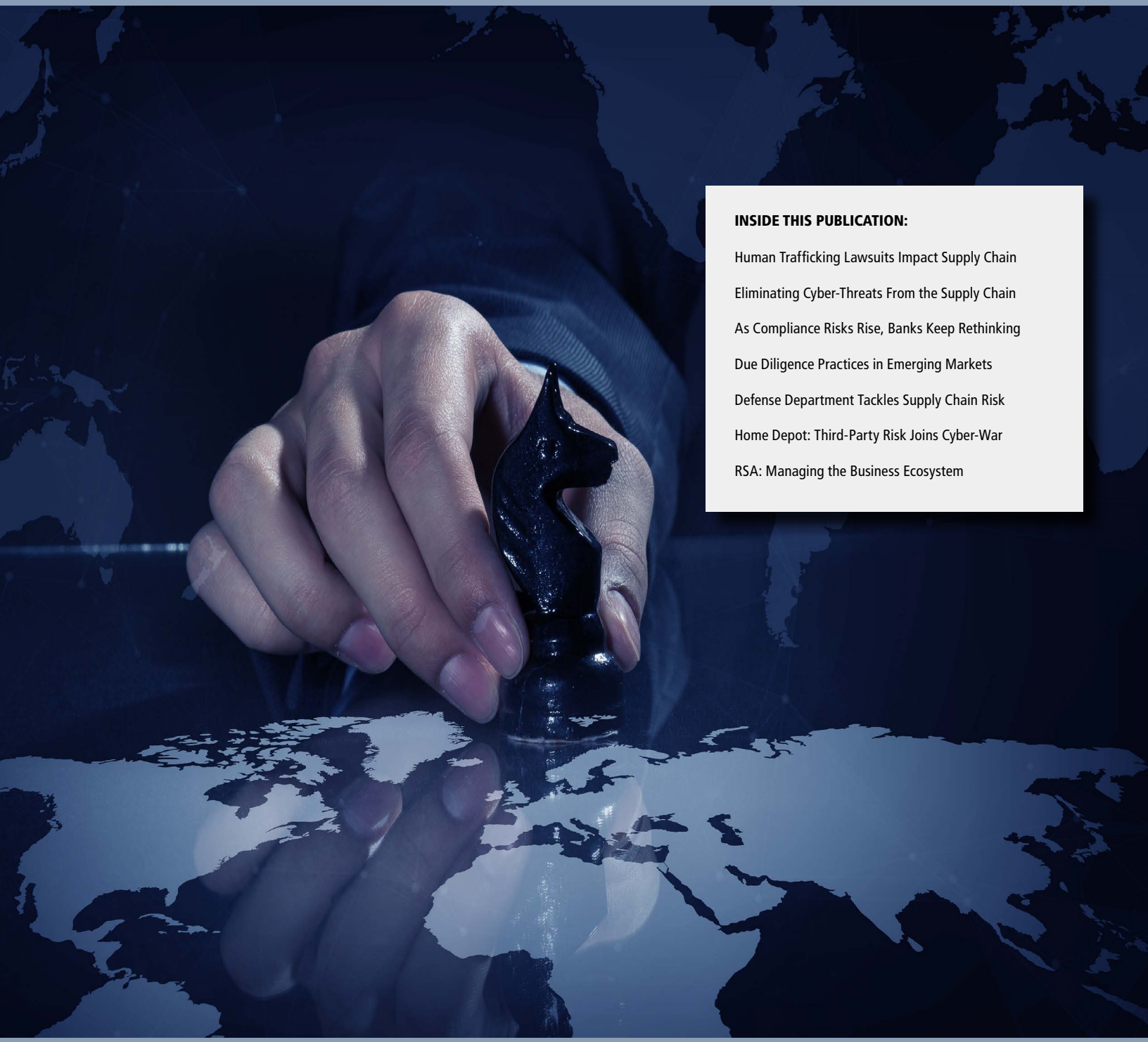
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Playing the Game of

Third-Party Risk

An e-Book publication sponsored by RSA

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. In today's competitive landscape, risks are dramatically changing and with increasing complexity, next generation security strategies are critical.

RSA Archer provides GRC professionals with a centralized solution to identify, assess, evaluate, treat, and monitor risks across the lines of business. Areas of focus include IT security and risk management, operational risk, regulatory and corporate compliance, audit management, business resiliency, and third-party governance. For more information, visit www.rsa.com

Inside this e-Book:

Human Trafficking Lawsuits Impact Supply Chain

Forget conflict minerals. Lawsuits against Nestlé and Costco both claim the companies used shrimp produced utilizing slave labor in Thailand

by Joe Mont

While you were worrying about tin, tungsten, tantalum, and gold in your supply chain—all minerals blamed for human rights abuses—recent lawsuits targeting cat food and shrimp cocktail are creating a whole new type of compliance headache.

In August 2015, a class-action lawsuit was filed against Nestlé for allegedly supporting a system of slave labor and human trafficking when sourcing seafood for its Fancy Feast brand of cat food. A similar lawsuit alleges that Costco knowingly sold frozen prawns that were the product of slave labor in Thailand; it demands those products be labeled to indicate that they are the product of slave labor.

Expect more cases like these as government regulations continue to address social issues. Notably, the California Transparency in Supply Chains Act and U.K. Modern Slavery Act require companies to disclose their efforts to eradicate forced labor and human trafficking from their supply chains. The California law was invoked in the Nestlé and Costco lawsuits.

"It is the tip of the iceberg and signal of a trend we are going to see more of," Dynda Thomas, a partner with the law firm Squire Patton Boggs , says of this new breed of litigation.

The Costco complaint argues that its use of forced labor is inconsistent with its California Transparency in Supply Chains Act disclosure. That state law requires businesses to disclose the efforts they are making (if any) to eradicate human trafficking and slavery from their supply chains. It applies to retailers and manufacturers with annual worldwide gross receipts that exceed $100 million and that do business in California.

> "These cases show the risks of making what people probably believed were solid, good faith statements about their efforts to eradicate slavery because they are now being used against them."
>
> Dynda Thomas, Partner, Squire Patton Boggs

Costco's disclosure under that law says that it "has a supplier Code of Conduct which prohibits human rights abuses in our supply chain" and that it conducts supply chain audits and imposes consequences to prevent and correct violations. The lawsuit, drawing from media reports uncovering forced labor in Thailand's shrimping industry, claims that the disclosure was both inaccurate and misleading.

The lawsuit against Nestlé similarly alleges that the company "knowingly supports a system of slave labor and human trafficking to produce its Fancy Feast cat food, while hiding its involvement with human rights violations from the public."

The lawsuit alleges that Nestlé works with a Thai partner, Thai Union Frozen Products, to import more than 28 million pounds of seafood-based pet food for brands sold in America, some ingredients of which were sourced using slave labor. The complaint also states that despite protection of human rights listed as one of Nestlé's Corporate Business Principles, the food giant "has failed to live up to its own ideals" as government sources have confirmed that fish and shrimp from Thailand are likely the product of forced labor.

Activists, litigants, and shareholders are all pressuring organizations to have a better understanding of their supply chains, says Mike Varney, partner in Crowe Horwath's global risk consulting practice. Lawsuits like these will increasingly make organizations "aware they have to consider both financial and non-financial elements in their decision making." They also, once again, drive home the point that companies must be fully engaged in supply chain risk management and have an "intimacy with their vendors."

"Think back 15 years ago. Nine times out of 10 you probably knew the person you were buying from, or knew a person from the organization," Varney says. "Now, with these wide, dispersed supply chain structures in all parts of the world, and with a lot of negotiations and discussions done over the phone or via e-mail with organizations in countries with different cultural norms—if you are not close to your vendors, have an engaged relationship, and a process where you vet them, audit them, and hold them accountable, you can end up in situations like this."

An unnerving reality of the lawsuits is the potential that companies have no good options when disclosing their efforts to be socially responsible. You can try ignoring issues like human trafficking until litigation, regulatory wrath, and bad publicity catch up with you; or you can put programs in place and discuss them openly—and immediately put yourself in the crosshairs of the plaintiffs bar.

Thomas worries that disclosures under the California Transparency Act will be used as fodder for litigation if those assurances prove to be unfounded or inadequate. "These cases show the risks of making what people probably believed were solid, good faith statements about their efforts to eradicate slavery because they are now being used against them," she says. "In Costco's case, they said they don't tolerate slavery in their supply chain. Then the evidence comes out that it exists. If they hadn't made that statement, they probably wouldn't be sued for this."

> "If you are not close to your vendors, have an engaged relationship, and a process where you vet them, audit them, and hold them accountable, you can end up in situations like this."
>
> Mike Varney, Partner, Crowe Horwath

Getting Ahead of It

One of the only ways to insulate company claims from successful litigation is to ensure that the claims are accurate and company programs are suitably effective, whether the issue at hand involves slavery, child labor, conflict minerals, cotton, cocoa, or palm oil. Companies need to achieve regulatory compliance, but also keep costs in check when waging the uphill battle to ensure that what could be thousands of suppliers are compliant.

A prerequisite is education, says James Calder, director of compliance programs for Assent Compliance. If possible, companies should develop a learning management system for suppliers and ensure that there is a clear, unambiguous communication of corporate policies. Also, track what suppliers have done for training as part of their onboarding process. Educational outreach should encompass both a vendor's management team and employees, with the latter group provided a hotline or similar mechanism to report concerns and violations of the agreed-upon Code of Conduct.

A supplier management system can sort through the data you collect on vendors and help make sense of surveys, inspection reports, supplier training, and due diligence auditing. Using this data, a company can establish risk profiles based on product and geography, prioritizing outreach and due diligence investigations. "Those will trigger activities within the program to quantify whether a supplier is high risk or not," Calder says. "Then, if you have a high-risk supplier, there is an assessment by subject matter experts and a much deeper survey and discussion. You may not necessarily need an audit at that point, but you want to get as much information from those suppliers as possible to develop the risk assessment."

Unannounced on-site visits and audits can be deployed for uncooperative or suspicious suppliers. "That's a pretty high level of due diligence because if you pop up on site without telling them you are coming, that's when you might catch issues," Calder says. "You need to have good auditors, people who understand the issue so they interview the right people and ask the right questions. Even if a supplier tries to hide stuff, if you ask the right questions you can find out if there is something wrong."

As for avoiding litigation, Calder has some simple advice for organizations: Have a plan and stick to it. "Make a commitment, and have senior management buy into it," he says. ■

CALIFORNIA'S DISCLOSURE REGIME

Below are selections from a resource guide to the California Transparency in Supply Chains Act.

The California Transparency in Supply Chains Act applies to any company doing business in California that has annual worldwide gross receipts of more than $100 million and that identifies itself as a retail seller or manufacturer on its California tax return. Companies subject to the Act must post disclosures on their Internet websites related to: verification, audits, certification, internal accountability, and training. [Report rules and suggestions are below.]

- Confirm whether the company engages in verification activities to identify, assess, and manage the risks of human trafficking ...
- ... disclose whether the company uses a third-party verifier.
- Describe the general methodology the company uses to verify entities in the product supply chain in assessing those risks, including general information about the frequency of verifications.
- Describe whether the company assesses and manages potential risks related to the presence of labor brokers or third-party recruiters in its supply chain.
- State whether the audits are independent and unannounced.
- Generally describe the audit methodology and how the company selects suppliers to audit.
- Provide statistics on the general timeline, frequency, and number of announced and unannounced audits.
- Disclose to what extent that the retail seller or manufacturer requires direct suppliers to certify that materials incorporated into the product comply with the laws regarding slavery and human trafficking of the country or countries in which they are doing business.
- Provide a general description of the certification requirement and the consequences for violating it.
- Provide a link to the company's code of conduct related to supplier workplace standards and provide general information on the types of preventative and corrective actions it takes.
- Disclose any mechanisms in place to help workers understand the company's fair labor requirements, including protections for workers who lodge grievances or report violations. Identify levels of employees being trained by category or type.
- Provide a general description of the nature of relevant training, including topics and general statistics regarding the duration and frequency of the training sessions conducted.

Source: Office of the Attorney General

Elminating Cyber-Threats From the IT Supply Chain

National Institute of Standards and Technology issues supply chain risk management guidance that chief compliance officers in the private sector should keep their eye on

By Jaclyn Jaeger

The longer a global supply chain grows, the less visibility and assurance corporations have into the integrity and security of their products and operations. Now NIST is trying to pierce that fog, and compliance officers in the private sector might want to take notice.

In April 2015 the National Institute of Standards and Technology issued its latest guidance, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"—a 282-page missive on how to better manage the supply chain for technology products, to root out cyber-threats that might leave a piece of IT equipment compromised or simply malfunctioning. NIST's guidance is intended for government agencies acquiring lots of IT and communication technology, but the principles behind it are just as useful elsewhere.


Boyens

"Every organization relies upon technology, whether it's in their manufacturing processes, their products, or services, or if it's to enable their business activity," says Jon Boyens, a senior adviser for information security at NIST and co-author of the guidance.

In today's globalized world, the components of a laptop or a cellular phone, for example, are routinely manufactured in many different locations, while assembly of the final product may take place in yet another part of the world. Now imagine how much more complex that supply chain becomes for a much larger system, such as the avionics in a commercial airplane or a communications network for the military.

"Each access point into the technology, which ultimately is assembled into one product or service, creates risk," Boyens says. Hackers might try to embed malicious software within those components, or poorly trained workers might just assemble a bad part. Either way, the threats to the supply chain are many, and the final result is the same: an untrustworthy product, that you might not even know exists.

"Cyber-supply chain risk management is still a fairly nascent discipline," Boyens says. "I would say it's where traditional supply chain risk management was about 15 years ago. It's still developing."

Risk Management

One part of the guidance describes three tiers of risk management to help organizations integrate ICT supply chain risk management (yes, there's an acronym for that: ICT SCRM) effectively. They are:

TIER 1: ORGANIZATION. In this tier, the company's executive leadership team defines the company's overall ICT SCRM strategy, policies, goals, and objectives. These activities "help to ensure that ICT SCRM mitigation strategies are cost-effective, efficient, and consistent with the strategic goals and objectives of the organization," the guidance states. This tier is also responsible for establishing a risk tolerance level for ICT supply chain risks.


Bisceglie

Senior leadership support is "non-negotiable," says Jennifer Bisceglie, president and CEO of Interos Solutions, a consulting firm that works on supply chain risk management. It must be connected to the business objective, she says, or leadership will not support it.

At the organization tier, another step is to establish a team with roles and responsibilities for leading and supporting ICT SCRM activities. "We advocate a team-based approach," Boyens stresses. The specific functions that may be involved in managing ICT supply chain risks can include compliance, risk, legal, IT, supply chain and logistics, acquisition and procurement, and other relevant functions, he says.

> "This does not negate the need for each organization to take the time to review their internal policies and processes to see where they might be introducing vulnerabilities into their operations, or accepting risk from their supplier base and partner."
>
> Jennifer Bisceglie, President & CEO, Interos Solutions

TIER 2: MISSION/BUSINESS PROCESS. This tier is responsible for developing actionable policies and procedures, guidance, and constraints. In this tier, program requirements are defined and managed, and they might include cost, schedule, performance, and a variety of critical non-functional requirements—such as reliability, dependability, safety, security, and quality. "Many threats

> "Every organization relies upon technology, whether it's in their manufacturing processes, their products, or services, or if it's to enable their business activity."
>
> Jon Boyens, Senior Adviser, NIST

to and through the supply chain are addressed at this level, in the management of trust relationships with system integrators suppliers, and external service providers of ICT products and services," the guidance states.

TIER 3: INFORMATION SYSTEM. This tier is where ICT SCRM activities are integrated into the system development lifecycle of IT systems and system components. "Many threats through the supply chain are addressed at this level, with the use of ICT SCRM-related information security requirements," the guidance explains.

Reducing ICT supply chain risks should be an enterprise-wide effort. "Generally, senior leaders provide the strategic direction, mid-level leaders plan and manage projects, and individuals on the front lines develop, implement, and operate the ICT supply chain infrastructure," the guidance states.

Post-Tier Steps

After these three tiers have been established, ICT SCRM should be integrated into enterprise-wide risk management processes by implementing the following steps:

- **Frame:** Establish the context for risk-based decisions and the current state of the information system or ICT supply chain infrastructure.
- **Assess: Review** and interpret severity, threat, vulnerability, likelihood, impact, and related information.
- **Respond:** Select, tailor, and implement mitigation controls once a risk has been identified.
- **Monitor:** Monitor risk on an ongoing basis, including changes to an information system or ICT supply chain infrastructure, using effective communications and a feedback loop for continuous improvement.

Any firm that's trying to implement supply chain risk management best practices can use the NIST guidance as a framework, although the exercise will always involve lots of effort and attention. "This does not negate the need for each organization to take the time to review their internal policies and processes to see where they might be introducing vulnerabilities into their operations, or accepting risk from their supplier base and partners," Bisceglie says.

Furthermore, Boyens says that the guidance is meant to complement, rather than replace, existing standards and guidelines, such as CoBIT 5.0 or ISO 27000. "Our risk management processes are consistent with other risk management processes in terms of identifying, assessing, and managing that risk," he says.

Because technology supply chains differ across and within organizations, those risk management plans "should be tailored to individual organizational, program, and operational contexts," the guidance stresses. Tailored plans will "help organizations to focus appropriate resources on the most critical functions and components based on organizational mission/business requirements and their risk environment."

"We need to change the workflow from reactive to proactive," Bisceglie says; supply chain risk management should be a process, rather than a compliance checklist activity. ■

MULTI-TIERED RISK MANAGEMENT

Below is an excerpt from the National Institute of Standards and Technology's guidance, describing the three organizational tiers that make up information and communication technology supply chain risk management (ICT SCRM).

Tier 1: Organizational level. In general, Tier 1 is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of the organization-wide ICT SCRM policies to guide the organization's activities in establishing and maintaining organization-wide ICT SCRM capability.

Tier 2: Mission/business process level. Tier 2 is engaged in prioritizing the organization's mission and business functions, conducting mission/business-level risk assessment, implementing Tier 1 strategy and guidance to establish an overarching organizational capability to manage ICT supply chain risks, and guiding organization-wide ICT acquisitions and their corresponding SDLCs.

Tier 3: Information system level. Tier 3 is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' [development life cycles].

The ICT SCRM activities can be performed by a variety of individuals or groups within an organization, ranging from a single individual to committees, divisions, programs, or any other organizational structures. ICT SCRM activities will be distinct for different organizations depending on their organization's structure, culture, mission, and many other factors.

It should be noted that this publication gives organizations the flexibility to either develop stand-alone documentation (e.g., policies, assessment and authorization plan and ICT SCRM plan) for ICT SCRM, or to integrate it into existing agency documentation.

Source: NIST

As Compliance Risks Rise, Banks Keep Rethinking

Non-financial risks (read: regulatory compliance failures) are now driving the compliance conversation at large firms more than financial risks

by Joe Mont

Sure, the biggest albatross around the banking world's neck right now is the Federal Reserve and its continued efforts to keep interest rates low. That policy has been punishing to banks' bottom line.

But make no mistake, banks have plenty of other albatrosses around their necks too—and most have to do with regulatory compliance risks.

Think of stress tests and visits from regulatory examiners; think of heightened capital requirements and nine-figure monetary penalties for legal violations. Banks have shuttered branches in risky geographies, are retreating from market making activities, cut formerly profitable correspondent banking relationships, and closed their doors to what some consider unsavory businesses (from strip clubs to marijuana dispensaries).

All of it to stay on the right side of regulatory compliance.

Some banks now even want to avoid taking large cash deposits. State Street recently started charging many of its customers for large dollar deposits. Likewise, JPMorgan Chase reportedly cut its own unwanted deposits by more than $150 billion by tacking on fees. Why give up the money? Near-zero interest rates are one reason, but there is also regulatory concern that this so-called "hot money" might cause systemic damage if too many customers try to take it back too quickly during a financial crisis.

These specific actions illustrate a broader picture: Banks are increasingly shifting their focus to non-financial risks.

According to EY researchers in a recently released survey of 52 financial firms across 27 countries, 89 percent of respondents reported a heightened focus on non-financial risks, including conduct, compliance, reputation, money laundering, and systems.

Many of the responding banks shared a similar opinion: the events that led to the large operational losses sustained during the past five years (fines, payments to purchasers of products, and fraud losses among them) were the result of weak oversight and control processes.

"This has triggered risk and control reviews in a number of banks and spurred changes to accountability to ensure the front office focuses on the quality of the controls in the end-to-end activity," the EY report says. "Banks have also increased evaluation of near-miss events and have sought mechanisms to improve information channels up through the organization, including whistleblower arrangements."

Banks have "to take a knife to any part of the business that is dragging down return," says Patricia Jackson, lead author of the EY report. Nearly a quarter of the surveyed firms are retreating from geographic areas, double the number who said they were last year. More than 40 percent are exiting business lines, and 90 percent are reevaluating them.

"We are sending whole reams of activity no longer in banking over to shadow finance," she says. "Project financing, infrastructure lending, energy finance are not in traditional banking now."

"The initial focus was on capital and liquidity," says Peter Davis, a principal in EY's financial services office. "This year, we saw the focus on non-financial risk and techniques for testing those." Those efforts include a sharper focus on culture and conduct. A considerable challenge is the ongoing struggle to embed risk appetite across the enterprise.

> "Internally banks have understood that to embed significant changes to management practices, controls, they need to have a solid culture that provides the foundation for those changes to take place."
>
> Andrés Portilla, Managing Director of Regulatory Affairs, Institute of International Finance

"Internally banks have understood that to embed significant changes to management practices [and] controls, they need to have a solid culture that provides the foundation for those changes to take place," Andrés Portilla, managing director of regulatory affairs for the Institute of International Finance, said during a webcast to discuss the EY study. "You can have adequate capital, adequate liquidity; but if you have the wrong kind of culture within the financial institution that is where the problems are going to come from."

Getting to Non-Financial

To bring greater focus to non-financial risk, many banks are creating new functions, often mandated by their boards, which review conduct risk as stringently as the firms historically looked at financial risk. "This conduct risk requires the education and training of internal personnel as well as current and potential third parties," says Greg Dickinson, CEO of Hiperos, a provider of risk-related technology to global banks. "Codes of Conduct, if not in existence already, are being created and personnel and external parties need to attest to them. All of this, of course, is based upon the bank's risk appetite and that too is being reexamined in light of the additional conduct issues that need to be incorporated into an overall risk score."

The focus on improving "culture," as demanded by banking regulators presents a considerable challenge: How to develop a comprehensive framework, rather than simply add another layer of checks and metrics of questionable value. Banks also report that implementing risk-sensitive compensation policies effectively is difficult.


Dickinson

"It's difficult to assess," Portilla says. "There are no numbers or metrics that show what kind of a culture you have within a financial institution." Supervisory assessments rely on interviews with the board and with senior and middle management as they "try to grasp what culture and environment they live with day to day."

A supervisory look at culture and risk appetite is nothing new, Jackson says, "but pressure on the industry in this area has intensified and intensified" and "there is still a large majority of firms who are struggling to link it to business decisions."

"That's got to be the next task," she says. "If you want to get accountability with your business lines, you need to tell them how much risk you are willing to run."

In response, expect banks to continue ongoing investments in technology that can assist with granular risk analysis and provide both qualitative and quantitative metrics. "It has to mesh together," she says. "You can't just go on chucking another thousand people at the problem. It is too costly."

The attention paid to bank culture and other non-financial risks will continue as institutions are prodded by regulators. Dickinson refers to recent guidance by the Office of the Comptroller of the Currency that delineates new responsibilities banks must assume as they assess risk and compliance before entering into a third-party relationship.

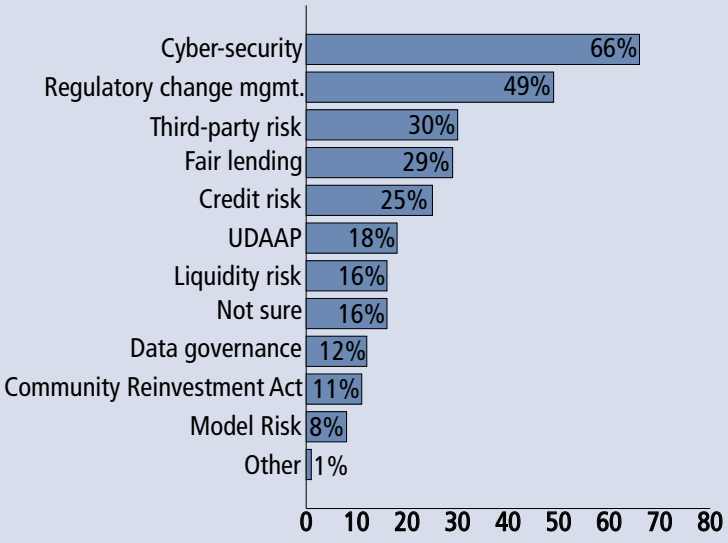
"These risks can range from information security to bribery, corruption, and beyond," Dickinson explains. "We all have read about breaches that occurred to financial organizations caused not by their own data security, but by a third party whose cyber-security was not secure enough."

Banks are "taking serious and comprehensive steps to expand their risk programs to incorporate conduct and compliance into third-party risk assessments," Dickinson says. "They are instituting internal codes of conduct as well as ensuring third parties attest to them."

Dickinson recalls a recent conversation with one financial executive who provided detail on a litany of several institutional changes: "We've completely overhauled our enterprise risk management framework, including all of the supporting key risk frameworks and policies; re-evaluated and articulated the firm's culture and values; created a single code of conduct across the firm; and clarified roles and responsibilities, as well as the performance appraisal and compensation process." ■

BANKS RANK RISK

The following are top risk concerns for financial institutions as detailed in Wolters Kluwer's recent Financial Services' Regulatory & Risk Management Indicator.



Source: Wolters Kluwer

Due Diligence Practices in Emerging Markets

CCOs wondering how their peers manage third-party risks and where they focus due diligence efforts will want to take a look at a new report from due diligence firm Arachnys

by Jaclyn Jaeger

Compliance officers wondering how their peers manage third-party risks and where they focus due diligence efforts these days will want to take a look at a new report on those practices.

Chief compliance officers responsible for emerging markets have long been hampered by poor access to corporate data, court records, and media reports in those regions. That has driven them to use technology for more comprehensive research on the third parties and individuals with whom they do business. "We really don't see any sector as being able to avoid having to invest more in due diligence," says Ed Long, head of research and report author for Arachnys, a British software firm that provides enhanced due diligence.

To get a better understanding of where in the world companies concentrate their due diligence efforts, Arachnys studied the volume and nature of its customers' search efforts in the last year. Out of 206 countries where companies conducted due diligence searches, China was, by far, the most-searched country in the world—more than twice as much as Russia, the No. 2 country. Arachnys published that report and gave Compliance Week a review of some of the results.

Exposure to high levels of corruption in China and sanction violations in Russia probably explain why many companies focus their due diligence efforts on those two countries. "The number of international sanctions imposed has increased interest among compliance officers in checking out ownership structures of Russian companies, and checking out what their exposure is to these companies," Long says.

> "The number of international sanctions imposed has increased interest among compliance officers in checking out ownership structures of Russian companies, and checking out what their exposure is to these companies."
>
> Ed Long, Head of Research, Arachnys

As one risk adviser at a global accounting firm explained in the report, "It's not the sanctions lists themselves that are causing my clients problems. It's how to decipher whether third parties are or aren't linked to the individuals or entities on the sanctioned list."

Following China and Russia, the United States ranked third for due diligence research activity. One reason may be that significant practical barriers still exist in the United States to finding corporate information, particularly because many companies are registered at the state level, rather than at the federal. "Due diligence research is less than plain sailing, driving the need for improved tech solutions to catch the small details that can otherwise fall through the cracks," the Arachnys report stated.

"What we see in the United States is competition to be the most opaque state," Long says. Delaware, for example, stands out as the one of the least transparent states, where obtaining any information—particularly on beneficial ownership of companies—other than the name and registration number can be difficult, he says.

One senior vice president of an investment bank was quoted in the Arachnys report as saying that tracing ultimate beneficial ownership of a business in the United States can take just as much time and effort as he spends researching companies in North Africa. "The information is usually available online, but you often have to work hard to get it, jumping through different hoops," the executive says.

Other countries where companies commonly focused their due diligence searches include Brazil, Mexico, India, and Nigeria. "Compliance and risk professionals continue to focus on the BRIC nations to a far higher degree than their MINT (Mexico, Indonesia, Nigeria, and Turkey), counterparts," the report stated. "[Arachnys] customers were four times more likely to run analysis on a BRIC nation than a MINT nation, for example, while over half of all searches in these countries were in China."

Industry Variances

Due diligence efforts also varied depending on industry, as well as country. The main driver is "how heavily regulated the industry is," says David Buxton, founder of Arachnys—the more heavily regulated the sector, the greater need to perform due diligence. As a result, the financial services, pharmaceutical, and oil and gas sectors tend to perform high levels of due diligence.

Aside from regulatory pressures, geography still plays a strong role. "We see companies in what might otherwise be low-risk industries—retail, for example—that have very significant compliance exposure because of the markets in which they operate," Buxton says.

Obstacles Persist

The report also assessed the unique compliance obstacles that each country poses when performing a due diligence search. As one head of research at an investment bank explained in the report, two barriers arise in China: language differences—"especially when we need to undertake quick, reactive research;" and unraveling how a com-

pany is owned.

"We've had multiple experiences of companies being red-flagged only to find them months or years later simply operating under a new name," the executive said in the report. "Understanding the data environment in China and knowing what information is out there relating to ultimate beneficial ownership is crucial."

With the language barrier in particular, information on registered companies is only provided in Chinese; unless you have a team of local experts working on this research, "it can be very challenging for Western-based companies to do due diligence work on Chinese companies," Long says. Furthermore, because registered companies in China are listed by province, "you really need to know where your company is registered to be able to find information on it," he adds.

Another country that poses several due diligence reporting obstacles is Mexico, where the country's federal structure, poor corporate transparency, and entrenched corruption makes research particularly difficult. According to the head of financial crime research at one multinational bank, "with other BRIC markets like Brazil, and even China, you see real progress in creating integrated, centralized, easy-to-use registries. That's not yet the case in Mexico."

"The key thing compliance officers should be doing is making sure they are going to the actual official sources of information," Buxton says. He adds that companies shouldn't always rely on third-party sources that "may not be up-to-date, or may or may not be accurate." On a practical level, that requires having a deep understanding of each country's unique compliance obstacles, and how to overcome them, he says.

A lot of companies simply don't know what data is available, or how to access it in every country, Long says. At the same time, "the amount of direct sources available has grown exponentially," he says; compliance officers have much more corporate disclosure data at their fingertips to research than ever before.

The good news is that by using a centralized system to conduct due diligence searches on corporate data, court records, and media reports, companies increasingly are simplifying and streamlining their due diligence efforts, while reducing their third-party risk exposure. Companies can expect that trend to continue as more countries continue to become more transparent. ■

UNITED STATES, EUROPEAN UNION SANCTIONS

Below is a list of U.S. and EU sanctions in 2014 related to the Russia-Ukraine crisis.

- Oct. 6, Sanctions Body – OFAC: Revision of General License 3 to include transactions involving Sberbank subsidiary DenizBank
- Sept. 12, Sanctions Body – EC: Scope of sanctions extended on 5 restricted Russian banks; 6 companies in energy and defense sectors and 24 individuals also targeted
- Sept. 12, Sanctions Body – OFAC: Specially Designated Nationals (SDN) list update adding a total of 17 entities, primarily targeting the oil and gas, financial services, and industrial sectors
- July 31, Sanctions Body – OFAC: SDN list update adding 2 Ukrainian and 2 Russian officials
- July 31, Sanctions Body – EC: Sector-wide sanctions imposed on 5 Russian banks, export restrictions to the Russian energy and defense sectors and new designations of 8 individuals and 3 corporate entities
- July 30, Sanctions Body – EC: Extension of restrictions on trade and investment in transport, communications, or energy sectors in Eastern Ukraine
- July 29, Sanctions Body – OFAC: SDN list update adding 1 industrial entity and 3 financial services entities
- July 25, Sanctions Body – EC: Further designations of 15 individuals and 18 entities (9Crimean companies and 9 institutions)
- July 16, Sanctions Body – OFAC: introduction of the new Sectoral Sanctions Identifications List; SDN lsit update to add 4 Russian officials, 1 Ukrainian official and 15 corporate entities, including 4 in the financial services sector
- June 27, Sanctions Body – EC: Imposition of an import ban on goods from Crimea and Sevastopol
- June 20, Sanctions Body – OFAC: SDN list update to add 1 Russian and 6 Ukrainian officials
- May 12, Sanctions Body – EC: Sanctions imposed on 13 Russian and Ukrainian individuals; first EU asset freezes for 2 Ukrainian Energy companies
- April 28, Sanctions Body – OFAC: SDN list update to add 7 Russian officials and 17 Russian corporate/financial entities
- April 28, Sanctions Body – EC: 15 individuals added to designated persons list
- April 11, Sanctions Body – OFAC: SDN list update to add 7 Crimean officials and one oil and gas company in Crimea
- March 21, Sanctions Body – EC: Designations extended to include further 12 Crimean and Russian individuals
- March 20, Sanctions Body – OFAC: SDN list update to add 20 Russian officials and one Russian bank
- March 17, Sanctions Body – OFAC: First designations: 11 Ukrainian and Russian officials are added to the SDN list
- March 17, Sanctions Body – EC: Asset freeze update to include 21 individual military and political figures from Crimea and Russia
- March 6, Sanctions Body – OFAC: issuance of initial Ukraine-related Presidential Executive Order authorizing sanctions
- March 6, Sanctions Body – EC: Asset freeze and travel ban on 18 senior officials of the ousted Ukrainian government

Source: Arachnys

Defense Department Tackles IT Supply Chain Risk

Defense Department is taking a hard look at supply chain risks posed by government contractors who provide IT products and services

by Jaclyn Jaeger

The Defense Department is taking a harder look at supply chain risks posed by government contractors who provide IT products and services, so CCOs at those businesses should prepare to review how their supply chain risks might affect eligibility to bid on future contracts.

In October 2015 the department issued a final rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) and implement Section 806 of the National Defense Authorization Act. The final rule generally retains the same controversial provisions contained in an interim rule issued in 2013, including a clause that allows the DoD to bar contractors from providing IT for a "national security system" if the contractor or its subcontractors present "a supply chain risk."

The final rule generally defines a national security system as an information system used for intelligence or military operations. A supply chain risk is "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

> "Supply management is a compliance function, with responsibility for policing a global network of suppliers and ensuring compliance with laws and regulations, government contracting rules, and company policies."
>
> Alan Chvotkin, Counsel, Professional Services Council

Although the rule itself is limited in scope, it is only the latest measure in a broader government-wide effort to protect supply chain integrity in government procurement. "This fits into the government's larger focus on the supply chain risk generally," says Peter Eyre, a partner in Crowell & Moring's government contracts group. The fear: that sophisticated operators could infiltrate or sabotage national security systems by inserting counterfeit parts or malware into products the government buys.

Exclusion Authority

The final rule gives the DoD far-reaching authority to exclude IT contractors without any hearing or explanation, which is a sore point for government industry groups. "There is no due process, and there is no appeal," says Alan Chvotkin, executive vice president and counsel of the Professional Services Council, the national trade association of the government professional and technical services industry. "That's a pretty broad set of authorities."

Under the final rule, these preliminary measures must be taken, however, before the DoD may exercise its authority:

- The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Chief Information Officer of the Defense Department must first make a joint recommendation that "there is a significant supply chain risk to a covered system;"
- The DoD must make a determination in writing, with the concurrence of the Under Secretary of Defense for Acquisition, Technology, and Logistics, that Section 806 authority is "necessary to protect national security by reducing supply chain risk," and that "less intrusive measures are not reasonably available to reduce such supply chain risk;" and
- Classified or unclassified notice of the determination must be provided to certain congressional committees.

From a practical standpoint, IT contractors need to protect themselves as best they can in case DoD invokes its exclusion authority. For example, contractors should have a range of alternative suppliers in case procurement officers decide that one poses a supply chain risk, says Michael Mutek, former general counsel of Raytheon's Intelligence, Information and Services business, a $6 billion business unit of Raytheon.

Although the Defense Department has power to exclude IT contractors at will, "I don't expect this to be widely invoked," Chvotkin says. It will be a "rare occasion" when the DoD uses its Section 806 authority, he predicts.

Nonetheless, the final rule puts further pressure on compliance officers of IT contractors to vet, monitor, and audit the entire supply chain. "You really need to do all you can to try to determine if you have an issue in your supply chain," says Mutek, now senior counsel at law firm Steptoe.

Furthermore, because the final rule does not identify specific standards or controls for IT contractors to mitigate supply chain risks, compliance will prove to be a particularly complex task. "There is no one-size-fits-all standard of risk assessment and risk mitigation," Chvotkin says.

'Not a Bright Line Rule'

The DoD explained in the final rule that standards or controls would depend on the risks and risk tolerance that would apply to each procurement. "It is not a bright line rule," Eyre says. Both the NDAA and the implementing regulation leave IT contractors with a great deal of discretion. "It is difficult to know exactly what controls will be satisfactory to the government."

The Defense Department explained this lack of clarity in the final rule itself: "Risk levels, risk tolerance, and appropriate risk management measures must be determined at the local level. Evaluation factors are specified at the individual acquisition level and not in the DFARS."

However, Chvotkin says IT contractors need more guidance than what they have. "There needs to be some benchmark, some framework for companies to know what they should be doing and how they'll know they're on the right path to get there," he says. "That is absent from this rule."

RULE PROPOSAL DETAILS

The following excerpt from the Department of Defense's final regulation, "Requirements Relating to Supply Chain Risk," provides details on amendments.

Significant Changes from the Interim Rule

1. Language is added to the rule to clarify that section 806 authority is only applicable when acquiring information technology, whether as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, including clarification of the prescriptions for DFARS provision 252.239–7017, Notice of Supply Chain Risk, and DFARS clause 252.239–7018, Supply Chain Risk.

2. Guidance on the use of an evaluation factor regarding supply chain risk is modified to require the inclusion of the evaluation factor when acquiring information technology, whether as a service or as a supply that is a covered system, is a part of a covered system, or is in support of a covered system. Additional text regarding an evaluation factor has been added at DFARS 212.301, 213.106–1, 214.201–5, and 214.503–1.

3. DFARS clause 252.239–7018, Supply Chain Risk, is changed as follows—

a. Paragraph (b), is modified to state that the contractor shall mitigate supply chain risk in the provision of supplies and services to the Government; and

b. Paragraph (c) is removed as the clause will no longer contain a requirement to flow down the clause to sub-contractors.

Source: Department of Defense

That being said, nothing in the rule precludes contractors from engaging in discussions with the government to determine whether particular sub-contractors or suppliers pose any risks or concerns, Eyre says.

Chvotkin agrees that some conversations still need to be had while the DoD continues to develop the application of the rule. "Companies ought to ask those questions, and I would hope DoD would be forthcoming in answering some of those questions on a case-by-case-basis," he says.

The final rule departs from the interim rule in several important ways. First, the scope of the rule has been narrowed. Whereas the proposed rule applied to "the development or delivery of any information technology, whether acquired as a service or as a supply," the final rule applies only if the IT is "part of" or "in support of" a national security system.

Rather than the rule applying to virtually every IT component in all systems used by the Defense Department, it expressly omits routine administrative and business applications, "including payroll, finance, logistics, and personnel management applications," according to the final rule.

Another difference from the proposed rule: where the original would have pushed down the responsibility to identify and mitigate supply chain risk on subcontractors, the final rule imposes that requirement only on prime contractors. "Nevertheless, the Defense Department reserves the right to exclude a subcontractor from performance of a contract, if DoD in their subjective judgment determines that a subcontractor poses a risk in performance," Chvotkin warns.

Translation: Even though the DoD has eliminated the flow down clause for its own purposes, prime contractors should still flow down some responsibility and authority to its subcontractors, "particularly because the government can deny access to a sub-contractor," Chvotkin says. "The prime contractor must protect itself."

You have to know who you're doing business with not just among your first-tier sub-contractors, "but all the way through the supply chain," Chvotkin says. "Having visibility into the supply chain is very important, particularly for these critical national security systems."

As cyber-incidents grow more common (and more severe), government agencies are only going to grow more cautious when deciding who wins future contracts. For national security systems in particular, agencies likely will assess both the past and current performance of an IT contractor's security controls in its supply chain.

That means compliance officers at IT contractors face greater responsibility, as well. Historically, supply management used to be an administrative function that rested with the purchasing department, "ensuring that you got the right part at the right time to the right place at right price," Mutek says.

Well, "supply management has evolved," he says. "It's no longer just a purchasing function. Supply management is a compliance function, with responsibility for policing a global network of suppliers and ensuring compliance with laws and regulations, government contracting rules, and company policies." ■

Home Depot: Third-Party Risk Joins Cyber-War

Third-party risk represents the 'next frontier' in the ongoing cyber-war, says Kelly Barrett vice president of internal audit & corporate compliance at Home Depot, where she navigated a cyber-breach in 2014

by Tammy Whitehouse

Third-party risk represents the "next frontier" in the ongoing cyber-war, says Kelly Barrett vice president of internal audit and corporate compliance at Home Depot, where she navigated a cyber-breach like it was "a blow to the head" and now tells the story of how the entity faced the crisis.

"I worry about third-party risk a lot," said Barrett, in an address to the Institute of Internal Auditors General Audit Management conference. While the company quickly addressed a breach into its own customer payment data in 2014, the experience has led to plenty more activity to shore up more risk, she said. Third-party risk is one that still keeps her up at night.


Barrett

"We are sharing tons of data with third parties," Barrett said. The company outsources, for example, its benefit plans and healthcare benefits to a third party, in whom she says she has plenty of confidence. Still, "when I think of all the information that is exchanged, it's frightening," she said, especially when considering how much of that is shared into a deep pipeline of sub-contractors and sub-subcontractors.

> Third-party risk represents the "next frontier" in the ongoing cyber-war. "I worry about third-party risk a lot. We are sharing tons of data with third parties. When I think of all the information that is exchanged it's frightening."
>
> Kelly Barrett, VP of Internal Audit and Corporate Governance, Home Depots

Home Depot is one of a growing list of household-name companies that have fallen victim to cyber-breaches. When the company discovered its breach in 2014, it was well on the way to shoring up its security after a 2010 deep dive risk assessment around data security and privacy. "We did not have our heads in the sand," she said. "The breach did not happen because we didn't understand our risk and didn't do anything about it.".

> "[The NIST framework] is daunting. It has thousands of controls. You have to have a conversation with your chief information security officer and make sure you have a methodical way of choosing the controls for your risk profile."
>
> Theresa Grafenstine, Inspector General, U.S. House of Representatives

Cyber-threats are becoming more sophisticated and calculated, said Theresa Grafenstine, inspector general for the U.S. House of Representatives, who also addressed the IIA conference. "This is a call to arms," she said. "I promise you we are in the middle of a cyber-war. We just haven't defined it that way yet."

Cyber-crooks aren't looking just for credit card information that they can sell on black markets. They are looking for personal information to use against individuals inside companies and organizations, so they can be turned into spies, Grafenstine said. "It's espionage."

Barrett and Grafenstine both said they favored the NIST framework as a means of getting control over an organization's cyber-risks. Although the framework is huge, Grafenstine said companies shouldn't wade into a cyber-risk mitigation effort by trying to adopt NIST in its entirety.


Grafenstine

"It's daunting," she said. "It has thousands of controls. You have to have a conversation with your chief information security officer and make sure you have a methodical way of choosing the controls for your risk profile. Maybe the first time, you go for the top five. That's better than doing nothing."

Barrett said tone at the top was significant for the company in navigating a crisis in a way that minimized the damage. "Our CEO was engaged every second," she said. Top management emphasized doing anything necessary to make customers comfortable about shopping in the company's stores, including shutting down the entire point-of-sale system if it was necessary to protect consumers. If it had come to that, "we would be out of business," Barrett pointed out. ■

RSA®

Harness Risk, Fuel the Enterprise RSA Archer

Managing the Business Ecosystem

Maturing your third-party governance

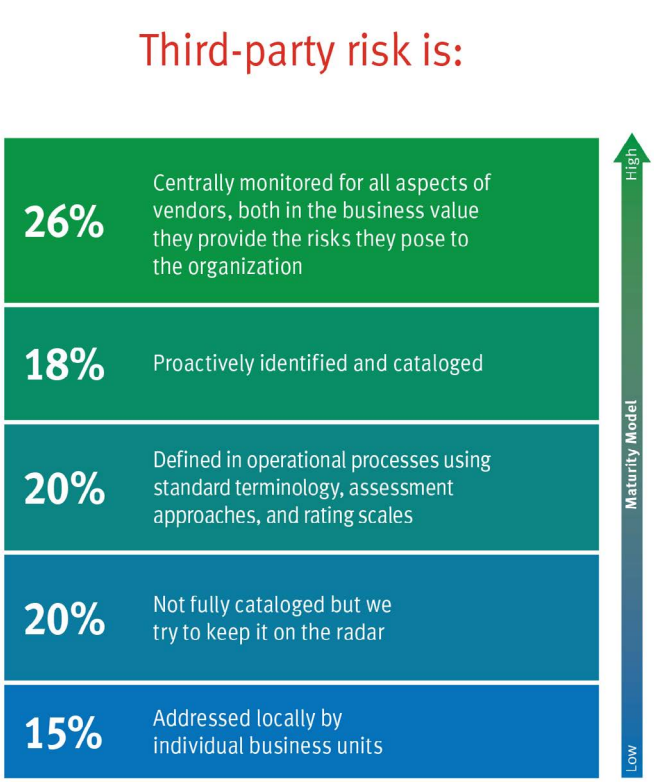
by Marshall Toburen, CIA, CISA, CBA (non-practicing)

KNOWING YOUR BUSINESS ECOSYSTEM - THE GROWING IMPERATIVE

Risk is on the mind of every executive today. There are risks that arise internal to your organization, those that are forced upon your business by external forces such as competition and regulation, and those that are inherited through your third party relationships.

Bad outcomes from third party risks are in the headlines daily. We witness stories of inferior and defective supplier products, cloud service outages, regulatory violations committed by third parties, and a barrage of third party provider data breaches. As businesses use more third party products and services to conduct business, the risks from these relationships also increase. The number, complexity and velocity of these risks make it difficult to track and respond effectively. Furthermore, the oversight of third party performance becomes increasingly important to ensure the quality of products and services delivered continue to meet required standards.

In October, 2015, RSA completed a global survey of nearly 400 organizations to gather insight into current trends and perceptions regarding Risk Management. The survey utilized RSA's proprietary Risk Intelligence Index to ask questions around key areas of risk and how organizations are addressing the changing risk landscape. According to the survey, third party risk is one of the fastest rising issues and 1/3 of the respondents indicate low maturity in addressing third party risk.



While risk is getting more and more exposure within the organization, organizations are not in a position to manage iteffectively. They continue to manage different types of risks like cyber, third party supplier, competition, business change, and product development within different business silos.

When you look across the spectrum of third party risk facing your business, there are a wide variety of issues and challenges that involve multiple business teams within your organization as well as the third parties themselves. Risks might include theft or external fraud, supply chain disruptions, reputational damages, product liability claims, business interruptions, and more.

Organizations are more frequently using third party suppliers to augment or deliver their products and services, and those suppliers have third parties providing services to them. With so many relationships to track, the complexity of third party governance can be difficult to understand and manage. Most organizations simply do not have the staff or resources to cope with this increased complexity. Organizations are often left wondering where to start and how to prioritize what is most important to the business. Unfortunately, this results in surprises that cause business disruptions.

To be effective, organizations must be able to consistently identify, assess, evaluate, treat and monitor third party risk across the business. They must respond to these risks before they become damaging and must be prepared when impactful supplier risks emerge. In addition, the first line of defense – your business managers—must understand their role in managing their third-party risks. Most teams are overwhelmed with work and cannot get in front of the problem. Without a way to identify priorities and accountability, risk management efforts are often misaligned and the business is left scrambling to react to risks when bad things happen.

To remedy supplier risk woes, your organization must be proactive in capturing prospective relationships, engaging impacted stakeholders, assessing third party risks across multiple risk categories, enforcing risk-based selection of vendors, and establishing performance metrics. By standardizing this third party risk and performance management process across the enterprise, you can establish a common language, measure-

RSA

ments, controls and processes to quickly prioritize and manage your risks. This accurate view of third party risks provides your executive team with an accurate picture so they can quickly allocate resources and make better business decisions.

MATURING THIRD PARTY GOVERNANCE PROCESSES

With so many relationships to track, the complexity of third party governance can be difficult to understand and manage. Most organizations simply do not have the staff and available resources to cope with this increased complexity. Their teams are often left wondering where to start and how to prioritize what is most important to the business.

As you begin your third party risk and performance management journey, a maturity "map" is a handy gauge to identify what processes are in place today and help you identify where your processes are today, as well as to identify your road to maturity. RSA has established a maturity journey map to outline the critical stages in a company's journey from compliance driven processes to a risk centric opportunity-focused stage. Thus, helping organizations mature from reactive environments to proactive.

This maturity journey is broken into five major stages: Siloed, Transition, Managed, Transform, and Advantaged.

» The **Siloed** stage focuses on baseline activities that all organizations need to have in place to effectively manage third party risk and performance.

» The **Managed** stage depicts the phase that organizations reach when they achieve a coordinated, sustainable third party risk and performance management program.

» The **Transition** and **Transform** stages focus on specific initiatives necessary to move the organization into the next stage of maturity.

» The **Advantaged** stage represents an advanced stage of maturity that characterizes an optimized third party risk and performance management program.

Building Blocks

Without these in place, an organization will face difficulties throughout their journey either due to a lack of focus, commitment, resources and/or strategy – making a successful third party governance program challenging. Foundational elements include:

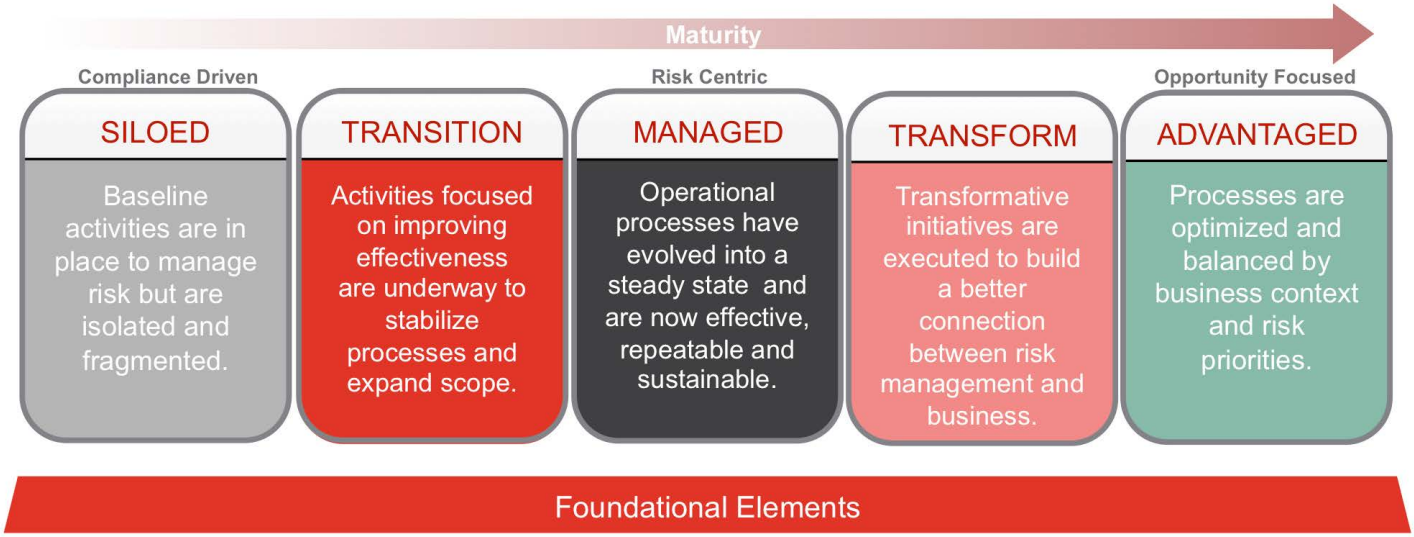
» **Management commitment** – The degree and level of leadership commitment to third party governance culture, strategy and priorities should be established as maturing risk processes takes time and resources.

» **Performance and acceptable risk** – Defined levels of performance and acceptable risk for third party governance need to be established to set the target state for the program and to ensure the business understands the level of risks involved.

» **Expectations and measurement** – Clear expectations and success criteria defined for the third party governance program must be communicated by management to guide strategies.

» **Stakeholder involvement** – Key business stakeholders and constituents need to agree on the importance of continuous improvement and maturity of third party governance processes.

» **Budget and resources** – Sufficient resources for the third party governance program must be committed to achieve success.



RSA

Moving Out of a Siloed Approach

When building an effective third party governance program, organizations must change their mindset from a siloed approach to a more managed methodology.

When organizations are Siloed, they have partial inventories of their people, processes and technology and the third parties that support them. Inventories reside in different locations, in different formats and may be maintained by different technologies. In some cases, there are multiple overlapping inventories without any one system of record. Inventories that typically exist at this stage include physical facilities, software applications, organizational structure (as depicted through the organization's financial statements) and a listing of human resources.

Various business unit managers, the purchasing department, legal and internal audit have identified what they believe to be key third party relationships, but the lists are maintained separately and may reflect significant differences. There isn't yet a robust formal approach to methodically identify third parties across the organization or to assess third party risk in a consistent manner. However, risk assessments may be performed in certain areas of the organization, for certain types of relationships, and for perceived high-risk third parties.

There is a desire to manage third party risk, but the organization is just beginning to understand what is needed to treat third party risk. The various lists of third parties and any associated risk assessments are beginning to be pooled together for evaluation by senior managers within key functional areas and on an overall basis. However, the list of third parties is incomplete and the risk assessment approaches are inconsistent.

Typically, pockets of third party profiles, details of engagements, and risk and performance data are spread across different teams within the organization. Thus, third party supplier risks are often not identified, assessed, treated and monitored consistently across all business lines. The team talks about risk with different measurements, controls and reporting. As a result, it becomes difficult to find a single source of truth about third party dependencies, risk, and performance. Without a consistent enterprise view of third party risk, your executive team does not have a clear picture to make business decisions.

As your organization determines that a Siloed approach will no longer meet the business objectives, you begin to move into a **Transition** focused on specific initiatives necessary to move the organization into the next stage of maturity, the **Managed** stage.

During this Transition, your organization begins formalizing their policies and procedures around third party governance. These policies and procedures must establish accountability for program oversight and the accountabilities of stakeholders in the first and second lines of defense. The approach to assessing and rating third party risk must be formalized as well as the process for approving new third party relationships and reaffirming the portfolio of existing third parties. If the organization is subject to regulatory obligations around third party governance, there should be a clear understanding how each regulatory obligation is addressed within the organization's formal policies and procedures.

Other steps organizations take during Transition include:

» Siloed inventories of third party relationships are consolidated. Each area that maintains a list of third parties should convert their inventory into a consolidated system of record, naming the third party and their contact details and the specific product and service engagements that they are providing to the organization.

» Siloed inventories are supplemented with yet to be identified third party relationships. Business unit managers should be queried to reaffirm their siloed lists or to document them, if such lists do not already exist. Individuals responsible for third party governance oversight may also identify relationships by interrogating legal contract inventories, reviewing expense account entries and accounts payable. The objective of this step is to ensure that the list of third party relationships is as accurate and complete as possible.

» Related business processes and internal controls are implemented to ensure that the on-boarding of all third party relationships results in cataloguing the third party relationship in the centralized repository.

» New and existing third party relationships are subject to a risk assessment. Risks assessed may include: risk associated with regulatory compliance violations and litigation; risk of financial loss from fraud and errors; risk from business interruption; risk from information mishandling or breach, risk to strategy execution, and reputation risk. Risk assessments include inherent risk as well as residual risk based on an assessment of the third party's internal controls to mitigate such risks.

» No new contracts are negotiated without performing contract risk assessments. These assessments should not only include standard risk transfer clauses but contain service level agreement performance metrics and required proof of insurance.

With these steps in place, your organization will have moved into the **Managed** stage of third party governance maturity. This is the phase that organizations reach when they achieve a coordinated, sustainable third party risk and performance management

program. By standardizing your third party risk and performance management process across the organization, you have established a common language, measurements, controls and processes to quickly prioritize and manage your risks.

Going from Good to Great

Going from a good third party governance program to a great third party governance program requires organizations achieve the fullest understanding of the business context of their third party relationships and how they support the organization and its objectives.

Transforming to a great program with optimum business context of the third party relationship requires understanding how third parties support the organization's business objectives and strategies, products and services, business processes, and IT infrastructure. This means having a comprehensive catalogue of the organization's business processes and mapping each third party product and service engagement to the business process that is being supported, and methodically asking if an identified business process is supported by a third party.

Understanding the relationship between business process and third party helps you better understand the significance of the relationship, improves the accuracy of risk assessments, and helps in understanding the importance of service level performance metrics. Establishing a complete picture of the interrelationship of IT infrastructure and mapping third party relationships to where they support hardware and software is essential to identify critical infrastructure dependencies on third parties, particularly as it relates to business resiliency. Finally, understanding how third parties support the achievement of business objectives and strategies shifts the program to a more proactive, strategy orientation.

Operating an **Advantaged** third party governance program is characterized as:

» The mapping of all infrastructure elements is complete, and there is a clear understanding of the "ownership" of strategies and objectives; the products and processes that support the strategies and objectives; the business processes that exist to enable the products and services and strategies and objectives; the IT infrastructure that supports each of the business processes; and the regulatory obligations that the organization must legally comply with. Accountability by named individual and business unit is core to a sound third party management program, reinforcing the desired risk management culture.

» Processes exist to identify gaps in known third party relationships and third parties are self-reporting key fourth party relationships, internal controls, and governance processes. Circumstances where fourth parties have multiple relationships across the third party portfolio are documented and factored into fourth party risk assessments based on the quality of reported third party governance and the type and amount of third party risk.

» Third party risk assessment results are as automated as practical, and the results of engagement-level inherent and residual risk assessments and performance metrics roll up to the vendor parent level to depict overall risk and performance at the third party parent company level. Third parties with inadequate proof of insurance and those with high risk but poor financial wherewithal are identified and carefully managed.

» Decisions to move forward with new and expanding third party relationships are methodically and consistently applied and consider all inputs. In addition, gating processes are enforced through technology to make decisions about third party risk prior to implementing new or materially changed products, processes and activities. Automation triggers risk decisions to be made when the existing level of residual risk increases above tolerance for individual engagements or overall relationships, and documented contingency plans exist to exit significant and high risk third party relationships.

» The advantaged stage is characterized by the ability to look beyond third parties to the third parties of your third parties and their supply chain dependencies. As you transform from the managed to advantaged stage you begin to catalog these "4th party" relationships and you obtain visibility into material dependencies on specific 4th parties across all of your third party relationships. This insight gives you the opportunity to evaluate systemic risk lurking in your external dependencies.

» Technology is used to ensure that all deficiencies related to proposed third party engagements are addressed prior to

RSA

contract signing. Approved exceptions to third party risk are cataloged and periodically reaffirmed.

» Approved exceptions to third party risk are catalogued and periodically reaffirmed.

» Third party risk reporting and monitoring is most robust. Stakeholders are receiving regular reports of third and fourth party risk. Changes that may affect third party risk is being reported from wherever they originate across the organization as are reports to monitor all approved third party risk-related exceptions.

» Third party risk information is being delivered in a variety of ways including dashboards, through push technology, on-demand, and through ad-hoc requests. In each case, stakeholders can dynamically drill into reports to traverse all interrelated records to understand the business context and drivers of risk.

» The second line of defense has the capability to easily configure the organization's third party governance management information system to tailor taxonomy, assessment methodology, workflow, and reporting so that it aligns to the unique requirements of the organization and to make modifications as the organization changes and best practices evolve.

ENGAGING THE LINES OF DEFENSE IN THIRD PARTY GOVERNANCE

Third party management software alone does not make for a good third party governance program. Regardless of industry or risk type, operational line managers, risk management oversight functions, and internal audit serve important roles in good day-to-day third party governance. The most effective risk management requires collaboration between these roles. The Three Lines of Defense (LoD) model characterizes the "people component" of an organization into the three primary functions related to an optimized risk management program:

» **The First Line of Defense** – Management control functions that own and manage risk. These are as business unit managers and operating managers.

» **The Second Line of Defense** – Risk management and compliance oversight functions (such as…ERM, ORM, Third Party Management, Corporate Compliance, Legal, etc.).

» **The Third Line of Defense** – Independent assurance functions (such as internal and external auditors)

The "Lines of Defense" model reinforces two important elements of risk management: defined roles and accountability.

» **Operating management** is responsible for understanding and managing their risks and internal controls.

» **Risk management and compliance oversight** is responsible for risk management frameworks, training, and challenging first line of defense risk assessments.

» **Internal Audit** (typically) is responsible for independently evaluating and reporting on the design and effectiveness of the organization's overall risk management program.

Each line of defense serves an important role for your third party governance program.

Business Units Engaging in Third Party Governance

Your first line of defense, your business units or operating management is responsible for following the organization's third party governance practices. In doing so, they must:

» Identify and monitor the third party relationships utilized by their business unit

» Collaborate with the risk management team to assess risk for each of their third party relationships

» Track the vendor's performance against agreed upon expectations.

Risk and Compliance Oversight

The second line of defense, your risk and compliance oversight teams, take the information gathered by the business units (your first line of defense) and begin employing more rigorous risk processes including:

» Policies and Practices – The risk management and compliance functions, in collaboration with the procurement function explicitly define the organization's policies and practices around third party governance including:

- Agreed upon terminology
- The risk assessment approach and rating scales
- Service level performance tracking
- On-boarding processes
- Review and approval of new third parties
- Periodic monitoring requirements
- Steps to be taken when relationships begin to deteriorate in terms of their risk profile or expected performance

RSA

» Risk Assessments – Risk management specialists including business continuity experts, information security experts, regulatory compliance specialists, and insurance and contract risk specialists have a role to play in evaluating and monitoring the risk of third party relationships. Specialists address questions like:

– How much information security risk exists after evaluating the adequacy of a third party's information security controls?

– Is risk being adequately transferred to the third party by way of contract?

– Does the third party have adequate proof of insurance to compensate your organization for errors and omissions in the delivery of their services?

– Can the third party introduce regulatory violations that your organization will be responsible for?
– Are they taking the appropriate actions to minimize the likelihood and impact of a violation?

– How much risk to your organization exists should the third party experience a disaster or business interruption?

– Has the third party taken appropriate steps, including tests, to reduce the likelihood and impact of such an interruption?

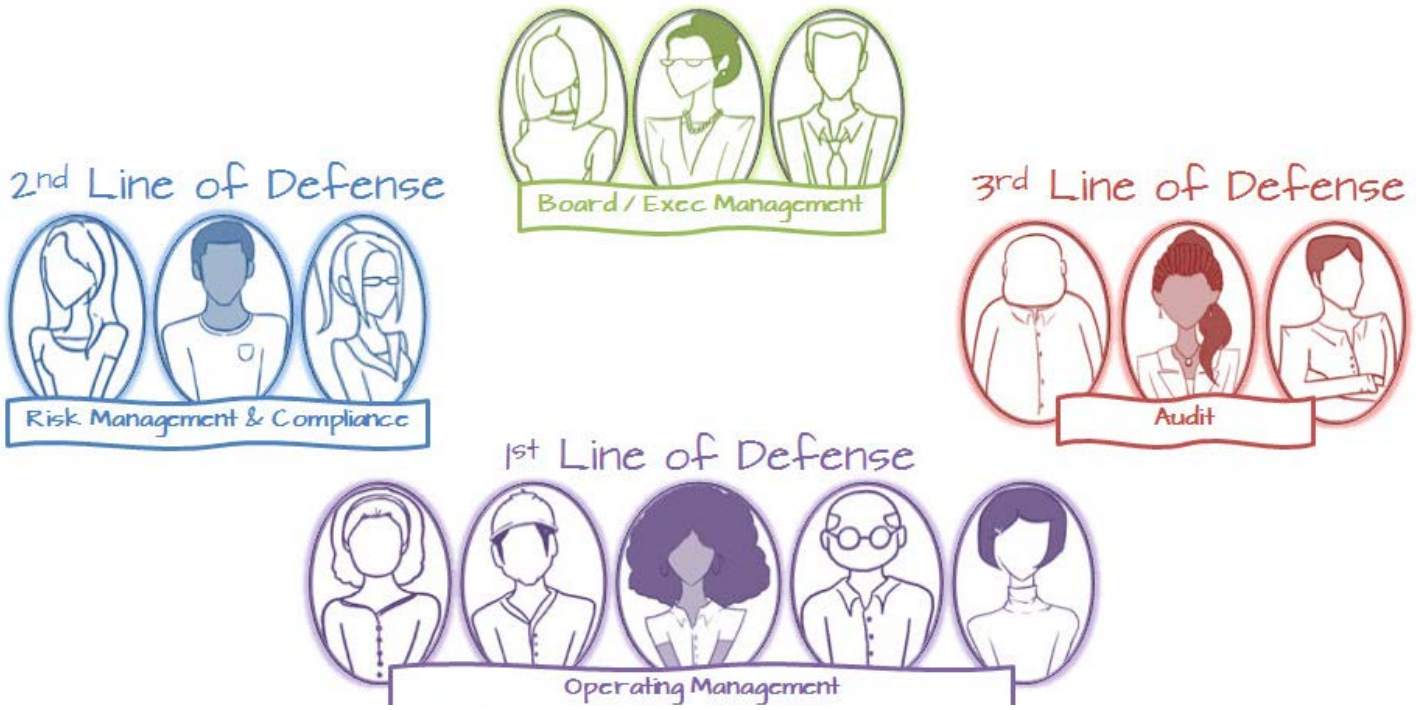
» Disbursements – The accounts payable and legal team must be on board with third party governance so that contracts are not signed and payments disbursed until the agreed upon persons have signed off. This sign off indicates the new or renewing third party relationship has been subject to the agreed upon risk assessments and conforms to the organization's risk profile or has otherwise been approved as an exception.

INTERNAL AUDIT'S THIRD PARTY GOVERNANCE PERSPECTIVE

by Patrick Potter

Internal Audit (IA) professionals (typically your third line of defense) are preoccupied enough evaluating risks and controls within the walls of their own companies, let alone worrying about what risks are being introduced by the myriad of third parties their company engages. However, this is a reality of most operating environments today and something IA cannot ignore. What complicates Internal Audit's scope is each third party has a different operating structure, business model and risk management approach IA may not be familiar with and may not jive with that of their own company.

Controls, such as on-boarding procedures, contracts and Non-Disclosure Agreements (NDA) are vital, but really the tip of the iceberg because of the close, long-term nature of most relationships. IA must ensure management is engaged in the on-



going monitoring of third party performance and controls, and in some cases, monitor that themselves. Below are three areas IA should think about as they strive to strengthen the third party environment within their organization.

What risks are third parties introducing into your control environment?

As mentioned, third parties have different operating structures, business models and risk management approaches than your company even though they may follow similar standards or authoritative sources. Their risk management approaches and thresholds might be different and they might not take the same corrective measures to address risks and implement controls as your company. As a result, risks might be introduced into your operating environment.

The following suggestions might help:

» Evaluate the third party's risk management practices to determine alignment with yours. Pay attention to risk approaches, thresholds, and acceptance of residual risk and risk metrics they monitor.

» Evaluate your company's third party evaluation and onboarding process to ensure it includes adequate steps to evaluate the third party up front, put in place the proper administrative controls and monitor the third party over time.

» Monitor third party-impacted risks to ensure they stay in alignment with your company's acceptable risk thresholds. Ensure you know which risks are impacted by your third parties and pay particular attention to how they change over time.

What access do third parties have to customer data, intellectual capital and trade secrets?

Third parties are often given your company's "keys to the kingdom" in terms of customer data, intellectual capital or trade secrets. This is some of the most critical information your company possesses and the most damaging if it's lost or misused. An NDA is a good legal document, but once the information is gone, it's gone and it's virtually impossible to know or influence how it's used outside your company.

Internal auditors should consider:

» How do your third parties secure and use the information?

» Once their engagement with your company is complete, what information is retained, returned or destroyed?

» How does the company implement information asset controls including classification of not only customer, but trade secrets and intellectual capital?

» Look for leakage – systems and access that are not tightly controlled yet contain this sensitive information, and who has access to them.

How could third parties cause our company to be non-compliant?

Regulators not only see your operating environment and span of control as what happens within your organization, but also look at your business model and the influence your company exerts, which could include your impact on third parties and vice versa. Do you know how a major instance of non-compliance to a critical mandate by a major third party might influence your organization? Could regulators turn their sights to your organization? How could sanctions, fines or other measures against a critical third party impact their ability to support your organization's strategic and operating objectives?

Here are a few considerations:

» Your company's attitude toward third parties has to be that you are your brother's keeper and have a pulse on their compliance posture, at least at a high level.

» How compliant are your third parties? Have they been sanctioned, fined or restricted from operating freely in the last 10 to 20 years?

» Have you performed an impact analysis to determine just how your critical third parties' potential instances of non-compliance might influence your company's own compliance posture, and what the impacts might be?

Third party governance is still evolving and maturing as company operating structures and models continue to incorporate third, fourth and more parties deep into the mix of how they run their business. Internal Audit must also drive their understanding and audit evaluations deep into your company's third party governance programs to ensure the process and control structure is commensurate with the level of complexity and risk these programs introduce. ■