Mitigating Third-Party Risks with Astrus

In today's global environment dealing with the risk of doing business with third parties, e.g. clients, suppliers and agents, is becoming more and more important. We see clients struggle with mitigating the risk of doing business with these third parties. A more strategic and risk based approach is key to avoid reputation damage, liability and financial penalties.

Drs. Leen Groen RA and Patrick Özer MSc

Drs. Leen Groen RA
is a director at KPMG Forensic, part of KPMG Advisory N.V.
groen.leen@kpmg.nl

Patrick Özer MSc
is a senior manager in the Forensic Technology team of KPMG Advisory N.V.
ozer.patrick@kpmg.nl

Introduction

Risk-based due diligence is an important element in dealing with third parties and this is also considered by regulators when assessing the effectiveness of a company's compliance program ([MOJ11]), ([POA10]), ([USDJ17]). Global transactions and regulatory scrutiny increasingly impel companies to examine their business relationships in order to assess risk, undertake informed negotiations, and comply with regulatory mandates. Failure to adequately assess clients, suppliers and agents, and to know how they operate can expose organizations to reputational damage, operational risk, governmental investigations as well as financial penalties and potential criminal liability.

To efficiently and effectively manage the third party risk, a risk-based approach is required. It is not possible or even desirable to perform the same scope of due diligence on all third parties (cost, time and effort). A risk-based approach is also reflected in regulations ([DNB15-1]) that include a component of third party risk management (TPRM) like Anti-Money Laundering and Anti-Bribery & Corruption.

An effective third-party risk program would likely include the following elements:

1. identification of the universe of third-party intermediaries (TPIs) and those that the organization determines to be within scope (i.e. to be included in the TPRM process);
2. managing the integrity due diligence process and risk assessment;
3. conducting the appropriate level of integrity due diligence (IDD);
4. ongoing monitoring of certain TPIs.

To ease the above risk-based due diligence process, KPMG developed the Astrus technology, which will be outlined in this article.

Astrus

Astrus due diligence is a cloud based solution, accessible through a portal, which provides efficient means to obtain information and assess risks associated with clients, suppliers and agents through a technology-enabled, research methodology. The result of Astrus due diligence is a report with standardized sections (see below). Astrus reports can access an extensive range of on-line public data records (more than 40,000 sources) including global sanctions and regulatory enforcement lists, corporate records, court filings, press, media and internet sources to identify important integrity and reputational information, which can be used to support due diligence assessments.

Experienced Corporate Intelligence specialists, capable of dealing with 88 different languages, manually analyze and evaluate the Astrus search results. In addition, Astrus uses innovative technologies like IBM Watson Explorer to evaluate and classify results to rule out false positives, hence reducing the investigation time.

40,000+ sources **88** languages

Standardized reporting

An Astrus due diligence report always contains the following sections:

1. an executive summary with all the key findings, including an overall risk indicator;
2. background details of the entity;
3. information relating to the shareholders;
4. adverse press/media comment;
5. litigation;
6. sanctions and high-risk entity lists;
7. key directors/principals.

Each section contains a risk indicator, ranging from green over amber to red. The details of each section are described in the body of the report itself.

1. Executive summary

As mentioned, the executive summary summarizes all the key findings arising from the report. The overall risk indicator is determined by the highest individual risk indicator identified in each reporting section. A chain is a strong as its weakest link.

2. Background details

The Astrus technology conducts searches into a wide range of commercially-available litigation sources. The searches are narrowed to records pertaining to the subject of the enquiry, focusing on its principal place of business. The availability of online litigation information varies significantly from country to country. In those cases where there are no or limited online resources available, additional and sometimes local research is required, which can also be provided by the Corporate Intelligence team.

Examples for applying a red risk indicator for background details are when an organization is subject to regulatory supervision, is insolvent, bankrupt, or when the auditor has resigned and has drawn attention to issues of an adverse nature that have led to resignation.

Examples for applying an amber risk indicator are when there are inconsistencies identified between: company name; company number; and/or date of incorporation or when an organization is significantly loss-making, or has net liabilities.

3. Shareholders

For this section, searches into online corporate registries and international credit bureau information sources are conducted to identify the significant shareholders (>5%). Also, information to identify the ultimate beneficial shareholders (>25%) in the legal entity is attempted to be retrieved.

Risk indicators: Company ABC

Area	Indicator	Details	Page
Adverse press/ media comment		Company ABC has a moderate public profile and has been the subject of adverse press comment in relation to an anti-trust investigation and a price-fixing scandal. According to a press report published on Media X in 2009, Company ABC was investigated by the Dutch Competition Authority in connection to an anti-trust case and a price-fixing cartel. According to reports of Organization for Economic Co-operation and Development ("OECD)" and the Regulatory Department of law firm Y, as of September 2013, Company ABC avoided fines by applying for clemency and helping the authorities identify cartel members and the price fixing scheme.	7
Litigation		No reference to Company ABC was identified in available online litigation records.	9
Sanctions and high-risk entities lists		No reference to Company ABC was identified in published lists of entities subject to international economic sanctions or other available lists of high-risk entities.	10
Director information / key executives		According to the Dutch corporate registry, Key principal 1 is the Chief Executive Officer and Chairman of the Board of Directors, Key principal 2 is the Chief Financial Officer, Key principal 3 and Key principal 4 are Members of the Board of Directors of Company ABC. No adverse information was identified in relation to these Key principals. As according to information retrieved from the Dutch and German corporate registry Company ABC's ultimate beneficial owner is the German Federal Government, the Executives and Directors of Company ABC may be considered politically exposed persons ("PEP").	11

Table 1. **Example of risk indicator overview - Astrus report.**

A red risk indicator will be assigned when for example a major shareholder (>25%) has a highly controversial reputation.

An amber risk indicator will be assigned when for example shareholder(s) cannot be identified from online public record sources, shareholder (>25%) is in administration, insolvent, bankrupt, has been liquidated, struck off or has otherwise ceased trading. The amber risk indicator is also assigned when an entity has an overly complex or opaque corporate structure (use of multiple offshore locations, trusts, foundations etc.).

4. Adverse press/media comment

This might be one of the most interesting sections. Adverse press or media comment will be highlighted concerning the target subject. Where the subject is part of a group of companies, any significant adverse press or media coverage concerning the activities of the group as a whole will also be highlighted. However, it is often not feasible to conduct detailed enquiries into the other group members, for there are companies with many, many subsidiaries.

A red risk indicator will be assigned when significant, sustained adverse press or media coverage is found, including a minimum of one high reliability source of information, for example the *Wall Street Journal*, *Economist* or *Financial Times*.

An amber risk indicator is assigned when for example reporting of a negative nature that is not necessarily sustained or significant is found. Or when matters of a serious nature affecting close business associates or family members are being found. Significant issues may include those such as links to fraud, money laundering, bribery or corruption, or other matters likely to give rise to a criminal offence. An amber indicator in this category may also include sustained or significant adverse reporting where the source reliability is low, such as social media or blog entries. This may also include less serious issues that are identified in high reliability sources.

5. Litigation

Within this section searches are conducted into a wide range of commercially-available litigation sources for records pertaining to the subject of the enquiry, focusing on its principal place of business. The availability of online litigation information varies significantly from country to country. Sometimes additional inquiries are required.

A red risk indicator is assigned when for example involvement as a defendant in major civil litigation, litigation initiated by a regulator or involvement in any criminal litigation is found in online resources. Also, repeated or numerous litigation as a defendant would be a ground to assign a red indicator.

An amber indicator is assigned when the entity has a litigious profile (in case the entity concerned is the plaintiff).

6. Sanctions and high-risk entities lists

For this section searches are conducted on lists of entities subject to financial sanctions and other lists of potentially high-risk entities, such as regulatory enforcement notices, law enforcement agency notices and other similar blacklists. This search includes the identification of possible Politically Exposed Persons, which is required from an Anti-Money Laundering perspective and is a high risk from a Bribery and Corruption perspective.

Examples for a red risk indicator are in case of an entity that is listed on a current financial sanctions or debarment list, if there is involvement of a director, key shareholder (>25%) or key principal of an organization who is listed on a current financial sanctions or debarment list, is an undischarged bankrupt, the subject is listed on a current regulatory enforcement list, is subject to current regulatory enforcement action, or has been subject to regulatory enforcement action or penalty in the last 12 months.

An amber indicator is assigned when the subject is formerly listed on a sanctions or debarment list, and is now discharged, formerly listed on a regulatory enforcement list (>12 months previously), provided that the action has been concluded, formerly listed on a law enforcement list, provided the action has been concluded or the individual has been discharged and there are no ongoing matters of a criminal nature, is listed as a Politically Exposed Person (current and former (within last 5 years) senior public officials, and their close family members), in case of a formerly disqualified director.

7. Key directors/principals

In this section details concerning the date of birth, nationality, education, career development, key corporate interests, adverse press and litigation are collected from online public record sources. This information is collected for all key directors which in addition will be checked against: commercially available lists of Politically Exposed Persons, financial sanctions and high-risk entities lists (see above).

Reasons for a red risk indicator can be for example misrepresentation of professional and/or academic qualifications.

An amber risk indicator is assigned when inconsistent information is identified between independent sources, e.g. date of birth information, current position or use of fictitious titles and awards.

Report on an individual

It is also possible to do an Astrus report on an individual. In this type of report, the sections 'shareholders' and 'key directors/principals' are not applicable, while the section 'corporate interests' is added. In the latter section, searches will be conducted within online corporate registries and international credit bureau information sources, to identify current or former corporate interests held by the individual and identify adverse press or media comment related to these interests.

Red risk indicators are raised among others in cases the entity is subject to involuntary insolvency or bankruptcy proceedings. Furthermore, the red indicator is assigned if the director or the principal has been involved in illegal or unethical conduct during their tenure of office.

An amber risk indicator is assigned in case the role or responsibility within an organization, has been overstated; the individual is involved in a large number of dissolved companies or lack of substantive information concerning source(s) of wealth.

Our vision of the future

Continuous monitoring

Doing a due diligence on a third party when entering a business relation is not enough. Things can and will change over the years and for this reason, our clients want to be informed when something significant changes on the side of their third party. This can vary from changes in ownership structure to litigation or adverse media. Astrus monitoring has been developed to mitigate the risk of changes in the risk level of a certain third party after a due diligence has been performed. Astrus monitoring monitors data sources for these significant changes and monitors adverse media and alerts the client when changes occur or new adverse media is identified. We foresee that more and more clients want to move in the direction of continuous monitoring of third parties.

New sections

In today's world, there is a growing need for more transparency. Take for example the issue of human rights. Stakeholders want to know if a company is doing business with third parties using forced labor or child labor in their factories. Or think about the topic of food fraud. More and more we want to know what the supply chain looks like, which stakeholders are involved and what the reputation is of these stakeholders.

We foresee new sections to an Astrus report for specific needs and/or sectors. At this moment we are working on an Astrus 'Green' paragraph that provides the requestor with more detailed information on specific sustainability issues. For this section, new data sources are used such as certification databases.

In the future, a request for an Astrus report might look like a Chinese takeaway menu: the requestor can pick and choose which special categories that need to be included.

Predicting the future

Another trend that we foresee is prediction based on history. Due diligence investigations are often performed to identify risks which may rise when entering into a business relationship with a third party. Based on the severity of the identified risks one may decide to not enter into the business relationship or set up procedures to mitigate the risks. Determining the appropriate risk mitigating strategies would take less effort if one was able to predict the target's behavioral pattern. This is quite difficult since the future and the target's behavior are determined by many variables which in addition are correlated with one another. However, we believe the Astrus technology will be heading in this direction. The previous sections dealt with the different topics that constitute an Astrus report. When these topics are combined they provide valuable data on the target's (historical) background, environment, relationships, litigation involvement, etc. Anonymizing and aggregating all Astrus reports, would populate a very large dataset which contains a vast amount of behavioral information. We believe that – in the future – such data may provide meaningful predictors to forecast any target's behavior.

Conclusion

Organizations feel the need to manage their third party risk more than ever. In the current information and data age organizations cannot hide and state that they were not aware of the risks that their business partner could pose. This is a problem that both large and smaller organizations are facing. Despite the fact that larger organizations often do have due diligence processes in place, it is still difficult to assess the risk of their entire business partner ecosystem. For smaller organization it can be difficult to have sufficient resources to assess all business partners. Solid due diligence with a tool like Astrus can help to overcome these hurdles, especially when a risk-based approach is in place.

Another effect of the information age is that society expects organizations to stay in control of their third party risk in real-time. Not only periodic due diligence, but continuous monitoring is necessary to accomplish this.

Obtaining a due diligence report is one thing, interpreting the provided results is another. Does a red risk indicator mean that you have to exit your (potential) business partner? We observe that organizations have difficulties with interpreting results from due diligence reports like Astrus. When a business partner is listed on a sanctions list this means that you cannot accept that business partner or have to terminate the relationship. With regard to the other high risk indicators the organization should be aware of the risk and implement additional measures to mitigate that high risk. Is the risk, after mitigating measures, higher than the risk appetite, the organization should consider terminating the relationship. Astrus may be a good starting point to ease the aforementioned problems.

References

[DNB15-1] DNB, *Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act*, 2015, www.toezicht.dnb.nl/en/binaries/51-212353.pdf.

[DNB15-2] DNB, *Integrity Risk Analysis - More where necessary, less where possible*, 2015, www.toezicht.dnb.nl/en/binaries/51-234068.pdf.

[IBM17] IBM, *Watson Explorer*, 2017, https://www.ibm.com/us-en/marketplace/content-analytics.

[MOJ11] Ministry of Justice, *The Bribery Act 2010 Guidance*, 2011.

[POA10] Parliament of Acts, *Bribery Act 2010*, The Stationery Office Limited, 2010.

[USDJ17] US Department of Justice, *Foreign Corrupt Practices Act*, 2017, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

Figure 1. **Drivers to perform third-party enhanced due diligence.**

About the authors

Drs. Leen Groen RA is a director at KPMG Forensic, part of KPMG Advisory N.V., and is responsible for the advisory services regarding Anti-Money Laundering, Sanctions, Anti-Bribery and Corruption and Fraud. He has extensive experience in conducting risk analysis and performing investigation into third parties in a diverse ranges of sectors.

Patrick Özer MSc is a senior manager in the Forensic Technology team of KPMG Advisory N.V. He has a background in Artificial Intelligence and has nine years of experience in conducting fraud investigations from an IT perspective. Patrick is specialized in digital fraud investigations, corporate intelligence and compliance investigations.

Use case

On behalf of a global investment bank, we provide risk-based due diligence reporting on prospective and current customers across a variety of banking products and relationships around the world. We additionally provide customized and targeted due diligence reporting to assist the institution with identification of information and risk in transactions including acquisitions, joint-ventures, trade finance and other bank investments. Additionally, we provide the bank with on-demand third-party monitoring, to assist with the identification of changes in customer profiling that can affect risk rankings or KYC information for the bank's data systems.