ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Conducting Enhanced Due Diligence Investigations in China

Compliance and Ethics

With increased regulatory scrutiny by US and Chinese authorities, and sustained effort by the Chinese government to stamp out public corruption, companies can no longer view conducting third-party due diligence as an avoidable cost. Risk-based due diligence is no longer an optional "nice to have" for companies that plan to conduct business in China.

As organizations review their third-party compliance program, it is important to ask the following questions: What level of due diligence is appropriate for each third party? What factors and process should a company consider when identifying which third parties present the highest level risk, and therefore the most thorough level of due diligence? What kinds of information are legally available to conduct due diligence?

Identifying a third party's compliance risk

Similar to the West, relationships facilitate business in China. However, the Chinese practice of guanxi – networks of interpersonal relationships and a web of favors given and received – complicates the operating environment, and by its very nature, increases the probability for bribery and corruption to occur.

The existence of guanxi coupled with data provided in a 2013 Corruption Perceptions Index by Transparency International that ranks China 80th on a list of 177 countries justifies caution and additional, more stringent due diligence of Chinese third parties.

The first step in the third party due diligence process involves determining whether a company can identify within its internal systems the population of third parties that may represent a corruption risk. For companies with disparate systems or no systems at all, this may be more difficult than for companies with an all-encompassing system.

The next step is to identify the types and categories of third parties and the relative corruption risk associated with those relationships. Broadly, the types of entities to consider include customers, vendors and third-party intermediaries. Examples of third-party intermediaries include distributors, agents, franchisees, joint venture partners and sales representatives.

Ideally, that information already exists in a third party compliance management solution that compiles data associated with each third party. Such technology facilitates a systematic approach that helps automate the risk-modeling process. It removes subjectivity, ensures consistency, reduces risk, and ultimately supports a credible and defensible third-party compliance program.

Automating the risk modeling and third party compliance process produces true risk-based due diligence that fully considers relevant data gathered for each third party. Such an automated approach, if properly done, will prescribe the appropriate level of due diligence to be conducted on individual third parties as well as automate due diligence questionnaires and anti-corruption declarations and training.

If a company does not have a centralized third-party solution in place, they must gather third party data from multiple sources such as the compliance department, in-country managers, and the internal audit function, as well as the Enterprise Resource Planning system(s).

With third-party data in a single location or platform, the next step involves determining the type and

purpose of the relationship by asking a series of questions such as: why the company engaged the third party, the closeness of the relationship between the company and the third party, the degree of control over the third party, whether potential funds that could be used for improper purposes are involved in the relationship (rebates, commissions, discounts, etc.), and whether the third party will interact with foreign government officials or foreign government instrumentality officials on the company's behalf.

The challenges of conducting due diligence in China

The language barrier is the first and most obvious challenge that a multinational faces. On that basis alone, companies engaging third parties should consider hiring a firm with staff that are fluent in Mandarin, English and Cantonese (if applicable) – in written and spoken form – to assist with the third-party due diligence effort.

Effective third-party due diligence depends on access to data. Current Chinese law is silent on the legality of private investigations such as the investigation of third parties. Yet, if the Chinese authorities believe that an investigator broke the law, they may arrest them for doing so; the difficulty for the investigator is knowing when he or she may be breaking the law. And some local governments such as that of Beijing tend to limit activities of firms conducting private investigations – especially those conducted by small entities operating as a "consulting company."

In the course of conducting due diligence, an inexperienced investigator may trigger the attention of the authorities, and, in turn, the government may contact the company that requested the due diligence to explain the investigator's actions. In the long-term, running afoul of Chinese law, even accidentally, does not bode well for a multinational that plans to conduct, or is conducting business in China.

China data privacy laws and regulations

Access to relevant, timely and accurate data poses a separate set of problems. Unfortunately, China does not maintain a centralized public records office that companies can readily access and gather data about their third parties. While China's data privacy is not as evolved as other countries, there are over 10 laws and regulations in place that include provisions relating to the protection of personal information. As a rule, companies should only use legally obtainable data to conduct due diligence.

Given that China lacks an overarching data privacy law, borrowing concepts and definitions from mature laws can help minimize the probability of violating data privacy regulations. As an example, using the definitions for personally identifiable information included in US law in conjunction with the Safe Harbor Principles may help reduce the risk that a data controller (an individual, company, or entity that determines the purpose and manner in which data is processed) and data processor (an individual, company, or entity that processes the data on behalf of the controller) will violate the patchwork of Chinese laws.

In short, without local in-depth knowledge of the laws that may apply to a third-party due diligence, those involved in conducting due diligence can quite easily and inadvertently violate the law.

Types of data to gather during the due diligence process

Depending on the level of risk associated with a third party, the level of due diligence varies. For the

riskiest third parties, multinationals should conduct Enhanced Due Diligence (EDD).

To provide the most actionable information to ensure compliance with Anti-Bribery and Anti-Corruption regulations as well as minimize the risk of violating data privacy laws, only highly trained; multilingual investigators with extensive knowledge of anti-corruption laws and third party due diligence best practices should conduct EDD.

An EDD includes a site visit, review of public records, identification and analysis of business partners, and interviews to determine the third party's reputation. It also normally includes gathering the third party's business license, articles of association, and analysis of the operation and ability to provide the agreed upon goods and/or services.

In addition to concerns regarding the legality of an investigation and the data privacy laws that may apply, third parties may fabricate critical documents such as bank statements, invoices, and contracts in order to disguise or conceal questionable or illegal activity. The ability to detect altered and fabricated documents is a critical skill that often requires a local expert to uncover the telltale signs that others may miss.

The limitations of online research

For third parties that present a moderate risk, companies can conduct an Open Source Investigation (OSI) via online media, or for low risk third parties, a Global Database Check, which includes a review of watch lists. Although an OSI is suitable in many respects for third parties with moderate risk, it provides limited information.

As mentioned previously, the Chinese government does not have a centralized records office, consequently data such as personal details of shareholders, or annual financial data rarely exists online.

Finally, the accuracy and completeness of search engines that index Chinese content is not as refined as Google's approach. As a result, the information gathered via an OSI may appear valid and suitable for third parties with moderate risk, but companies should not rely on that approach for high-risk third parties.

Conclusion

Conducting Enhanced Due Diligence provides multinationals with critical intelligence regarding their third parties. In China, conducting EDD comes with its own set of risks.

Current Chinese law does not recognize nor ban private investigations, therefore, those involved in third-party due diligence must function within a 'gray area' of the law. Nonetheless, the Chinese authorities continue to impose restrictions on the establishment and operation of the private investigators.

While the country has a number of laws and regulations relating to privacy, China has yet to enact a law that covers all aspects of data privacy, including commonly accepted definitions and frameworks to handle the gathering, usage and dissemination of data.

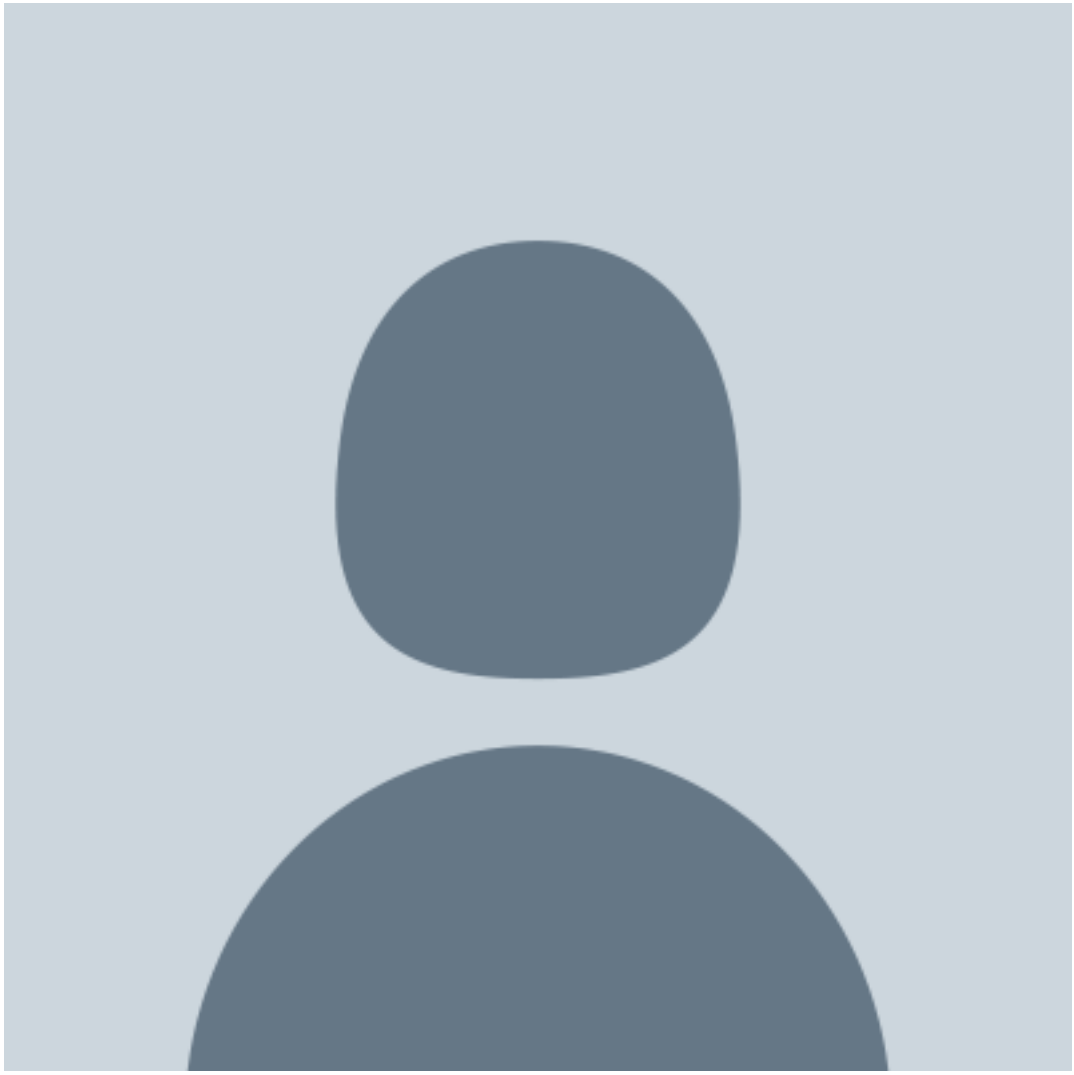
Given that China does not maintain a centralized public records office, without the ability to source

and gather certain key data legally, companies may face challenges assembling the data they need to conduct third-party due diligence.

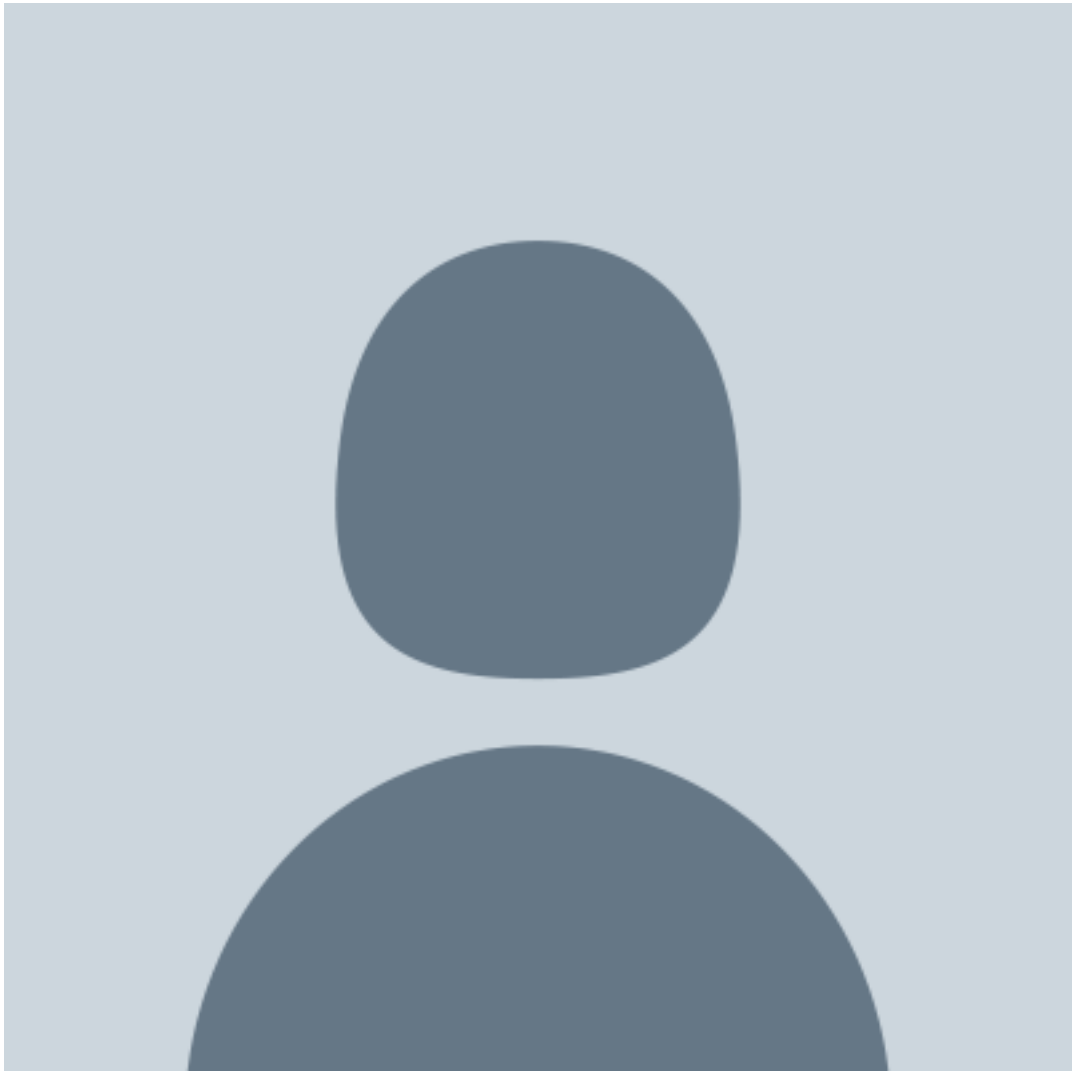
Finally, the language barrier and prevailing business culture further complicates the landscape and justifies the engagement of local experts to conduct due diligence of a company's third parties.

Read the first article in this series "China's Changing Compliance Landscape" in the June 2014 issue of the *ACC Docket*!

Dennis Haist



Weining Zou



Caroline Lee