Third-party risk management

kpmg.com

KPMG INTERNATIONAL

What you don't know about **your business partners can hurt you**

Globalization and increasing regulatory pressures require organizations to examine their business relationships in order to assess risk, take informed decisions, and comply with laws. Government agencies are demanding high standards of business integrity. Failure to adequately scrutinize clients, vendors, agents and business partners, and to know who they are and how they operate, could expose organizations to reputational damage, operational risk and government inquiry, monetary penalties and even criminal liability.

Ignorance is no defense – and therefore what you don't know about your business partners can hurt you.

Whether you are a financial institution on-boarding clients with funds from a potentially suspicious origin or a global entity conducting business in a distant foreign jurisdiction, you are at risk. As organizations enter and operate in new markets, they are likely to have to rely on third parties, many of whom operate far from headquarters, in a foreign language, with different customs and ways of conducting business. Regulators are making it a high priority to police such relationships, and when something goes wrong, the penalties can be significant.

The majority of recent enforcements under the US Foreign Corrupt Practices

> "Risk-based due **diligence** is particularly important with **third parties** and will also be considered by **DOJ and SEC** in assessing the **effectiveness** of a company's **compliance program.**"
>
> *A Resource Guide to the U.S. Foreign Corrupt Practices Act*
>
> By the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission

Act (FCPA) have been in relation to acts carried out by agents or intermediaries, which have had serious repercussions for the organizations employing third-party intermediaries (TPIs).

The FCPA guidance issued by the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) in 2012 noted that the following guiding principles always apply when evaluating TPIs:

First, as part of risk-based due diligence, an organization should understand certain information about its TPIs including their qualifications, reputation and relationship with foreign government officials.

Second, organizations should understand the business rationale for the inclusion of the TPI in the transaction.

Third, organizations should perform some form of ongoing monitoring of the TPIs.

In the financial services industry, a number of regulators have criticized banks for inadequate due-diligence measures to tackle risks around their third parties, including customers, correspondent banks, agents and others. In the UK, the then Financial Services Authority (FSA) complained that most firms rely heavily on an informal "market view" of the integrity of third parties and that often very basic checks were performed, such as only searching the third party's Web site. In the US, the US Department of the Treasury's Financial Crimes Enforcement Network has sanctioned banks that have failed to conduct adequate due diligence on certain foreign correspondent accounts as required under the US Bank Secrecy Act.

Many laws and regulations require organizations to "know" their third-party intermediaries (TPIs).

FIGURE 1

Source: Third-party risk management, KPMG International, 2013.

A program for successful third-party risk management

KPMG's recent Global Anti-Bribery and Corruption Survey noted that multinational corporations say that the difficulty in performing effective due diligence on foreign agents/third parties is one of their most challenging anti-bribery and corruption issues. As a result, organizations are looking to build processes and programs to manage third-party risk that is efficient, scalable and fits their unique requirements. It also needs to be embedded into their overall compliance program. Many organizations have only just begun to develop processes to on-board new TPIs and put their existing TPIs through a third-party risk management (TPRM) program. An effective third-party risk program would likely include the following elements:

1. Identification of the universe of 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.

KPMG professionals can assist you in determining which elements of the TPRM process would meet the unique requirements for your organization, as well as which technology/tools might be necessary to enhance efficiency and provide the appropriate level of IDD and monitoring of the TPIs.

1 Identification of the universe of TPIs

TPIs include business partners, distributors, agents, consultants, vendors, customers, logistics providers and others (Figure 2). Organizations may have thousands of TPIs archived in systems in various geographies. Thus, the initial challenge is to understand the universe of TPIs, the location of the data and the means with which to efficiently extract the specific data that will ultimately be used for the risk assessment.

Ease of data compilation can depend on whether or not the information is centralized and to what extent it is digitized. If it is held in many locations around the world, it is likely to be more difficult to collect. Organizations that must comply with the conflict minerals provision of Dodd-Frank will have to research the various tiers of their supply chain to understand the source of their product components. Whatever the individual circumstances of the organization, it is important to obtain sufficient information to be used for the risk assessment. Making strong efforts early on to obtain data from company systems may save time otherwise spent in the next phase on sending questionnaires or on other forms of data collection.

Once the universe of third parties and related data has been compiled, organizations would then need to apply initial analytics to eliminate those third parties that would clearly fall out of the scope. The filtering analytics are likely to include whether the organization has conducted any business with the TPI in the recent past (24 months). If the FCPA is the primary driver for the assessment, a US organization may wish to eliminate domestic TPIs. Duplicates, such as 10 separate locations for a single vendor, should also be filtered out but keeping any relevant information in the process. There are other filtering criteria that an organization may want to include, and so the size of the mesh will vary depending on their specific requirements. KPMG professionals can help organizations to identify where the information resides, what is relevant and what information needs to be extracted. Once extracted, the information can be put it in a format that can then be used for risk assessment.

FIGURE 2: Examples of Third Party Intermediaries

- Regulatory consultants
- Product registration agents
- Health and safety consultants
- Purchasing agents
- Lobbyists
- Promotional consultants

- Travel and event vendors
- Distributors
- Customs agents
- Freight forwarders
- Shippers wholesalers

- Joint venture partners
- Acquisition targets
- Sales agents
- Brokers
- Resellers

2 Managing the integrity due diligence process and risk assessment

After identifying and prioritizing the portfolio of TPIs or where a new TPI needs to be on-boarded, there should be a defined process that is then managed to gather further information about a TPI and to perform a risk assessment to determine the appropriate level of integrity due diligence (IDD) for that particular TPI.

Gathering further information

Organizations will need to use certain criteria and attributes to assess and rank the risks associated with each TPI. These criteria are likely to vary by organization and may include:

- Country of operation, where service will be provided
- Nature of relationship
- Country of payment
- Type of industry
- Length of relationship
- Significance of relationship
- Nature of relationship
- Degree of government involvement
- Length of time in business
- Annual volume of transactions.

Some of the information needed to compile the risk attributes of the TPIs will be found in the client's databases or with the business sponsor, but other information will have to be collected from elsewhere. Operational and compliance-focused information can be collected by sending out tailored due diligence questionnaires to the internal business sponsor of the TPIs and/or to the TPI itself. Such completed information could then be used to risk-assess the TPI.

Technology enablers

Some organizations have taken a somewhat unsystematic approach to TPRM, often resulting in an array of electronic spread sheets that are hard to analyze and control. But there are better and more efficient solutions available. The technology solutions in the market can provide:

- Web-enabled functionality
- Due diligence questionnaire and survey capabilities
- Customizable reporting dashboards to manage and control the process.

KPMG professionals can assist in evaluating the various technology solutions and in configuring a solution to:

- On-board the data relative to the in-scope TPIs
- Provide assistance to determine the applicable TPI risk attributes
- Determine the relative weighting of the risk attributes
- Develop the due diligence questionnaires.

These systems are often developed on site by KPMG professionals and behind their clients' firewall. Alternatively, an organization can use KPMG's technology solution and have KPMG Forensic maintain the process, data, etc.

Risk assessment

Once the organization has identified the in-scope TPIs and obtained sufficient information, it could then assess the relative risk of each of the TPIs. The organization can apply different weightings to the attributes noted above, according to the organization's risk appetite and compliance strategy. The application of the risk factors is flexible in the KPMG model and can be tailored to the specific risk appetites of clients.

Following the completion of the risk assessment process, the TPIs can be categorized by risk so that the appropriate level of due diligence can be performed. Depending on the risk profile of the TPI, the client may undertake the following measures:

- Deem that no further IDD is needed
- Perform high-level screening of sanctions/politically exposed persons (PEPs), perhaps with a negative media search
- Perform enhanced desktop due diligence
- Perform full, in-country due diligence investigative procedures
- Cease the relationship with the TPI.

Typical features of a well-designed TPRM process

- Centralized, transparent workflow that tracks end-to-end due diligence requests in real-time and tracks handoffs across various roles (client's business sponsor, TPI representative, client compliance, and other configurable roles).
- Automates and stores TPI information through a Web front end, available to internal client personnel and external users as determined appropriate.
- Enables end-to-end visibility through real-time reporting and configurable dashboard capabilities.
- Facilitates a globally consistent approach to intermediary due diligence across client footprints (configured to multiple languages).
- Provides the capability to conduct risk analysis based on an established risk model and assigned scores.
- Enables a full-featured mobile capability across the user community.

3 Conducting the appropriate level of integrity due diligence

KPMG professionals can help clients to identify the appropriate level of due diligence for TPIs, based upon such factors as jurisdictional risk, the nature of the industry and the service provided, the importance of the relationship, etc. They can help create cost-effective, timely, and responsive reporting. The risk criteria is set in accordance with the client's policy to drive consistency of application across its portfolio of third parties. Further, based upon the results of such tier-structured reporting, they can assist clients to undertake further inquiries around the world if needed.

Perform enhanced desktop due diligence

KPMG's Corporate Intelligence professionals have developed Astrus, a digital solution designed to find information relevant to assessing the risks inherent with conducting business with a particular third party. Astrus reports cover an extensive range of global online public data records, including global sanctions and regulatory enforcement lists, corporate records, court filings, press, media, and Internet sources. Astrus offers a consistent, scalable and cost-effective solution to due diligence needs.

Astrus has been designed and built in response to clients' needs to maintain accurate and up-to-date reference information, for a variety of compliance purposes. Astrus provides risk-based integrity due diligence solutions responsive to regulatory guidance and client risk profiles. Astrus also provides clients with a secure Web portal hosted in KPMG's Forensic data center, through which clients can set monitoring profiles according to their compliance needs. Astrus can provide:

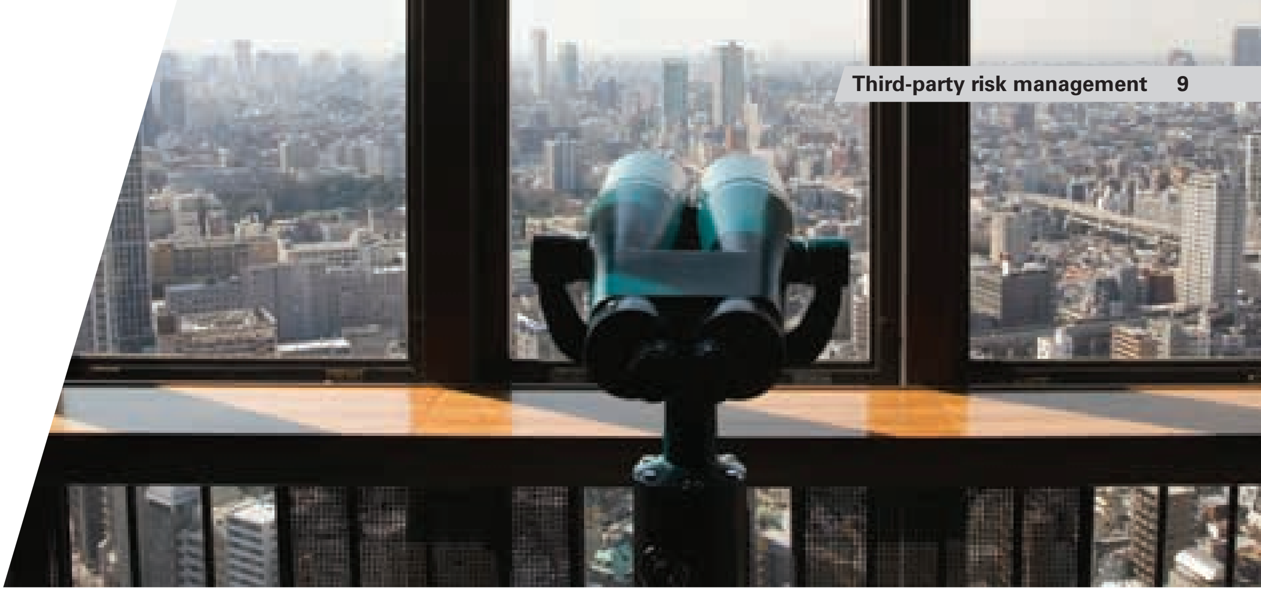
- An understanding of a third party's owners and shareholders; corporate structure and operations; reputational issues, including allegations in the public record or media; criminal and/or civil litigation, as available in a given jurisdiction; persons or companies that are sanctioned; PEPs
- Owner and management team profiles for criminal background (as available), litigation, business background and biographical data, reputational information, sanctions
- A clear and concise summary of key findings and possible risks, highlighted with traffic light indicators
- An objective assessment of facts related to integrity risk issues
- Cost-effective information regarding third-parties, with turnaround times usually of about five business days
- English and local language information and quality assurance reviews

Astrus allows for robust and targeted due diligence reports that are responsive to the assessed risk-ranking of third-party relationships.

Perform high-level screening of TPIs for sanctions/PEP

For TPIs with a lower risk profile, KPMG firms offer a lower cost targeted process of high-level sanction and PEP screening only. These targeted procedures can include a search of such databases as:

- The US Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals List and other national lists of sanctioned persons and companies
- The US Excluded Parties List for the Office of the Inspectors-General and commercial debarments
- US state-specific regulating bodies for licensing and sanctions
- Leading aggregators of sanctioned parties to identify sanctioned parties, state-owned companies, government officials, and other PEPs
- Global media for potentially adverse reputational information.



The Astrus solution accesses tens of thousands of individual data sources worldwide. These include premium content data sources and deep Web sources:

ASTRUS SOURCES OF INFORMATION	TYPICAL BENEFITS OF THE KPMG APPROACH
Premium content data aggregators (e.g., Bloomberg, Dow Jones Watchlist, etc.)	Access to multiple and iterative third-party data aggregators to cast a broad net for results. KPMG is data-source agnostic, and continually adds new data sources.
Deep Web content (e.g., behind passwords, firewalls, or requiring user search terms)	Uses proprietary technology to search Web content not indexed via traditional search engines. Through the global KPMG Corporate Intelligence network, relevant data sources are constantly updated.
Surface Web content (e.g., not requiring log-ins or form submission)	Uses market-leading search technology to create searchable indexes of relevant information sources. Content that is critical to the index (e.g., OFAC Specially Designated Nationals list) is updated every 24 hours.
Non-English language sources	Astrus covers major European languages and other languages such as Russian, Chinese and Arabic. The search technology indexes data in over 88 languages.
KPMG independent research	A wider reach than individual data vendors. It identifies and uses primary data sources wherever available in preference to secondary data sources. Astrus takes into account the reliability of information sources when assessing risk indicators.

Perform full in-country due diligence investigative procedures

Sometimes even the most sophisticated online due diligence isn't enough. Organizations may elect to undertake an in-depth IDD of a TPI, based on its preliminary risk rating, jurisdictional limitations and other previously identified risk factors. Alternatively, based on the findings of earlier due diligence (including a high-level screening or a full Astrus report), the client may seek additional procedures to clarify the findings, address gaps or inconsistencies, or examine relationships more closely.

KPMG's global network of Corporate Intelligence and other Forensic professionals can undertake an in-depth IDD that typically consists of targeted procedures combining deep desk research and field investigations to retrieve documents and information, conduct interviews and site visits. KPMG's network of professionals can assist with prospective business partners and with local jurisdiction sources that may include business and commercial contacts, current or former associates of the TPI, etc. They may also contact colleagues in relevant jurisdictions who have in-country subject-matter experience of political, government and business practices.

4 Ongoing monitoring of certain TPIs

Astrus Monitoring offers automated monitoring of trusted external data sources to alert you to information changes that impact your risk assessment of third parties with whom you do business. Astrus Monitoring can provide a precise and highly configurable system, capable of integrating and monitoring data from multiple information sources. Astrus Monitoring has been specified and built in response to clients' needs to maintain accurate and up-to-date reference information, whether for Anti-Money Laundering (AML) or Anti-Bribery and Corruption (AB&C) compliance purposes. Astrus monitoring has been designed to offer a credible and cost-effective alternative to manual monitoring processes. Changing to an event-driven system can help reduce your ongoing compliance costs and alert you at an earlier date to critical customer and counterparty data changes.

How Astrus Monitoring can turn risk to advantage

- Astrus Monitoring is a technology-based system used to consolidate data from a wide range of primary data sources worldwide, such as corporate registries, regulators, stock exchanges and central banks. Additionally, Astrus Monitoring can be used to integrate leading data aggregators, such as Bloomberg or Bureau van Dijk, to extend information coverage. As required, we can build additional data source integrations to your specification.
- Astrus Monitoring is highly configurable, allowing you to specify which data sources and which data fields within these sources are monitored and at what frequency. Monitoring profiles can be customized to match your organization's Anti-Money Laundering, Anti-Bribery & Corruption or other compliance guidelines.
- Astrus Monitoring can introduce a high degree of conformity to your monitoring processes. It maintains a detailed audit and evidence trail including screen capture information and digitally signed reports to support regulatory compliance. A centralized process for specifying which data sources are used under what circumstances and at what frequency provides comfort that processes designed to address regulatory compliance are applied consistently.
- Astrus Monitoring provides alerting and escalation functionality to help your business ensure that critical changes are reviewed on a timely basis. Reporting dashboards and key performance indicator metrics can be extracted to help you manage your compliance risks effectively.
- Astrus provides a fully hosted and supported system. Data source integrations are maintained on your behalf. If data sources change, they will be updated within a short period. This reduces your risk that you are inadvertently relying on out-of-date information sources.
- Manual periodic reviews typically cover a large range of records to identify a relatively small number of relevant changes. As Astrus Monitoring precisely identifies these relevant changes as well as maintaining a full record of non changed records, you can potentially reduce your manual review effort, saving you time and money.

In summary

- Organizations are building third-party risk management programs in response to regulatory pressures, cost reduction programs and in an overall desire to reduce risk by better understanding who they are conducting business with.
- There are certain challenges with building out TPRM programs but they are outweighed by the potential savings and benefits.
- The use of appropriate technology can certainly make the process much more efficient, repeatable and controllable.
- Applying the appropriate integrity due diligence to the right risk profile is critical to a successful program.
- Program elements including risk factors and risk weightings can and should be tailored based on unique organization/industry circumstances.
- What you don't know about your business partners can hurt you… don't be caught off-guard.

Contact us

Peter Armstrong
KPMG in Canada
T: +1 416 777 8011
E: pearmstrong@kpmg.ca

Laura Durkin
KPMG in the US
T: +1 212 872 5779
E: ldurkin@kpmg.com

Nigel Layton
Partner
Forensic – Astrus & CI
KPMG in the UK
T: +44 20 76945012
E: nigel.layton@kpmg.co.uk

James Rose
Senior Manager
Forensic – Astrus & CI
KPMG in the UK
T: +44 20 76945671
E: james.rose@kpmg.co.uk

Marc Miller
KPMG in the US
T: +1 212 872 6916
E: marcmiller@kpmg.com

Graham Murphy
KPMG in the US
T: +1 312 665 1840
E: grahammurphy@kpmg.com

kpmg.com/astrus

kpmg.com/app

Download on the App Store

Designed by Evalueserve.
Publication name: Third-party risk management
Publication number: 130525
Publication date: August 2014