Deloitte.

# Considerations for effective Third Party Due Diligence as part of a successful Third Party Risk Management programme

## Third Party Due Diligence – a vital but challenging process

Regular headlines about organisations caught out by issues of corruption or tax evasion in relation to donors, agents, distributors or joint venture partners highlight more than ever the need for effective Third Party Risk Management ("TPRM") including Third Party Due Diligence ("TPDD"), and the cost of getting it wrong. Similarly, supply chain integrity problems such as human rights issues – including the alleged use of forced labour by suppliers – all too frequently see established and otherwise reputable brands brought into the headlines for the wrong reasons. Indeed, the question of product safety, and the traceability of product components through the supply chain, is one which continues to be of key importance in a number of sectors (including the food, pharmaceutical, and luxury items sectors) with even legitimate distribution channels in developed nations being increasingly infiltrated by counterfeits.

Increasing regulatory pressures and the need to mitigate an increasing range of risks creates, making it essential that any approach to understanding and assessing an organisation's third parties is risk-based and proportionate, allowing for the efficient distribution of resources while reducing overall risk exposure.

For multinational organisations dependent on a growing network of external third parties, failure to properly manage the increasing number of risks posed by such relationships can have serious consequences, including regulatory fines, criminal prosecutions, reputational damage, and operational impact.

"Third parties and intermediaries in particular are the single greatest area of bribery risk for companies."

Transparency International UK

## Six considerations or questions

Based on almost 25 years of helping clients manage third party risk through effective due diligence, we have identified six considerations and questions that we believe are important in effectively taking on this challenge:

1. Do you understand your third party population and the different levels of risk posed by your third parties?
2. Does your approach to TPDD adequately mitigate the relevant risks?
3. Are your third parties screened on a regular – or even ongoing – basis?
4. Does your organisation have central oversight over the TPDD approach? Is there sufficient SME specialism to deal with the outputs of any TPDD activities?
5. Have you defined your red lines from a risk perspective?
6. Are you using technology to enhance the value, efficiency and cost-effectiveness of TPDD activities?

Further detail on each of the above is provided on subsequent pages.

## Considerations for – and the challenges of – a successful TPDD approach

### Six Questions to consider:

1. **Do you understand your third party population and the different levels of risk posed by your third parties?**

Key to successful TPRM is understanding your third party population and the type and severity of risk they may pose to your organisation, as different third parties will typically require a different approach. For distributors and agents for instance, bribery and corruption remain a significant risk, while with an ever-increasing public focus on 'responsible' value chains, violations relating to human rights or sustainability issues will be key when looking at suppliers.

Understanding the severity of risk posed to your organisation by different third parties allows for the most efficient distribution of resources (both in terms of budget and internal and external specialists) when mitigating risks associated with these relationships, allowing you to focus greater resources on those third parties performing the most high-risk activities or that are of most strategic importance to your business.

Risk segmentation is therefore the foundation of any successful TPRM programme and requires an organisation to understand and map out who its third parties are; where they are located (and who their contacts are within the organisation); what services they provide to the organisation; what regulations apply to the services being provided; how strategically important they are; and how these factors affect their overall risk profile.

The UK Bribery Act requires that:

"A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities."

**2. Does your approach to TPDD adequately mitigate the relevant risks?**

TPDD is a core component of any successful TPRM framework, and a thorough understanding of one's third party population enables TPDD to be conducted proportionally and on a risk-basis, typically using a tier-based approach with the level of screening conducted proportionate to the risk presented by the relationship. For instance, automated screening tools can be extremely helpful in screening higher volumes of third parties considered lower risk, whereas higher risk third parties – or those of strategic significance to the organisation – typically require a more in-depth human-led approach conducted by subject matter experts with knowledge of the relevant regulatory frameworks and research tools, as well as jurisdictional complexities and nuances.

Segmentation further allows an organisation to screen against multiple relevant risks for a particular third party, beyond just anti-bribery and corruption (the traditional domain of TPDD). Such risks may include environmental issues, labour issues, human rights and child labour issues as well as food safety, all of which are also subject to regulatory pressures and are increasingly coming under close scrutiny by the public, with the potential for significant reputational fall-out for any organisation perceived to not be adequately addressing and combating such issues.

Head of Ethics, Integrity & Compliance for listed UK multinational:

"a few years ago my main third party risk concern was about bribery on the sales side, but increasingly supply chain risks are on the agenda and this needs an adjusted approach in order to manage them properly"

## What different levels of screening may look like:

**Lower risk – automated media and/or key list screening**

Screening on lower risk parties typically focuses solely on the third party itself, which is screened against sanctions lists and regulatory watch-lists, and may also include adverse media searches for specific red flag issues as identified through key search terms.

**Medium and higher risk – full public record research**

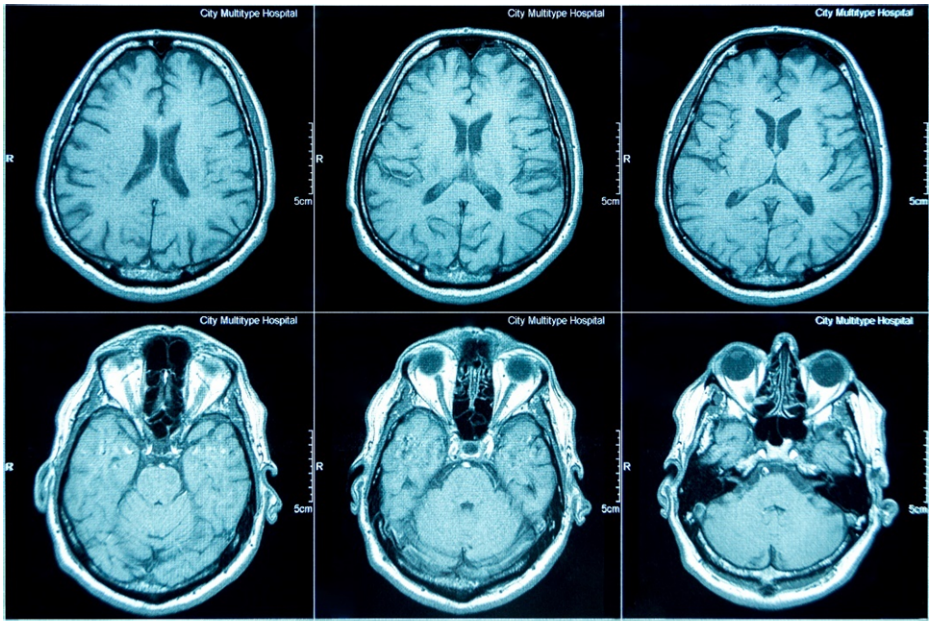
Due diligence searches on higher risk third parties typically include in-depth public record research in English and the key business language(s) of the relevant jurisdiction, and typically seek to identify information in relation to both the third party and key associated individuals (such as UBOs or key management). Such information gathering typically seeks to identify information relating to the identity of the company; its business background, activities, track record and reputation; its ownership (including seeking to identify beneficial owners and indications of state ownership); political or official connections held by the company or its shareholders and key managers; and their involvement in specific 'red flag' issues.

**Higher risk and strategic relationships – human intelligence**

Where a deeper insight into a third party is required than can be provided by public record information alone, information can also be gathered through human sources in the relevant jurisdiction and sector, with this approach typically gaining more in-depth information on issues such as the subject's reputation, track record and modus operandi, political links, and 'red flag' issues. This methodology is also valuable in jurisdictions which do not have a free press or lack an active tradition of investigative media.

**3. Are your third parties screened on a regular – or even ongoing – basis?**

When considering whether your TPDD approach successfully mitigates against relevant risks, it is also important to consider how you monitor your third parties once the initial due diligence exercise has been completed. While routinely reviewing risk assessments (for instance refreshing searches every 2-3 years) does contribute to reducing risk exposure to a certain extent, leveraging technology to monitor these on an on-going basis (a relatively new development in this space) is a cost-effective tool that can help identify substantial issues in "real time". In recent years for instance, a multinational industrials business paid the US Securities and Exchange Commission and Department of Justice millions of dollars in fines to settle FCPA offenses relating to the payment of bribes by its intermediaries to officials in various jurisdictions over a period of several years. There had been allegations of wrong-doing by the intermediaries in the public domain years before the company was investigated, which ongoing monitoring would have identified a lot sooner and allowed the company to cease – or more tightly control – its relationship prior to the damage being inflicted on the company itself.




Developments in Artificial Intelligence (AI), Machine Learning (ML) and multilingual Natural Language Processing (NLP) have allowed for persistent monitoring capability that can search millions sources for adverse events relating to third parties, reporting in real time.

**4. Does your organisation have central oversight over the TPDD approach? Is there sufficient SME specialism to deal with the outputs of any TPDD activities?**

While some organisations closely control and manage TPDD activities centrally, others devolve responsibility to their regional businesses. In our experience, while regional teams can add invaluable jurisdictional insight into the TPDD process (for example in terms of which individuals should be included and the risk profile and areas of focus of certain local third parties), some level of central oversight is vital to ensure consistency across the process and to avoid the temptation for certain local business to perform less meaningful due diligence activities to ensure revenue generating activities are not "undermined". This does not mean a single standard methodology should be employed across the world – indeed it is vital that for higher risk third parties TPDD is done using meaningful local data sources and by individuals who understand jurisdictional nuances - but where different approaches are taken across regions this should be a deliberate approach.

A centralised ownership approach to TPDD also allows for consistency and accountability in any required remediation activities, for example in responding to TPDD that identifies allegations of corruption or other risks. In turn, it is essential that those dealing with such issues have adequate understanding of the applicable regulatory frameworks to ensure that these items are dealt with adequately.

## Consideration: Global versus jurisdiction-specific searches

Global data sources – such as company information sites, global media databases, curated watchlists and aggregated litigation databases – are extremely valuable TPDD tools, helping companies gain quick and wide-ranging understanding of "low-hanging" third party risks. However, for higher risk third parties, meaningful searches of jurisdiction-specific data sources are key to gaining a proper understanding of the risks of such parties. For example, we find that company information sites can be unreliable for many African jurisdictions in trying to identify beneficial owners and so local registry records can be key. Similarly, in China local litigation information is surprisingly detailed and can provide very valuable insight on bribery and corruption issues that simply is not forthcoming from global data searches.

**5. Have you defined your red lines from a risk perspective?**

Another important component of a successful TPDD approach is understanding your organisation's risk appetite, defining deal killers and having a clear process in place to deal with the results of the due diligence risk assessments as well as any non-compliant third parties. It is key that action is taken where required to minimise exposure to risk, not least because, should something go wrong, being aware of specific risks and not acting on these will not be viewed positively by any regulators.

**6. Are you using technology to enhance the value, efficiency and cost-effectiveness of TPDD activities?**

In addition to the abovementioned developments on automated ongoing monitoring, we have seen many clients' ability to successfully manage TPDD and TPRM enhanced by tech-enabled TPRM platforms that automate actions (such as populating questionnaires; risk segmentation activities; remediation activities), ensuring that key risks are not missed; allowing your internal specialists to avoid admin tasks and focus on what is important; and also helping with the central oversight point set out above. There are now a number of different tools that can be configured specifically to your organisation's needs which many companies operating in emerging markets are now utilising to their benefit.

## Key Contacts

**Mark Bethell:**
Partner
+44 20 7007 5913
mabethell@deloitte.co.uk;

**Camilla Volcic:**
Senior Manager & TPDD specialist
cvolcic@deloitte.co.uk
+44 20 7007 6658

**Rick Dickerson:**
Senior Manager & TPDD specialist
rdickerson@deloitte.co.uk
+44 20 7303 2123

**Jorge Rivera:**
Senior Manager & TPDD specialist
jorrivera@deloitte.co.uk
+44 20 7303 8131