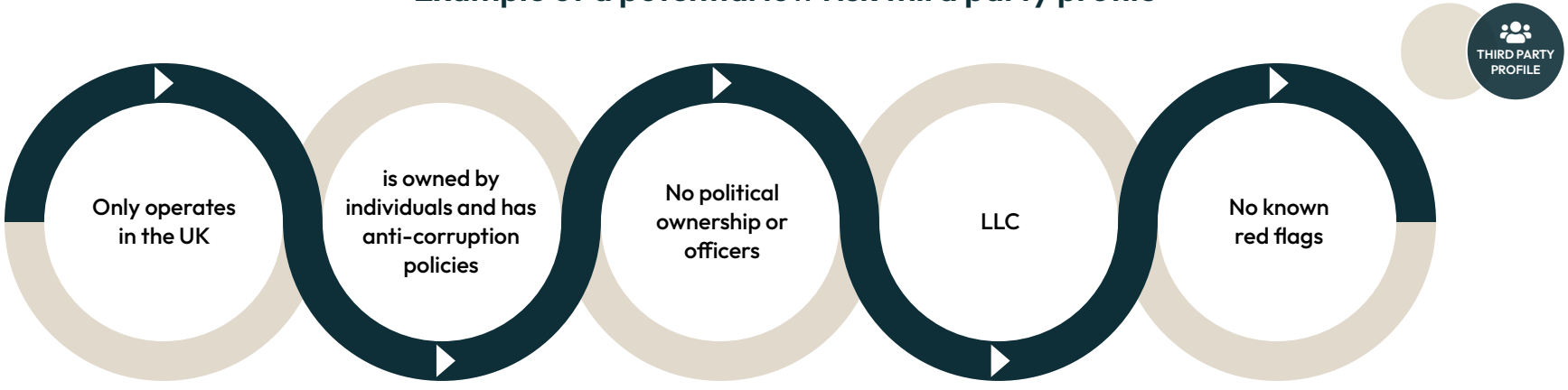
Reputation & Standing

Look into the third party's public reputation and standing: what do we actually know about them? Are we aware of any existing red flags that we might need to further investigate or mitigate?

Example of a potential high risk third party profile



Example of a potential low risk third party profile



Conducting risk-based due diligence

After you have collected information on both the degree of exposure and third party profile, likely through internal and external questionnaires, it's time to categorize your third parties into risk levels. Use a scoring system to plot the exposure risk against the third party risk to determine the appropriate level of due diligence. Your chart might look something like this:

Both how you determine levels for your third parties and what types of due diligence those levels include will be based on many factors in your organization including your risk appetite. With that said, here is one way to approach risk rating your third parties:

Level 1 : Very Low Risk

Conduct a sanctions screening to ensure that no matches are identified and that the third party indeed represents a low risk relationship.

Level 2 : Low Risk

Expand searches to include adverse media databases and political exposure databases and if matches are identified then further investigate the third party via external questionnaires.

Level 3 : Medium Risk

Have human-led red flag research conducted and further investigate the risks via external questionnaires and compliance evaluations.

Level 4 : High Risk

Conduct enhanced due diligence by looking at the full public profile and access all available public and legal records in the relevant jurisdictions. Rely on thorough external questionnaires as well as compliance evaluations and strong mitigating actions.

Level 5 : Very High Risk

Conduct boots on the ground investigations and deploy experts to conduct on-site interviews and audits. Compliance evaluations are a must and the same applies to strong mitigating actions.

Failure to adopt a risk-based approach

Numerous challenges will be presented when implementing a third party risk rating process and building a strong third party due diligence program is no easy feat. However, failing to adopt a consistent approach to third party due diligence leaves your organization vulnerable to far higher risks. A siloed approach to third party due diligence and risk-rating may lead to:

- Critical data scattered across the business rather than centralized, making it difficult to create a comprehensive and adequate third party risk profile
- Decisions are made without objective and systematic criteria and are instead based on the risk appetite of individuals throughout the organization (no matter how well-intentioned, bias is bound to happen, so ensure your process does not rely on personal judgment to make decisions)
- Low adoption rates due to complex, hard to follow processes
- A lack of focus from the compliance team as third parties are not consistently risk-rated
- Risk of not performing the appropriate due diligence on high risk third parties due to the business' limited resources
- Compliance leaders having little to no insight into what is really going on across the third party population
- Unstructured record keeping making it impossible to document the due diligence process when needed.

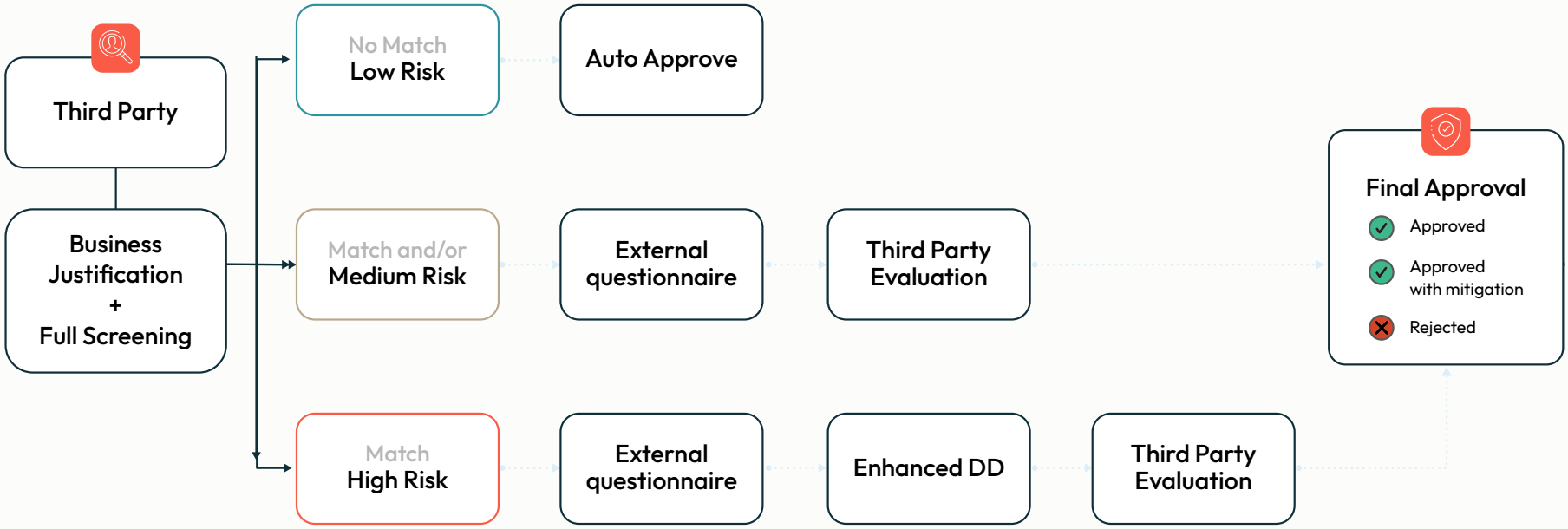
Adopting a connected approach to third party risk rating

While most organizations rely on time-consuming manual processes, juggle multiple vendors, and lack sufficient local insight to mitigate risk, there is a better way. A robust technology solution enables compliance leaders to focus on strategic planning and optimizing the process rather than being consumed by administrative headaches.

Technology can also alleviate many of the most common challenges associated with third party risk rating. Automating your risk rating process can scale your program without over-indexing the compliance team's valuable resources. Here are a few ways automation can enhance third party risk rating:

1. Easily access critical information with one centralized due diligence platform.
2. Scale objective and consistent decision making by adopting a methodological and systematic approach to third party risk rating.
3. Focus your resources by automatically approving very low risk third parties and configuring manual evaluation steps where they're needed the most.
4. Access insights in real time with an immediate overview of all third parties for complete visibility for all relevant stakeholders.
5. Empower your business and build trust with transparent and clear due diligence processes that keep stakeholders informed every step of the way.
6. Apply the appropriate amount of scrutiny to allocate resources based on risk and ensure decisions are made at the right level.
7. Enable automated on-going monitoring to ensure that you are managing risks beyond the approval stage of your due diligence process.

Sample Due Diligence Workflow



Automation can go a long way in helping your team create a comprehensive and consistent third party risk management program, but crucial to its success is getting buy-in from the business. Make the case up front for why following compliance processes matter and secure buy-in from key stakeholders well ahead of launching your new risk rating program. An impactful way to do this is by including the business from the outset of the process and asking for their feedback along the way.

Other necessary support might come from the board, which can be a powerful approval to have on your side when you are trying to get other individuals or teams to adopt the new process. In short, think through how you will ensure buy-in around third party risk rating in advance, not when you are about to launch the program.

After you have launched the new third party risk rating process, focus on maintaining that credibility, which can be very easy to lose if the process starts to go awry. Be open to feedback from all parts of the organization and be prepared to make adjustments to the process overtime.

At the end of the day, the risks third parties present are not going away anytime soon. Risk rating your third parties has the potential to transform the way your company manages and mitigates risks in a streamlined, cost-effective, and consistent manner. As you begin implementing risk rating in your organization, remember to customize this process to your organization's unique qualities including industry, geographical concerns, and risk appetite. We hope this eBook has been insightful and helpful in your third party risk rating journey.

GAN Integrity enables the world's largest brands to do the right thing.

We fulfil our mission by enabling global teams to manage ethics, compliance, and risk with our Integrity Platform, a no-code application building platform.

Seadrill · DANONE NORTH AMERICA · CLARIOS · BARRICK · infront

Schedule a meeting to start driving ethical change

To contact us, visit **ganintegrity.com**