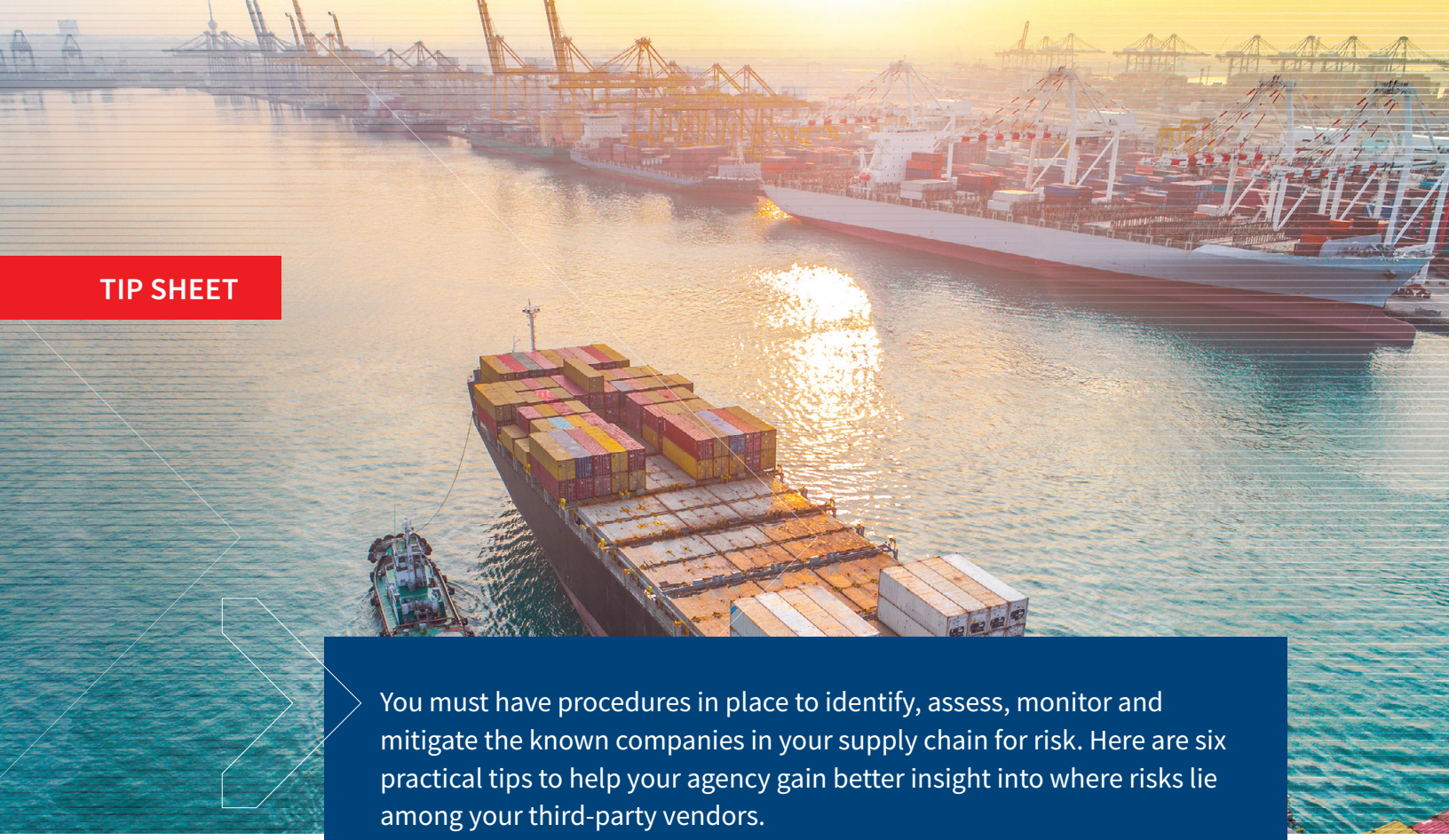
LexisNexis® RISK SOLUTIONS | Government

TIP SHEET

6 tips for conducting vendor due diligence and reducing risk in your supply chain

Working with third parties is a necessity for obtaining specialized expertise and resources without having to invest in developing those skills or services in-house. But external partners, whether they're consultants or suppliers, bring with them an element of risk.

In today's regulatory climate, effective due diligence of vendors has never been more important. From anti-bribery and corruption laws to sanctioned regimes and PEPs, you need be aware of any potential threats to your government agency's reputation.



TIP SHEET

You must have procedures in place to identify, assess, monitor and mitigate the known companies in your supply chain for risk. Here are six practical tips to help your agency gain better insight into where risks lie among your third-party vendors.

1. Don't rely on traditional credit history sources

Most businesses in the U.S. are small businesses with thin files, or no credit history at all. That's especially true if they've been in existence for fewer than five years. You'll need to tap additional and alternative data sources to go from a thin file to a complete picture of your vendor's financial stability.

2. Question self-reported data

If the information your agency has about a business has only been provided by the business itself, it may not be accurate. Agency data can be incorrect, outdated or incomplete. It may also differ from data another agency has on file about that business. You'll need to verify the facts to establish a single version of the truth and fill in all the blanks before you have a complete understanding of the company.

To be efficient, you should have the ability to search thousands of public records sources and validate self-reported data on a single platform in seconds, versus searching multiple websites or disparate data sources.

3. Uncover related businesses

Looking at a supplier as a standalone business may not give you the full story. You'll want to uncover if the business is linked to others businesses. And if so, are those entities legitimate? Are they involved in suspicious activities? Hint: If those relationships appear to have been deliberately concealed by complex organizational layers or are shell companies with hidden ownership, you need to do more digging!

TIP SHEET

4. Look for risky personal connections

You can't separate a business from its owners. Your due diligence must extend to the company's officers. Examine what personal connections they have. If they can be linked to suspicious individuals or activities, you may not want to do business with them.

5. Monitor for changes

Businesses are dynamic. They can quickly change names, owners, locations and more. Due diligence at the beginning of the relationship isn't enough. You need to also be monitoring your suppliers for changes that might suggest increased risk.

6. Ensure Compliance with Executive Order 13873 and the 2019 National Defense Authorization Act

In 2019 President Trump issued an Executive Order to "Secure the Information and Communications Technology (ICTS) and Services Supply Chain." Aimed at preventing economic and industrial espionage against the U.S., it grants the Secretary of Commerce far-reaching authority.

The Secretary can prohibit or modify transactions involving ICTS emanating from countries known to be foreign adversaries that could pose a risk to:

CRITICAL INFRASTRUCTURE

THE U.S. DIGITAL ECONOMY

U.S. NATIONAL SECURITY

U.S. CITIZENS' SAFETY

All industries are potentially affected by the regulations, which allow for case-by-case reviews of transactions at the Secretary's discretion. As seen in FAR 52.204-24, 25 and 26, any person who violates the regulations may be liable for a civil penalty up to $320,584 per violation or twice the value of the relevant transaction, as well as damages pursuant to a mitigation measure.

These new, sweeping regulations and the severity of possible penalties make conducting effective due diligence of suppliers more crucial now than ever before. You need access to the best business data and technology to manage your vendor risk.

Make informed buying decisions

When analyzing a potential supplier, you must have visibility into the complete risk profile of the business and its owners and the ability to link entities and individuals across disparate data sources and non-obvious relationships. LexisNexis® Risk Solutions offers a full array of business data solutions that leverage unparalleled data reach and proven analytics to streamline due diligence at onboarding and throughout the lifetime of the relationship.

Tap into precise business intelligence to drive informed vendor decisions, strengthen your procurement process, comply with Executive Order 13873 regulations and diminish your supply chain risk.

For more tips on vetting suppliers, contact your LexisNexis Risk Solutions representative or call us at 888.579.7638.

LexisNexis® RISK SOLUTIONS | Government

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue.