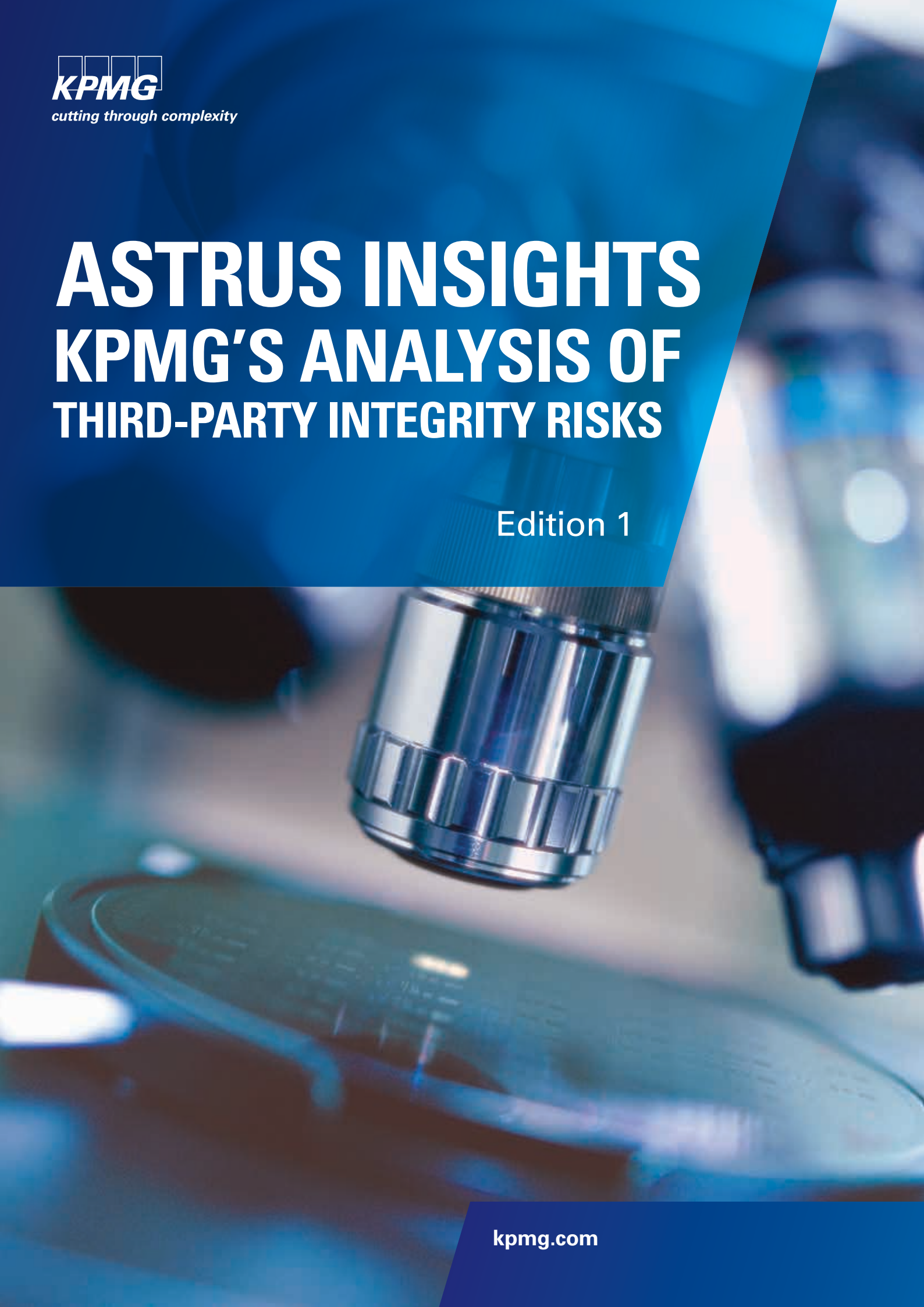
KPMG
cutting through complexity

ASTRUS INSIGHTS
KPMG'S ANALYSIS OF THIRD-PARTY INTEGRITY RISKS

Edition 1



kpmg.com

KPMG's analysis of third-party risk provides valuable insights from nearly 8,000 integrity due diligence reports covering 172 countries. This is the first edition in a planned series of publications considering third-party integrity risk.

Contents

The **big** picture

Global transactions and regulatory scrutiny increasingly require firms to examine their business relationships in order to assess risk, undertake informed negotiations, and comply with regulatory mandates. Failure to adequately evaluate clients, vendors, agents and business partners, and to know how they operate, can expose organizations to reputational damage, operational risk and government investigations, as well as monetary penalties and potential criminal liability.

In this first edition of Astrus Insights, KPMG International has analyzed the findings of around 8,000 integrity due diligence reports that our member firms have conducted on third-parties across the globe to understand what lessons can be learned about the nature of risks to which organizations are exposed through their third-party business associations.

The results of the analysis of these reports challenge some of the widely held assumptions about due diligence practices and the nature of third-party risk.

The key findings from the analysis is that over 20 percent of subjects were given an overall risk rating of red, meaning they were associated with significant risks (such as allegations or incidences of corruption, fraud, money laundering or other unethical or illegal practices). Sixty-six percent of reports were rated amber overall, meaning risk issues were identified, but these were not necessarily serious (such as opaque ownership structures; association of the subjects with politically exposed persons; significant involvement of the subject in civil litigation). Only 12 percent of reports received a green rating and the "all-clear" from an integrity risk perspective.

> "Failure to adequately assess clients, **agents and business partners**, and to know how they operate, can expose organizations to reputational damage, operational risk and **government investigations**, as well as monetary penalties and potential **criminal liability**."

ANALYSIS OF THIRD-PARTY RISK

23%
66%
12%

Note: The total number of reports included in the analysis was 7,824.

Significant integrity risk identified with the subject(s) of the report

Potential integrity risk identified with the subject(s) of the report

No integrity risk identified with the subject(s) of the report

Source: Astrus Insights, 2013

Astrus approach to **integrity** due diligence

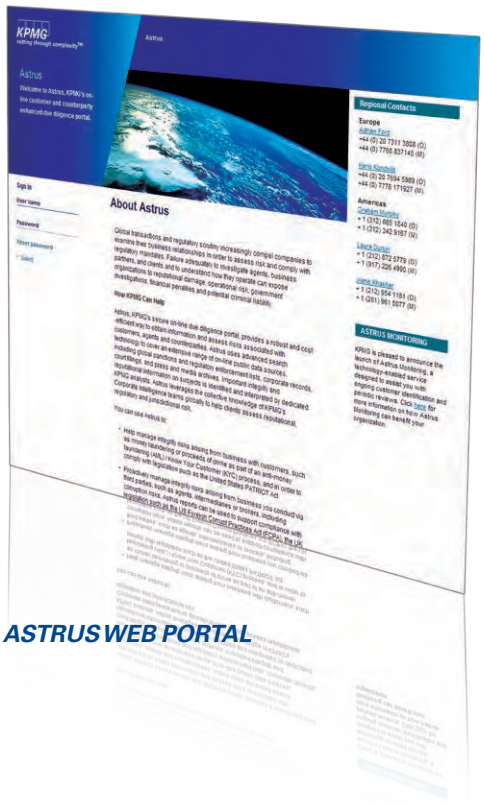
Astrus integrity due diligence draws on an extensive range of public information sources across the world and includes analysis by experienced Corporate Intelligence specialists. Integrity risk factors are categorized according to the company or individual's background details; shareholders; directors; adverse press and media comment; litigation; exposure to sanctions, Politically Exposed Persons (PEPs) and published lists of high risk entities. Each risk factor is weighted as green, amber or red according to the significance of integrity risks identified. This analysis extracts data from integrity due diligence reports, including risk flag indicators, split by report subject, industry and geographical region. We have further analyzed key terminology to determine the types of risks identified in the reports.

Among other reasons, organizations typically commission Astrus integrity due diligence reports to fulfil their due diligence requirements in relation to compliance with anti-bribery and corruption laws and anti-money laundering regulations. Other potential uses include supplier risk assessments, transaction due diligence and due diligence on senior executives.

Astrus Insights compares empirical findings from completed due diligence reports with views expressed by regulators responsible for overseeing organizations' compliance with legal requirements.

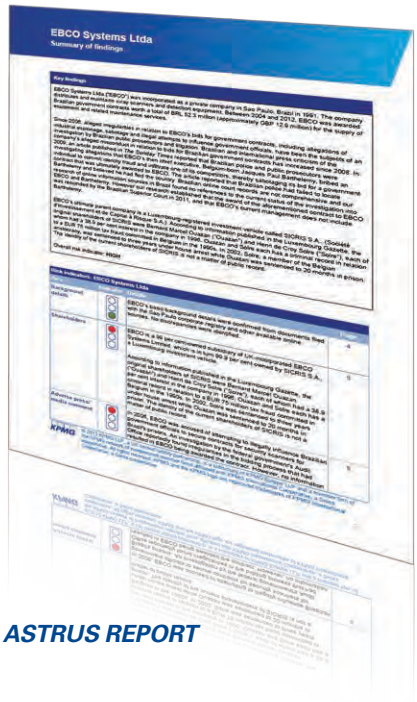
You can find out more about Astrus at the end of this document.

> "This analysis extracts data from integrity due diligence reports, including **risk flag indicators**, split by report subject, industry and **geographical region**."



ASTRUS WEB PORTAL

REPORTING DASHBOARD



ASTRUS REPORT

9/10

"Nearly **9** out of **10** integrity due **diligence** reports identified some kind of **risk** that warranted review and **23 percent** of reports **analyzed** had an overall risk rating of red."

FS is risky business

Analysis of the reports by sector shows that the Financial Services (FS) sector presents by far the highest third-party integrity risks. Over 40 percent of all reports in the FS sector were rated red. Analysis of the most alarming reports in our population (reports that included serious risks in four or more categories), revealed that 90 percent had been completed for banks and that 60 percent were on subjects in the banking sector. FS companies need to take extra care with due diligence or they could open themselves up to significant risks.

Prevalence of risk

Nearly 9 out of 10 reports identified some kind of risk associated with the third-party that warranted review and 23 percent of reports analyzed had an overall risk rating of red, suggesting an association with the third party could give rise to serious legal, reputational or commercial risks. With the continuing trend for regulators and consumers to hold companies accountable for the actions of their third-parties, organizations cannot afford not to do their due diligence.

Individuals present most risk

Restricting screening (typically against sanctions and Politically Exposed Persons (PEP) lists, and negative media searches) to just the name of the organization will miss the majority of potential risk flags. Our analysis shows that individuals and not organizations present the highest level of risk. Where the subject of a report was an organization, in 84 percent of cases an elevated risk was caused by negative information on the directors or shareholders of the business.

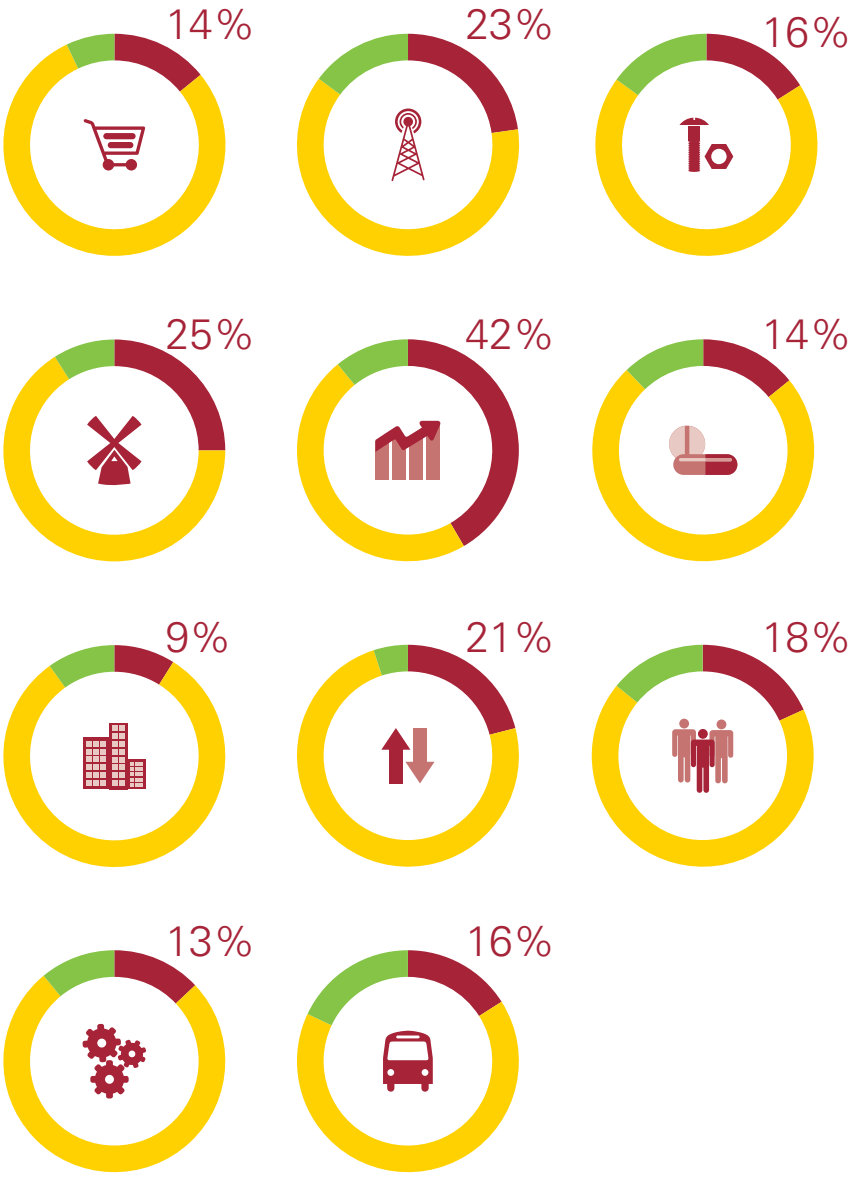
High bribery and corruption risks in certain non-FS sectors

Three other sectors – Technology, Media and Telecommunications (TMT); Energy, Natural Resources and Chemicals (ENRC); and Miscellaneous (general trading companies, for example) – present particularly high risks, with over 20 percent of reports rated red. In 30 percent of these reports, bribery or corruption were key determining factors for risk. All regions, including offshore financial centers, were represented, with Western Europe featured largely as result of a focus by regulators on anti-bribery and corruption.

Fraud is the number one risk

Our analysis shows that the most prevalent risk uncovered by our due diligence is fraud associated with the third-party. More than any other type of risk, account for the highest number of red-rated reports. Fraud risk is followed by bribery and corruption, money-laundering, regulatory violations, business disputes and sanctions. This holds true across 7 of the 11 industry sectors analyzed.

ANALYSIS OF THIRD-PARTY RISK BY SECTOR



CM	Consumer Markets
TMT	Technology, Media and Telecommunications
DI	Diversified Industrials
ENRC	Energy, Natural Resources and Chemicals
FS	Financial Services
HLS	Healthcare and Life Sciences
IBC	Infrastructure, Building and Construction
MISC	General trading companies
PS	Public Sector
TBS	Technical Business Services
TLT	Transport, Leisure and Tourism

Significant integrity risk identified with the subject(s) of the report

Potential integrity risk identified with the subject(s) of the report

No integrity risk identified with the subject(s) of the report

Source: Astrus Insights, 2013

FS is risky
business

40%

Over 40 percent of reports on subjects in the FS industry are rated red. This industry is by far the most exposed to highest third-party risks at the moment.

20%

Three other sectors still present significant risks, with more than one in five reports rated red. In the ENRC sector, 25 percent of reports are rated red. TMT and Miscellaneous (general trading companies) also noted over a 20 percent risk of red flags.

10%

The Infrastructure, Building and Construction (IBC) sector, in comparison, had less than 10 percent red reports.

> The financial services **sector** stands out as the sector with the most **third-party risk**.

It was not only the subjects of the reports that showed that the FS sector posed the highest risks, but analysis of the clients ordering the reports also revealed a higher propensity for red flag reports amongst banking sector clients.

90%

of highest risk reports (reports that included serious risks in four or more categories) were completed for banks as part of their due diligence procedures.

60%

of highest risk reports were on banking subjects.

The types of risk exposed by these reports include fraud, corruption, insider trading, bad business decisions and negligence, leading to bankruptcy.

Case study

An international bank was reviewing a correspondent banking relationship in the Middle East. Research revealed that the bank's shareholders had been accused of corruption; the bank had allegedly conducted transactions for terrorist organizations; and had reportedly been involved in stock manipulation. The bank had been fined for deficient anti-money laundering controls and several of its directors were politically exposed persons. The majority of the investigations and allegations against the bank were identified through research in countries beyond the bank's country of operations and required an international review of litigation and blacklist checks, and full reviews of the bank's ultimate beneficial owners and directors.

The Astrus due diligence report identified a number of critical red flags that may otherwise have gone undetected, including significant concerns over the subject's level of regulatory compliance that may not have met the standards required by the banking client.

What the **regulators** say

What do banks need to be doing?

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 intermediaries.

In the UK, the Financial Services Authority (FSA) (supersede by the Financial Conduct Authority) identified that most firms rely heavily on an informal 'market view' of the integrity of third-parties and very basic checks, such as printing the third party websites.

The FSA noted that three quarters of banks failed to take adequate measures to establish the legitimacy of the source of wealth of customers who are PEPs. More than a third of banks failed to put in place effective measures to identify PEPs and over half the banks failed to carry out robust due diligence in high risk situations.

In our experience, irrespective of whether the customer is a PEP or not, an objective assessment of the source of wealth, source of funds and business activities is a critical aspect of due diligence.

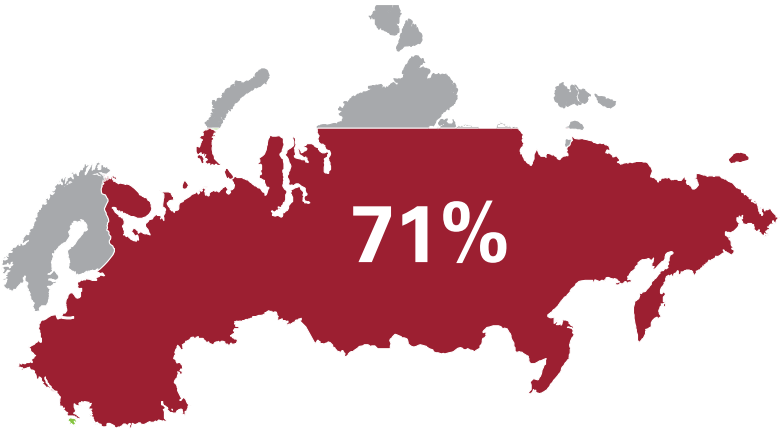
In recent action against a major international bank, the US Financial Crimes Enforcement Network (FinCEN) noted that the bank had failed to conduct adequate due diligence on certain foreign correspondent accounts as required under the US Bank Secrecy Act.

A record fine was imposed on the bank by the US Department of Justice as settlement for the charges of money laundering. The Department of Justice alleges that bank had failed to conduct any due diligence on some of its account holders, in large part contributing to the money-laundering scandal.

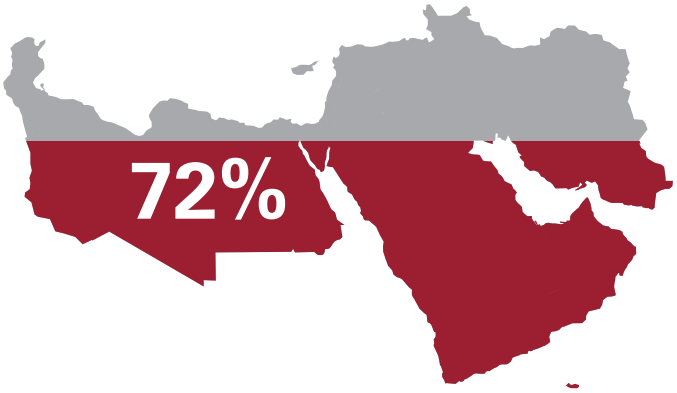
Our results confirm that financial services companies need to take extra care with due diligence or they open themselves up to significant risks.

Hotspots for Financial Services risk

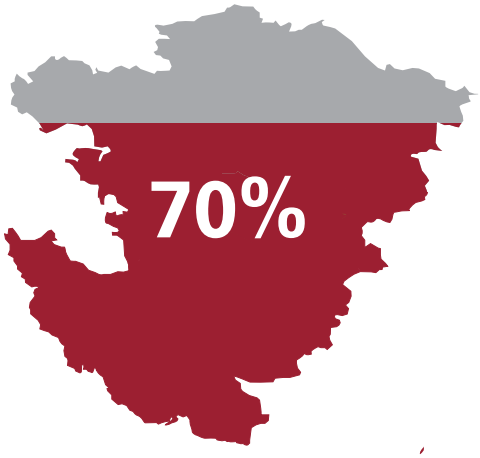
Further analysis of the red rated reports by region and sector tells us more about the hotspots for third-party risk. In the FS sector, there are three geographical regions that stand out: 71 percent of reports covering Central and Eastern Europe (including Russia) along with 70 percent of Central Asian reports and 72 percent of Middle East and North Africa reports were rated red.



Central and Eastern Europe



Middle East and North Africa



Central Asia

Source: Astrus Insights, 2013

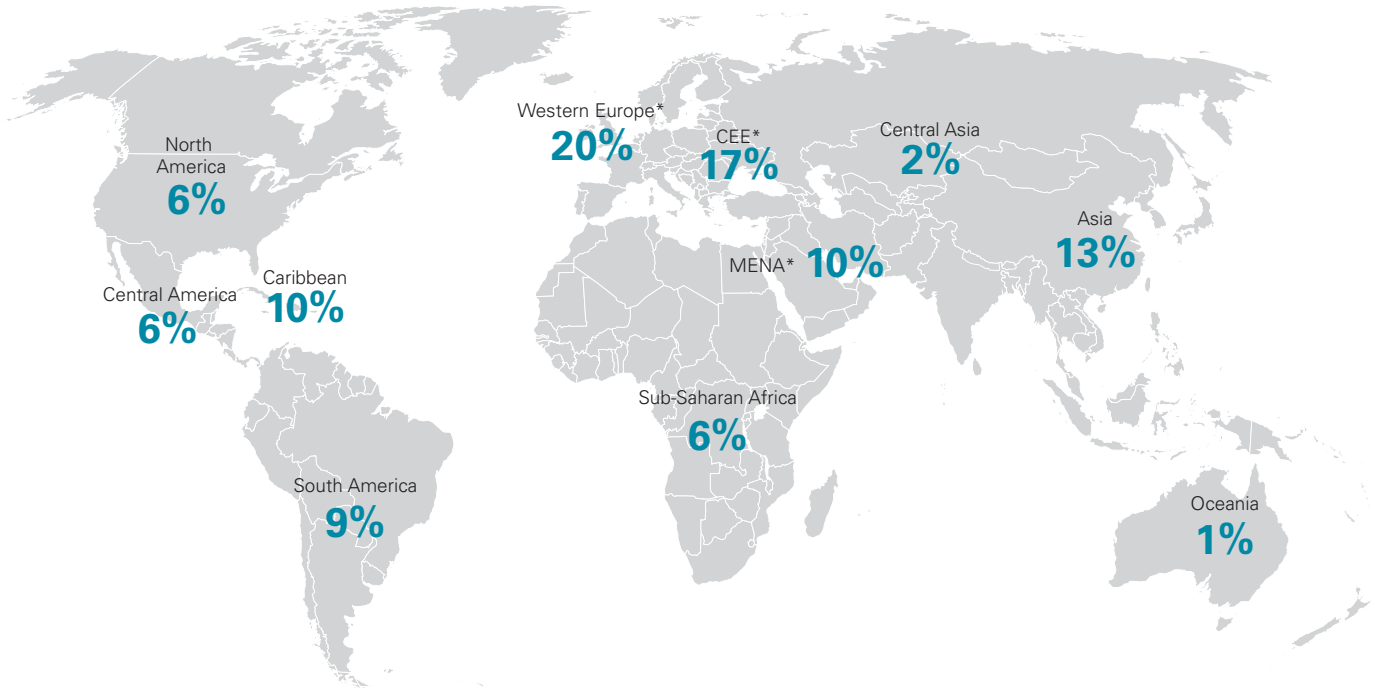
Bribery and corruption a **key risk** in non-FS sectors

In three non-FS sectors **red flag reports** account for more than 20 percent of the total:

Red flag reports linked to keyword terms **'bribery'** or **'corruption'** in these sectors:

*'Miscellaneous' sector includes general trading companies and smaller businesses not obviously aligned to a specific sector

Distribution[1] of red flag reports by jurisdiction for these three sectors.



* Western Europe includes a number of organizations that have been subject to regulatory action under the US FCPA and other anti-bribery legislation.
*CEE represents Central & Eastern Europe
*MENA represents Middle East & North Africa

[1] Obviously impacted by the number of reports requested for the said regions.

Source: Astrus Insights, 2013

What the **regulators** say

What organizations need to be doing

There is clear evidence that regulators see a need to focus on the individuals behind the organization; after all, bribes are paid and received by individuals, not legal entities. The US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act and other similar pieces of legislation can hold individuals accountable for corrupt practices. Individuals can face significant fines and imprisonment if found guilty of bribery and corruption.

The indictment of eight senior executives of an international engineering company under the FCPA in December 2011 demonstrated that the enforcement activities of the FCPA are intended to focus on individuals as much as companies. The indictment charged the defendants with bribing Argentinean government officials in return for a contract. The individual executives of the company may have thought they were in the clear as in 2008 the company and its Argentinean subsidiary settled charges that included bribery of the Argentinean government officials.

If your third-parties are individuals or agents acting on your behalf, remember that the majority of recent enforcements under the FCPA have been in relation to acts carried out by agents or intermediaries, which have had serious repercussions for the companies concerned.

The Astrus Insights analysis provides a clear indication that companies need to better manage the risks associated with their third parties. More specifically, companies need to:

1. Understand the universe of their third-party relationships and perform risk analytics on them to determine those that would be in scope for further review.
2. Execute a risk assessment and process to determine appropriate levels of review on those third-party intermediaries (TPIs) where further information is required;
3. Based on the assessment, perform appropriate risk-based due diligence to obtain the critical information that can help in managing business risk.

> **73 percent** of respondents found **performing** effective due **diligence** on foreign third-party intermediaries **challenging** or very challenging.

KPMG's Global anti-bribery and Corruption Survey 2011

> **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 US Foreign Corrupt Practices Act | November 2012

Case study

A US firm was looking for a way to manage its logistics in Russia and was referred to a customs broker. On the surface, the company appeared to have a good reputation and had not been referenced in sanctions or blacklist checks. The firm's main contact point at the company, the general director of the customs broker, had a good reputation. However, further investigation revealed that the shareholders were caught up in allegations that they had paid bribes to customs officials and had faced various administrative fines through other businesses. They were also embroiled in litigation in the US as a result of their activities there and were suing their business partner for fraud.

Intermediaries and agents involved in customs clearance activities are generally considered higher risk and warrant enhanced due diligence, even if it is indicated that they have a good reputation.

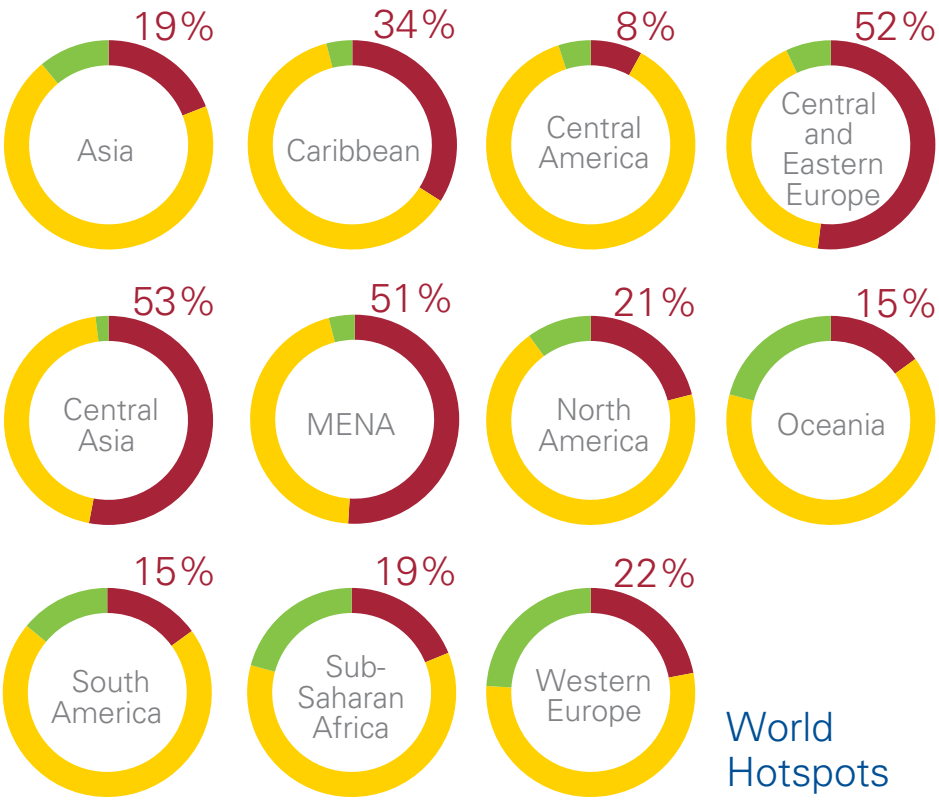
Proportion of **red rated** reports by **sector** and **sub-region**

Sub region versus sector	CM	TMT	DI	ENRC	FS	HLS	IBC	PS	TBS	TLT
Asia	14%	12%	15%	12%	46%	15%	8%	22%	2%	16%
Caribbean	22%	48%	25%	38%	33%	25%	34%	25%	56%	39%
Central America	4%	15%	2%	20%	35%	4%	3%	5%	16%	9%
Central and Eastern Europe	25%	43%	27%	48%	**71%**	36%	26%	71%	8%	21%
Central Asia	-	33%	-	60%	**70%**	40%	-	-	-	33%
MENA	22%	18%	20%	43%	**72%**	24%	36%	63%	30%	54%
North America	33%	15%	2%	15%	27%	14%	16%	63%	29%	28%
Oceania	-	-	17%	22%	26%	-	-	25%	-	9%
South America	13%	23%	19%	31%	31%	10%	8%	6%	4%	13%
Sub-Saharan Africa	19%	22%	19%	28%	45%	9%	7%	13%	13%	9%
Western Europe	19%	23%	22%	30%	25%	8%	21%	23%	14%	14%

Subjects in the Financial Services sector have a particularly high likelihood of association with risk in Central and Eastern Europe, Central Asia and MENA; these subjects may be worthy candidates for enhanced due diligence.

Source: Astrus Insights, 2013

Analysis of risk by **geography**



Source: Astrus Insights, 2013

Western Europe, Oceania, South America and Sub-Saharan Africa, but interestingly not North America, are the only regions to achieve above average results for reports identifying no or low risk. The results for sub-Saharan Africa are slightly skewed by the fact that 50 percent of reports in that region were on subjects in South Africa.

Central and Eastern Europe (incorporating Russia), Central Asia and MENA stand out as the three regions posing the highest third-party risks. More than half of the reports in each of these regions were rated as red.

Russia remains a significant investment destination and area of interest for due diligence. The World Bank figures for foreign direct investment (net inflows) to Russia between 2008 and 2012 show that it received USD 207bn, or 3 percent of global foreign direct investment. Fifty-seven percent of our reports on Russian subjects were rated red, demonstrating a preponderance of red flags for Russian businesses.

Our analysis also indicates that country risk remains an important factor in determining the overall risk assessment of a third-party.

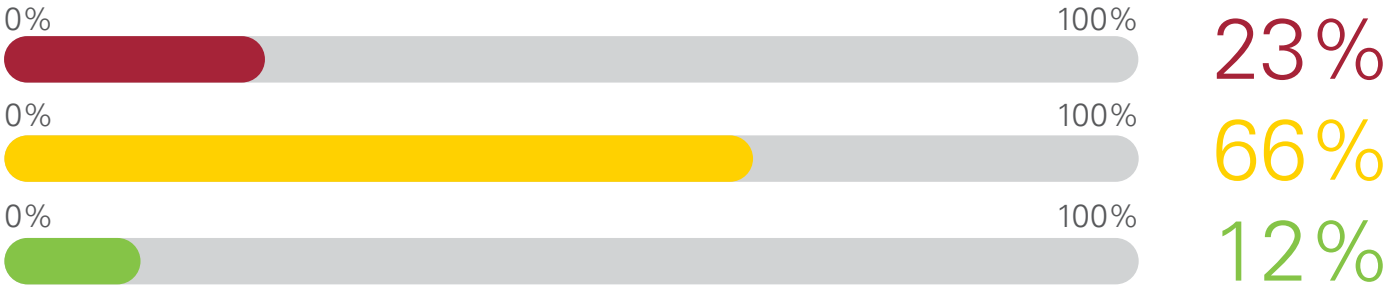
The transparency of information, including the freedom of the press and civil society, can have a big impact on the success of any due diligence and, where limited, may make effective identification of risk factors more difficult.

What makes **red, red?**

Our analysis of what makes a third-party a '**red**' risk provided some surprising results and challenged some widely held assumptions about the nature of third-party risk and how to manage third-party due diligence

FACTORS LEADING TO RED RISK RATING

ANALYSIS OF THIRD-PARTY RISK ASSOCIATED WITH THE SUBJECT OF THE INQUIRY



Breakdown of nearly 8,000 reports analyzed by overall risk rating

- Significant integrity risk identified with the subject(s) of the report
- Potential integrity risk identified with the subject(s) of the report
- No integrity risk identified with the subject(s) of the report

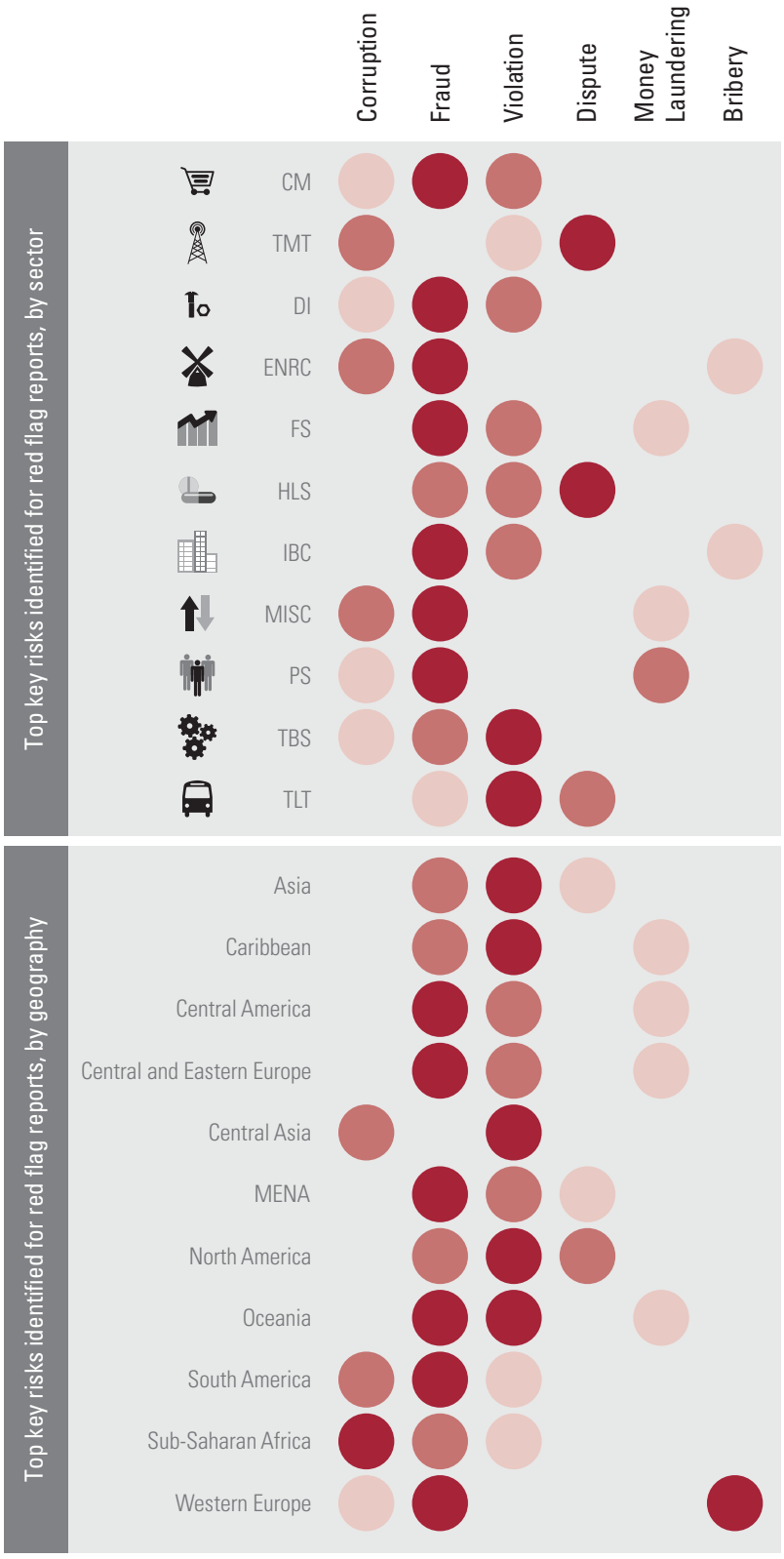
Source: Astrus Insights, 2013

Fighting **fraud**

> **Our analysis** shows that the most prevalent risk to be uncovered from our due diligence is **fraud** associated with the **third-party**.

Key drivers for third-party integrity due diligence include the management of anti-money laundering and anti-bribery and Corruption risk. But what about fraud? Our analysis shows that the most prevalent risk uncovered by our due diligence is fraud associated with the third-party. This exceeds all other risks, including regulatory violations, bribery and corruption, money laundering, business disputes, sanctions and PEP associations. Financial fraud has hit record highs (see KPMG's Fraud Barometer 2013*). Our findings show there are clear benefits to using due diligence to identify potential fraud risks.

Many of the risks identified on red rated reports were a result of fraud allegations or investigations directly linked to the third-party. Fraud risks are high across the majority of sectors and geographies.



Our results correlate with what we know about increases in fraud risk

- The most common key word in the executive summary of a red rated Astrus report
- The second most common key word in the executive summary of a red rated Astrus report
- The third most common key word in the executive summary of a red rated Astrus report

Source: Astrus Insights, 2013

* KPMG's Fighting Fraud website:
http://www.kpmg.com/uk/en/services/advisory/risk-consulting/services/forensic/fighting-fraud/pages/default.aspx

Fraud impact

A fraud risk associated with a third-party has many implications, but understanding this early on in a relationship, through the due diligence process, enables organizations not only to avoid damage to their reputation, but to more accurately assess the transactions contemplated through a relationship. For example, if you are looking at an agent, what controls and remunerations are appropriate for the services provided? This is a question a good due diligence exercise should help you address.

Our findings show that fraud risk is not affected by geographical location, industry type or third-party activity: it is prevalent across all situations, including some that may be deemed benign based on a basic risk assessment.

Early due diligence will help organizations fulfil their regulatory requirements, but may also highlight commercial risks, including potential fraud by a third party.

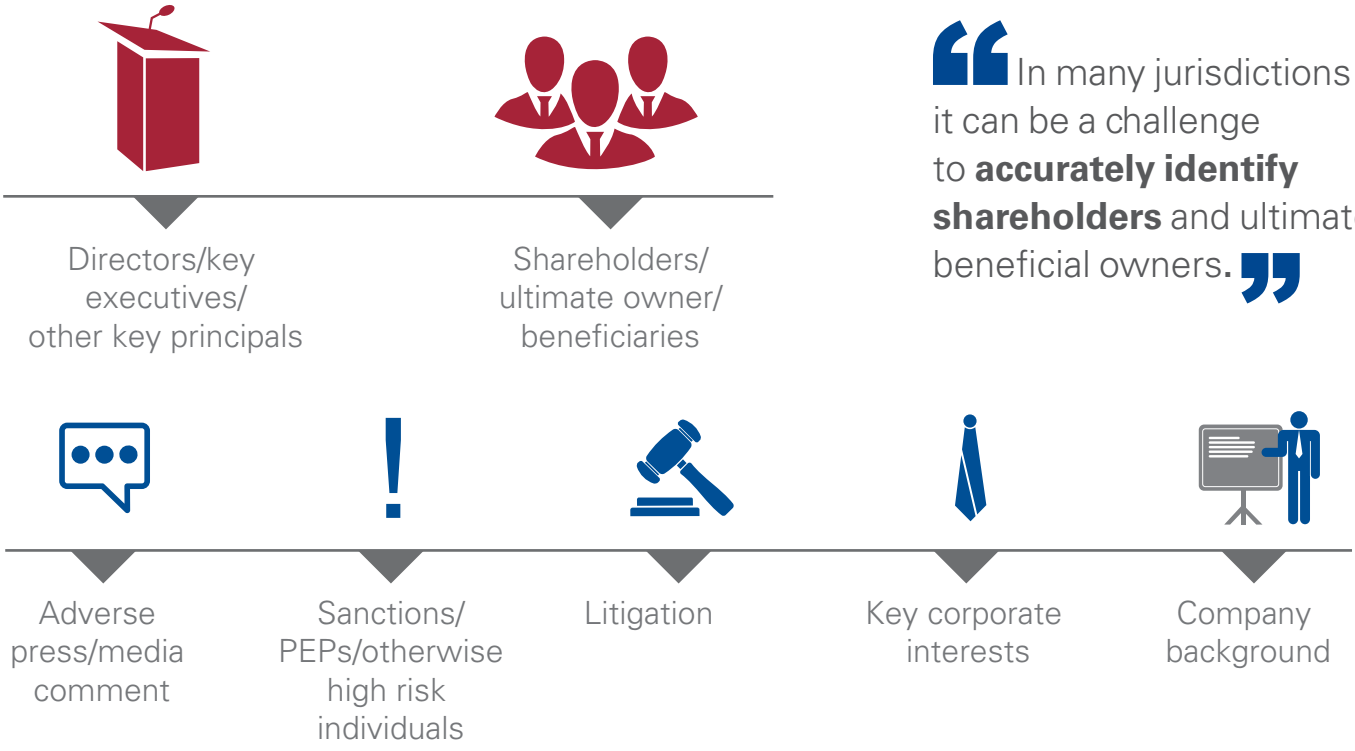
Case study

A UK-headquarted firm in the transport industry was dealing with a UK-based manufacturer of logistics and lifting equipment. Research of the shareholder structure of the company, regional and national press, and litigation records revealed that the shareholders of the business had been accused of serious fraud and of orchestrating a £4m shortfall in their former business by falsifying invoices for stock that was never delivered. Former business partners were now pursuing a claim for damages against the shareholders of the firm's supplier and the shareholders were involved in a variety of lawsuits that the firm was not aware of.

This case illustrates that firms can be exposed to fraud risks through third-party relationships in any situation. Timely identification of these risks through effective due diligence can help prevent a company from getting involved in a relationship that could pose serious commercial and financial risk.

People pose the **highest risks**

As well as types of risk uncovered, our analysis considered the underlying factors behind red-flagged reports. The two most significant factors were negative information identified against either the directors or the shareholders/ultimate beneficial owners (UBOs) of the third party.



Source: Astrus Insights, 2013

> "In many jurisdictions it can be a challenge to **accurately identify shareholders** and ultimate beneficial owners."

The findings clearly demonstrate that third-party due diligence that is focused solely on the subject organization, and not its principals and shareholders, misses the majority of risks: it is the people behind the organization that really matter and this is the single largest risk factor.

In many jurisdictions it can be a challenge to accurately identify shareholders and ultimate beneficial owners (UBOs). The information is often not readily available in corporate filings, or the use of proxy or nominee shareholders or bearer shares confuses matters.

Higher risk organizations (such as trusts, foundations, international business corporations registered in tax havens or special purpose vehicles) may have no or negligible independent identity. Piercing the corporate veil beyond the immediate third-party entity and any nominee owners or directors to identify UBOs is essential.

It is also important to recognize when a stated owner is not the true beneficiary, as this defeats the benefits of screening the UBO for adverse press/media, government associations and against sanctions lists.

In our experience, due diligence is only truly effective when adequate information is obtained to prove who the UBO is who they claim to be. Typically, this requires an iterative research process and the use of a variety of sources to follow up on information around ownership.

> "Does your due diligence process accurately capture who the key shareholders and directors of the company are, including **ultimate beneficial owners?**"

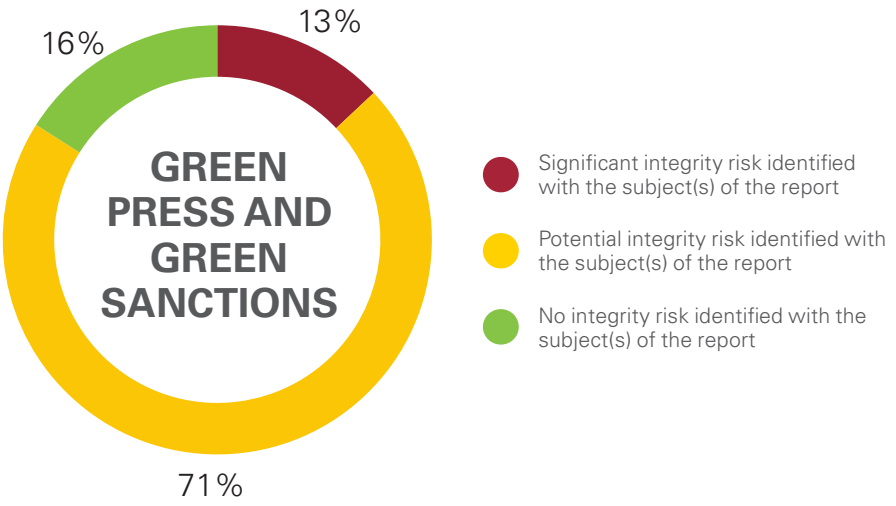
What's missing from an **internet search?**

If your third-party due diligence policy is based on sanctions and press searches alone, **you are missing a huge 84 percent of potential integrity risks**.

This is explained by the following analysis: if a report is rated green for press (in other words, there is no negative news in press and online media sources on the subject) and green for sanctions, then there is only a 16 percent chance the overall rating for the third party will be green, if other factors are taken into account. By considering other factors, such as scrutiny of the background details of the organization, its shareholders, directors and litigation information, there is a 71 percent chance it will be rated amber risk and a 13 percent chance it will be red.

Organizations will often start their third-party due diligence with a basic sanctions check. Even combining press searches with sanctions checks may not identify key risks. Technology and automation play an increasingly important role in the third-party due diligence process, but ultimately a degree of manual and iterative research is required in many jurisdictions to accurately capture risks. Organizations will need to go beyond a standard screening solution, which typically just incorporates sanctions and press checks.

> "The analysis shows us that sanctions and press checks alone miss '**red flag**' risks."



Source: Astrus Insights, 2013

Case study

Consider these two separate cases. In one case, a firm was reviewing a warehousing and logistics supplier in central Europe: the subject organization was given the all-clear for press and sanctions checks, and there was no adverse press in relation to the directors and shareholders of the business. However, a search of litigation and corporate filings identified the company was in serious financial difficulty, following a petition for bankruptcy by its creditors. The organization had several legal cases pending but the client was not aware of these.

In the second case, an oil and gas firm had been recommended a joint venture partner in a central African country. The company appeared to have the requisite track record, some well-known international customers, and was endorsed by local and international players in the oil and gas market. However, due diligence uncovered that the UBOs of the company were all politically exposed and had been accused of corruption and embezzlement of funds and been linked to arms smuggling scandals. The seriousness of the allegations caused the firm to re-evaluate the recommendation it had received.

About **Astrus**

Astrus is KPMG's cost-effective, proactive due diligence solution that helps you obtain information and assess risks associated with third-parties, such as customers, agents and other business partners.

VALUE FOR MONEY

Astrus reports are prepared on demand. Instead of overwhelming you with raw data, they offer concise, fully sourced, digestible summaries highlighting key issues so that you can focus on those that warrant the most attention.

UNCONSTRAINED DATA SOURCES

KPMG is data source-independent. We use the substantial collective experience of our firms' global Corporate Intelligence teams. We review an extensive range of over 40,000 data sources, which we carefully evaluate to determine the reliability and consistency of the information we gather.

SCALE AND CONSISTENCY IN A CUSTOMIZABLE SERVICE

KPMG offers a truly scalable service. Our firms have prepared thousands of Astrus reports on subjects in more than 170 countries. Our risk grading approach is tailored to your organization's risk appetite and is consistently applied across your portfolio.

INSIGHT. NOT BOX-TICKING

When do discrepancies or contradictions matter? When should the absence of information itself be a source of concern? Astrus analysts are trained in KPMG's global Corporate Intelligence methodology. KPMG also offers full-scope integrity due diligence investigations and on the ground Forensic investigations as required.

Contact us

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

Adrian Ford
KPMG in the UK
T: +44 20 7311 3808
E: adrian.ford@kpmg.co.uk

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

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

kpmg.com/astrus

Designed by Evalueserve.
Publication name: Astrus Insights
Publication number: 130374a
Publication date: August 2013