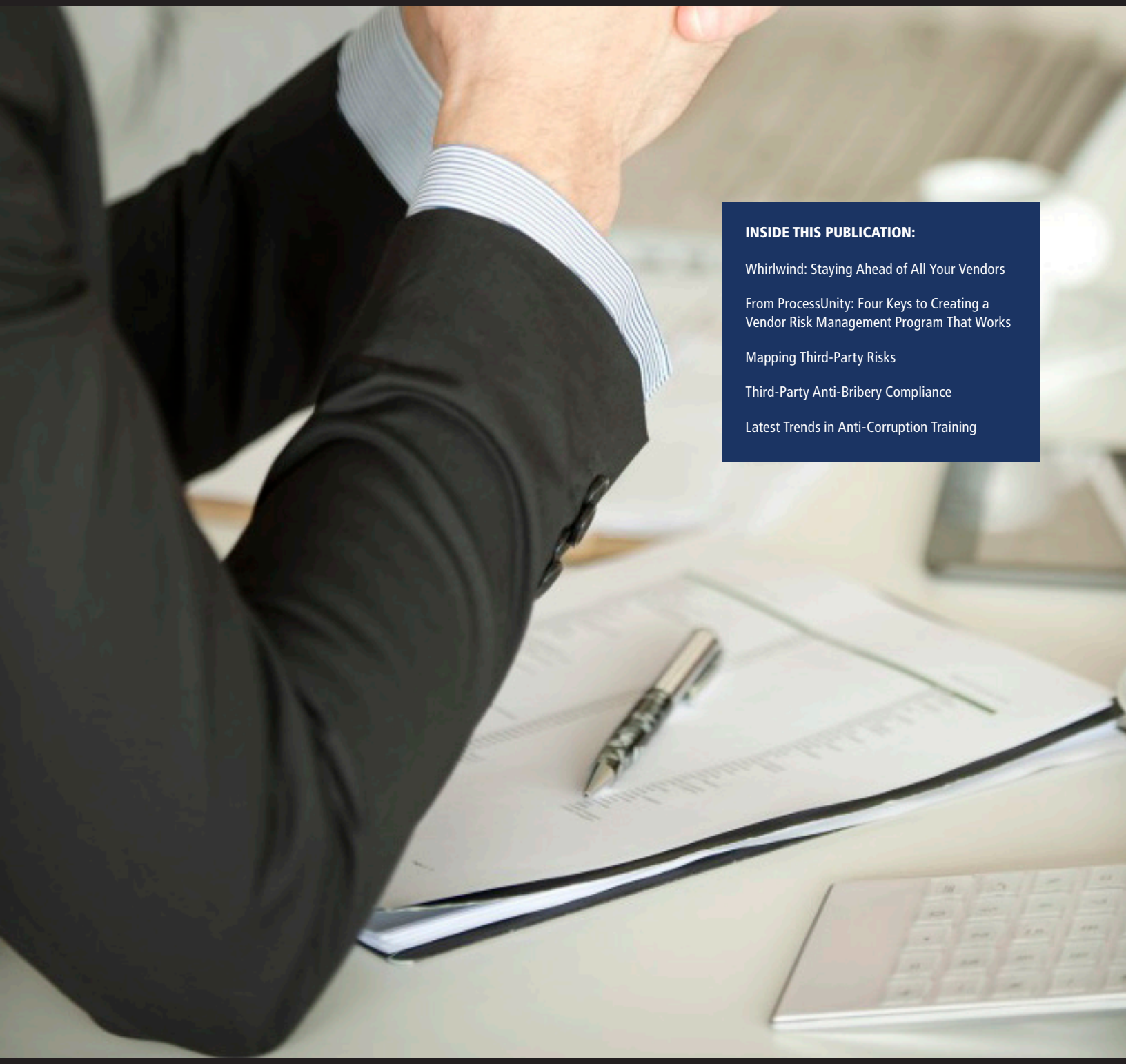
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Managing Third-Party Risks

An e-Book publication sponsored by PROCESS UNITY

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 resources for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

ProcessUnity & Third-Party Risk Management

ProcessUnity is a leading provider of cloud-based applications for risk management. The company's software as a service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes.

ProcessUnity Vendor Cloud helps companies effectively identify and mitigate risks posed by third-party service providers in critical risk areas such as information security, service delivery, supply chain processing, financial processing, reputation and regulatory compliance. Vendor Cloud provides organizations with clear visibility into the business impact of third-party risk via direct links from vendors and their services to specific business elements such as processes and lines of business. Powerful assessment tools enable evaluation of vendor performance based on customer-defined criteria through automated, questionnaire-based self-assessments as well as through detailed audits of vendor controls. Flexible reports and dashboards enable ongoing monitoring of vendor ratings, assessment progress, and status of remediation activity. Learn more at http://www.processunity.com.

Inside this e-Book:

SHOP TALK

Whirlwind: Staying Ahead of All Your Vendors

In our latest Compliance Week executive forum, cohosted by ProcessUnity, we gathered a dozen CCOs to talk about vendor risks and building a systematic approach to handling them.

Participants gather to discuss vendor risk at the recent CW, ProcessUnity roundtable held in New York City.

By Aarti Maharaj

The list of companies tripped up over misconduct committed by their third parties is long. In fact, try recalling a big anti-corruption scandal that did not involve a company's third parties.

Compliance officers straddle the horns of that dilemma: in today's complex business environment, almost every company depends on outside vendors and other third parties to some extent. But for all the efficiency gains that tactic might bring to operations, good luck taming the growing risk exposure that comes along with it.

Pondering a way out of that dilemma was the subject of Compliance Week's most recent executive roundtable, held in New York and co-hosted by Process Unity. The dozen participants all agreed that the idea of vendor governance is a valuable one, even if individual business's success at it varies widely.

"Vendors are an integral part of a company's service, so companies need to have the right risk assessment programs in place to protect themselves," said Sean Cronin, general manager at ProcessUnity.

Data breaches at third parties, for example, have gained increased attention as the number of hacking incidents continues to rise. Cases abound where companies hire third parties that lack the right risk management systems to handle sensitive customer information. Cronin and several roundtable participants said the risk is so acute, they even use data security as the first test to assess the risks of a vendor—if the vendor can't pass that one, the argument goes, don't even bother with all the other risks; just drop the vendor right there.

"Data breaches are one of the most common third-party risk we are seeing in the market," Cronin said. "Risk and compliance officers should evaluate the data integrity practices of a third party to reduce the chances of a breach from occurring—full transparency should be required of all vendors, especially from those who deal with sensitive information."

Several people at the roundtable admitted that even the first step for effective vendor governance—identifying all the vendors your company uses—can be a challenge. Multiple units of a large organization may approach the same vendor from different directions, which can leave the compliance officer unclear both on how many vendors you really have, and how much risk any specific vendor might bring. The question is how to develop a centralized system that monitors all vendor usage and ensures that vendor risks are well-understood.

"If someone were to ask if you know who all your vendors are, that would be a difficult question to answer," said one compliance officer at the forum. "The challenge is prioritizing our focus accordingly, and identifying what types of vendors we need to do more due diligence on and what is the best approach to deal with the big risks."

For many roundtable participants, providing an enterprise-wide view of the company's vendors is only scratching the surface, since the risks within each ven-

dor can be much more challenging: A large vendor delivering office supplies might be low-risk; a small vendor delivering cargo to foreign governments might be hugely risky.

"You must identify 'other' relationships, whether they are affiliates, partners, or other entities that are acting on your behalf, that may expose you to risks—that is considered a third-party relationship." Cronin said. "Once you understand who they are, the next step is reviewing their services and looking for potential loopholes."

"Compliance officers naturally take a risk-based approach to define what diligence must be applied to which third parties, by whom and how often," added Elisabeth Gehringer, chief ethics and compliance officer at Realogy Corp. "Compliance officers should delineate who performs the diligence, who makes the determination on whether the vendor relationship can proceed against any findings, and when diligence must be performed again."

Doing the Risk Assessment

The best practice in theory is that business units themselves perform the risk assessment on vendors they use, with guidance from the compliance officer on how to perform that assessment and what to do when red flags are found. In practice, however, getting that guidance to business units, and ensuring that the guidance itself is useful to them, is no easy task.

Some companies have established committees that provide the necessary information to employees involved in vendor management. Others rely on other "second line of defense" functions like the procurement department (assuming your company has one).

"Our business units have a renewed appreciation for vendor management," said Jay Cohen, chief compliance officer at Assurant Corp. "We have a diverse set of vendors, and our sourcing office drives awareness among employees to ensure that we do a good job at selecting the right vendors and providing effective oversight."

Developing a committee that sets the parameters for effective vendor governance is an emerging idea at multiple large companies. At GE Capital, for example, committees are involved in both "defining the population of what the company views as 'third party' for the purposes of risk management, and this also applies to the ongoing onboarding of vendors," said Luke Brussel, chief anti-corruption officer at GE Capital.

The compliance department helped to define the scope of third-party risk for GE, he said, and then established committees within each business area to evaluate vendor risk and decide whether to ac-

PARTICIPANTS

The following panelists participated in the March 24 CW & ProcessUnity roundtable on vendor risk management.

William Brown
Chief Compliance Officer, Knights of Columbus

Luke Brussel
Anti-Corruption Compliance Leader, GE Capital

David Camputo
Chief Audit Executive, Endurance

Jay Cohen
Chief Compliance Officer, Assurant Inc.

Sean Cronin
General Manager, ProcessUnity

Pete Feeley
Corporate Chief Compliance Officer, Guardian Life Insurance

Noreen Fierro
Chief Compliance Officer, Group Insurance Division, Prudential Financial

Elisabeth Gehringer
Chief Ethics & Compliance Officer, Realogy Holdings Corp.

Michael Gioffre
Chief Compliance & Ethics Officer, Voya Financial Inc.

Christopher Zentner
VP Ethics & Compliance, ACE

cept certain vendors as part of the onboarding process.

In cases where a company has thousands of vendors and monitoring them all might seem too daunting, Cronin suggests that compliance officers start by stratifying vendors based on the services that they offer. "As you start to dig deeper into the process, you get a better sense of which vendors can handle critical data, and what strategies are required to prevent or respond to a risk event," he said.

David Camputo, chief audit executive at Endurance Holdings, walked through his company's efforts to automate vendor management. Camputo explained that an application was established within the procurement function at Endurance to house contracts for the company's vendors in a global database. The database contains information relating to the contract including the name of the employee responsible for the transaction in the first place.

In effect, when the time for renewal comes around, that employee is automatically notified, and the renewal terms and conditions are then reviewed by legal. At any point in the process, a report can be obtained to monitor the vendors and their contracts. "As we grow in size and complexity, vendor dependence is increasing and we instituted a formal process to track and monitor our providers to get ahead of the curve," he said.

Even assuming a company can master its own vendors and other third parties, another concern raised at the roundtable was what to do about your vendors' vendors—that is, your fourth-, fifth-, and other parties? So far regulatory guidance is rather scarce on that point, while reputational risks for those far-off vendors can be sky high. (Think of clothing retailers aghast at the 1,100 lives lost when a sweatshop collapsed in 2013 in Savar, Bangladesh, with Western-branded clothes among the victims.)

Staying ahead of such risks, Cronin said, requires a company to deconstruct its own immediate vendors; from there, crafting best practices to handle fourth and fifth parties gets easier.

"In our experience we have found that it is always good to act like a regulator with your own vendors," Cronin said. "Once a compliance officer has an inventory of their vendors, they need to understand which services those vendors outsource to fourth and fifth parties. They need to regulate their vendors as you would to your own."

Others at the roundtable agreed. "Whether it is a centralized oversight that all companies can rely on or establishing a process where the same work is not repeated is one potential approach," Cohen said. "It is up to the compliance community to really drive new solutions here." ■

OVERHEARD AT THE ROUNDTABLE

What did roundtable participants have to say about vendor risk management? See below for some of their insights.

"Data breaches are one of the most common third-party risk we are seeing in the market. Risk and compliance officers should evaluate the data integrity practices of a third party to reduce the chances of a breach from occurring—full transparency should be required of all vendors, especially from those who deal with sensitive information."

Sean Cronin,
ProcessUnity

"If someone were to ask if you know who all your vendors are, that would be a difficult question to answer. The challenge is prioritizing our focus accordingly, and identifying what types of vendors we need to do more due diligence on and what is the best approach to deal with the big risks."

Anonymous

"Compliance officers naturally take a risk-based approach to define what diligence must be applied to which third parties, by whom and how often. Compliance officers should delineate who performs the diligence, who makes the determination on whether the vendor relationship can proceed against any findings, and when it must be diligence again."

Elizabeth Gehringer,
Realogy Corp.

"Our business units have a renewed appreciation for vendor management. We have a diverse set of vendors, and our sourcing office drives awareness among employees to ensure that we do a good job at selecting the right vendors and providing effective oversight."

Jay Cohen,
Assurant Corp.

Michael Gioffre, chief compliance & ethics officer for Voya Financial.

Noreen Fierro, chief compliance officer for Prudential Financial's Group Insurance Division.

ProcessUnity General Manager Sean Cronin.

Guardian Life Insurance Corporate Chief Compliance Officer Pete Feeley at left; at right, Elisabeth Gehringer, chief ethics and compliance officer for Realogy Holdings Corp.

Jay Cohen, chief compliance officer at Assurant, spoke about his employees' understanding of the company's vendor management process.

Four Keys to Creating a Vendor Risk Management Program That Works

What is vendor risk management?

It wasn't long ago—perhaps just five or ten years—that your company viewed third-party vendors as merely providers of goods and services to your business. The conventional wisdom back then characterized vendors (including consultants and contractors) as suppliers, not business partners, so their problems weren't your problems.

But that was then and this is now. Several influences have forced a change in how you look at vendors and the risks they might pose to your business.

Globalization has created a dependence on critical activities outsourced to an increasing number of partners and vendors; this in turn has fueled a dramatic rise in the third-party ecosystem. It's highly likely that your company now outsources significant aspects of its business to outside providers.

Whether it's accepting orders over the Web, manufacturing various products or components, or delivering services across town or to far-flung markets, your company relies on other companies to fill important needs of one sort or another. In effect, this makes them extensions of your own company. What's more, in this age of globalization, your critical suppliers can be anywhere in the world, including "in the cloud."

Having a dependency on outsiders increases your company's vendor-related risk. Oftentimes, your vendors are provided access to your intellectual property or to sensitive customer information. With significant security compromises making headlines, it's no surprise that most organizations are now requiring vendors to abide by not only their internal standards, but also by industry and governmental regulations surrounding privacy and security.

This heightened regulatory environment is a major influence, designed to force companies like yours to assess and address internal and external risks. It is an effort to maintain stability and to protect customers and investors alike. Regulations such as Basel II, Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Federal Financial Institutions Examination Council (FFIEC) guidelines, among others, mandate that risk management policies extend to third-party vendors, outsourcers, contractors, and consultants. Third (and fourth) parties have the potential to insert risk into your environment because they are outside your direct sphere of control.

Good corporate governance—which can't be legislated—means you have an obligation to understand vendor risk and to actively take steps to mitigate the risk and its impact on your business. Simply put,you need a single, collective view of your vendor risk in order to manage it well and have a more stable and productive business ecosystem.

Why assess vendor risk management?

For most companies, regulatory requirements are the leading reason to conduct vendor risk management (VRM) assessments. External regulators as well as internal auditors are expecting that you thoroughly understand the range of risks inherent in doing business with outside organizations and that you have taken measures to lessen the impact of those risks on your own business.

Regulatory compliance is well and good, but there are additional motivations to assess third-party risk. One reason is to protect your company's brand and reputation from being damaged by another company's actions. Consider how Walmart's reputation was tainted when 112 people died in a fire at a Bangladesh clothing factory in November 2012.[1] The company that owned the factory, Tazreen, was an unauthorized supplier to Walmart's official clothing vendor. Apparel bearing Walmart's Faded Glory label were found in the rubble. While Walmart claimed it didn't know Tazreen was manufacturing its clothing, the Wall Street Journal and other news media associated the global retailer with dangerous working conditions in developing countries.

The more deeply you understand your partners' ways of business, the easier it will be for you to maintain quality of service (QoS). This includes both the level of service to you from your vendors and to your customers from your company—especially when your vendors touch your customers directly; for example, contract personnel who provide delivery and installation on your behalf. Could their behavior reflect poorly on your company? You bet, because customers often don't see the distinction between your company and your contracted service providers.

What is a vendor risk management program?

A vendor risk management program is a formal way to evaluate, track, and measure third-party risk; to assess its impact on all aspects of your business and to develop compensating controls

1 "Walmart toughens regulations after Bangladesh fire," CNN Money. Jan. 22, 2013

Looking further up the supply line

When we talk about third-party risk, we mean the companies that you do business with directly. But those companies also have vendors that become fourth parties to you, and they, too, can pose a potential risk. For example, you may have a partner whose IT systems are hosted in the cloud with a fourth party. This is becoming increasingly common.

You need to understand how well-protected that cloud environment is. There could be yet another business hosted on that same cloud that is a major target for cyber-attacks. A sustained attack could knock your vendor's business offline for a period of time. How would your company be impacted if your partner's IT systems are down? What measures can you take to mitigate that risk?

or other forms of mitigation to lessen the impact on your business if something should happen. A program of this nature gives you consistency for managing your vendors and a way to share information about them within your organization.

Whether your VRM program is manual or automated, homegrown or off-the-shelf, the important thing is that it reflects and enforces your internal controls framework, ensures your compliance with government or industry regulations, and achieves consistency with all of your vendors.

Want a VRM program that works? Follow these four principles

Managing vendor risk is an ongoing process. As your company embarks on or continues with this process, you want to get the most benefit from the program and ensure that the information you learn is used organization-wide to make better decisions. Here are four basic principles that will help you develop a VRM program that works well for your organization:

1. Identify potential vendor risks.
2. Develop effective strategies for addressing higher risk vendors.
3. Align vendor control environments with your internal framework.
4. Implement ongoing oversight utilizing metrics and external alerts.

Let's look at each point and what it means to you.

Identify potential vendor risks

Many companies that implement a VRM program wrongly assume they have to deeply assess every business partner. In fact, doing so can be a waste of time and money. Of the hundreds or even thousands of vendors you work with, only a small percentage may present a serious risk to your business, and these are the ones to evaluate thoroughly.

Some of your vendors deserve far more scrutiny than others because of the strategic role they play in your company's ability to generate revenue from your goods and services. Others may provide a minor service but have the potential to expose confidential information. Therefore, you want to categorize and prioritize your vendors and then focus your assessments on the risks that are germane to specific vendors and the services they provide. Consider which aspects of your business a vendor touches. IT systems? Critical or sensitive data? Business processes? Facilities? Manufacturing? What are your concerns in this area? What is your regulatory exposure? Is this a strategic vendor or a bit player?

For example, suppose you contract a company to accept electronic payments over the Web. This is a high-value partner as it

collects revenue for your company and presents your brand to the world. This company touches your customers' highly sensitive credit card data. A breach of this data could be a financial and public relations nightmare for your company—even if you aren't directly responsible for the breach. Your risk assessment must include what measures the company has in place to secure this data. Furthermore, this company's Web applications might be hosted on yet another service provider's computer systems, dictating the need to expand your risk assessment to this fourth-party company.

Identifying when to assess a vendor is also key. When you start the assessment process early in the relationship, it will help to dismiss any company that has "issues" before you engage in a contractual relationship. For vendors with whom you currently do business, a suggested time to assess them would be prior to renewing the contracts. This will ensure you have time to engage with the vendor and ascertain that control and reliability are adequate for the services they are providing.

Whether your VRM program is manual or automated, homegrown or off-the-shelf, the important thing is that it reflects and enforces your internal controls framework, ensures your compliance with government or industry regulations, and achieves consistency with all of your vendors.

Develop effective strategies for addressing higher-risk vendors

When you have a vendor that your VRM process has identified as presenting substantial risk and you are willing to accept this vendor as a business partner, you need strategies to work with the company in order to keep the vendor's issues from causing you harm. In order to effectively do so, you must consider the following:

» Know what aspect of your business you are trying to protect and focus on minimizing the risk in that area. Make risk mitigation part of the negotiation and contract service-level agreement (SLA).

» Work closely with the vendor to identify and resolve issues to lessen your risk.

» Assess the vendor prior to contract renewal or more frequently; conduct ad hoc reviews when concerns arise.

» Gather outside information about the vendor, such as from Moody's or Dun & Bradstreet, to assess financial health. These services might advise you of issues that are affecting your partner's performance.

» Use metrics to measure the vendor's performance over the time of your relationship. This can show if the partner's service level is improving, holding steady or declining.

» Have a plan of what to do if a vendor exceeds your threshold for risk. You also should have plans for all vendors in the event they are put out of business for any reason, such as an act of nature or financial collapse.

Align vendor control environments with your internal framework

Your company already has a control environment to mitigate your internal risks—likely based on ISO, NIST, or PCI control sets or reflecting the COSO or COBIT risk/process frameworks. Now you must work with your vendor to assess the effectiveness of controls it has in place for the risks you've identified with that company. Realize that you can't get the same level of detail from a vendor as you do from your internal groups.

However, some service providers, including cloud service providers, will have an SSAE 16 SOC report, which provides a control benchmark to use when comparing outsourced service providers. Should your vendor not have an SOC report, your organization can stipulate the need for audits in your vendor agreement.

Regardless of how you gain insight into a vendor's internal

When determining vendor internal control requirements, you should recognize that no single standard or guideline is appropriate for every organization. A best practice is to identify services and capabilities of the vendor and map them to the relevant industry regulations and control standards. This effort can be helpful in meeting compliance goals.

control systems, you should perform a gap analysis of your controls versus the vendor's controls, and work together to close the gap and align the vendor's controls to your specific needs. These needs should be aligned with industry control standards and guidelines.

When determining vendor internal control requirements, you should recognize that no single standard or guideline is appropriate for every organization. A best practice is to identify services and capabilities of the vendor and map them to the relevant industry regulations and control standards. This effort can be helpful in meeting compliance goals.

Implement ongoing oversight utilizing metrics and external alerts

Once you've identified your key vendor risks, metrics are a way to measure actual performance against those risks. Set up metric exception levels and what risks are tied to it. For example, suppose you have a business process that relies heavily on contract workers. You expect some level of worker turnover, but lately the turnover rate has become excessively high. The exodus of workers not only affects your productivity, but it also exposes you to higher training costs for replacement workers and leads to a potential for data breaches by ex-workers who still have system access.

External alert services also can clue you in to potential problems, such as when a key vendor has an issue that may impact your business. Say your vendor is being acquired, or a major lawsuit has been filed against the company. An early alert gives you the opportunity to meet with your partner sooner rather than later to discuss the issue and develop a plan to minimize your risk.

When developing measurements, it's important to identify the business value that is intended to be gained with the function or capability being measured, and then define objective criteria that can be used to assess this value. This is important because subjective measures can be open to interpretation by the audience evaluating the metric. Some measures to consider include:

- Performance and SLA expectations
- Disruption in workflow based on vendor performance
- Expectation or vendor-issued warnings that workflow may be disrupted for any reason
- Breach of the vendor network, systems, or facilities
- Information/results on tests of internal security (physical or systems) controls
- Vendor (non)compliance with laws, rules, regulations, policies, and procedures

Your next steps

Vendors provide value in the expertise and services they offer; however, it is imperative that companies maintain active oversight. As a manager of business risk, you must recognize that when a vendor performs a service or function on your behalf, your company bears the ultimate responsibility for minimizing business exposure and ensuring compliance.

Because varying levels of risk remain with the company that offers the product or service, a strong and comprehensive automated VRM program is necessary to truly understand and track the risks your vendors pose to your business interests. Once you thoroughly understand, measure, and track your risks, you can develop strategies to mitigate them to protect your company from harm.

With effective vendor risk management, your company can minimize the risk of less direct oversight or control and maximize the benefits gained through a well-managed vendor relationship.

Mapping Third-Party Risks

By Jaclyn Jaeger

Many third-party risk-management efforts start with the goal of providing full visibility over a company's universe of third-party relationships.

The trouble is that many companies still don't have a firm grasp on how to achieve that transparency, or even where to begin, exposing themselves to significant legal and compliance risks. Most tend to focus on traditional third-party relationships—such as suppliers, distributors, agents, and joint ventures, for example.

Experts say that they instead cast a broader net to include anyone who represents the company. These third parties might include suppliers' suppliers, resellers, sub-contractors, and more.

Most global companies, however, have thousands—if not tens of thousands of third parties—and all of them must be monitored to ensure they adhere to the company's business practices. To efficiently and effectively get better control over a company's full universe of third-party relationships, the real difficultly is to "take that population of third parties and get it down to a manageable number," Graham Murphy, a principal in KPMG's U.S. forensic advisory services practice, says.

The best advice is starting with a plan. Make inter-departmental team that includes regional and business leaders, as well as any country representatives, he says.

Next, identify the size and scope of your third-party universe—a task much easier said than done. "Most businesses procure services in a decentralized way," Walter Hoogmoed, a principal with Deloitte, says. Without any sort of master list, assembling an initial inventory of third parties involves leveraging multiple databases from multiple business units.

Develop a Matrix

Once you've gathered that master list, you'll want to separate high-risk third parties from low-risk third parties in order to more easily manage the third-party risk-management process, depending on which risk the company wants to focus on most. "If you want to concentrate on the FCPA, for example, you may want to eliminate domestic suppliers," Murphy says. "You should look at your third-party risk mitigation program as a part of your anti-bribery and anti-corruption program."

> "The business manager that runs the business process should own the risk and be accountable for the exposure associated with that third party."
>
> Walter Hoogmoed, Principal, Deloitte

Criteria used to assess and rank the risks associated with each third party include:

- Country of operation where service will be provided;
- Nature of third-party relationship and services provided;

SUPPLY CHAIN RISKS

Below is an excerpt from a recent CW article, which provides results from two similar studies on supply chain risk management

Could companies be doing a much better job of managing supply chain risks? Two studies suggest they could.

From tech companies facing child labor accusations in China to the retail industry reeling from poor working conditions in Bangladesh to the auto industry facing supply chain breakdowns in Germany and Japan, no industry anywhere in the world is immune from a supply chain disruption.

Multinational companies managing a complex web of thousands of suppliers are especially prone to such disruptions—defective products, price volatility, political instability, bankruptcy, and more—because business units and suppliers have traditionally held a narrow view of supply chain risk, ignoring other potential risks (and opportunities) elsewhere in the supply chain.

A survey conducted by PwC and the Massachusetts Institute of Technology found that only 41 percent of 209 global companies surveyed have mature supply chain processes in place to effectively address incidents; 59 percent of companies have immature processes in place. Only nine percent are fully prepared.

An overall awareness of the risks and opportunities posed by the supply chain starts at the highest level of the organization, agrees Andrew Bartolini, chief research officer at supply chain advisory firm Ardent Partners. "It starts with the senior executives having this understanding and making it a focus," he says.

"The backdrop of all of this is the globalization and blending of markets into one another," says Bartolini. The need for companies to have better visibility into, and awareness of, their complex supply chains "has increased in importance, because risks have increased exponentially."

When asked how supply chain complexity drivers have evolved over the past three years, 95 percent of respondents in the PwC survey stated that dependencies between supply chain entities have increased; 94 percent stated that changes in the extended supply chain network configuration occur more frequently; and 94 percent stated that new product introductions have become more frequent.

Source: Compliance Week.

- Type of industry;
- Length of the third-party relationship; and
- Degree of involvement with foreign government officials.

Third parties that pose the greatest risk from an anti-bribery and corruption standpoint are those that have regular interaction with foreign government officials. "Because a company has political connections, it doesn't mean you don't do business with them; it may just mean you want to put processes and controls around that so you don't run afoul of anti-corruption laws," Murphy adds.

Another consideration when vetting third-party risk is to consider how frequently you use that particular third party. "You may want to eliminate those entities that you haven't done any business with over the last few years," Murphy says.

Triaging third parties helps set the wheels in motion for how much due diligence to perform on each third-party relationship moving forward. "Based on the inherent risk of that relationship, you might do more rigorous control testing," Hoogmoed says. For some third parties, a due diligence questionnaire might suffice, whereas others might require on-site audits, he says. Then determine who actually owns the risk. Who is purchasing from that third party? Who is approving payment to that third party?

"Every line of business has some sort of procurement, operation, or relationship manager that deals with third parties on a day-to-day basis," Hoogmoed says. "The business manager that runs the business process should own the risk and be accountable for the exposure associated with that third party."

Remediation Measures

Once you've mapped the total universe of third-party relationships, the next step is to monitor third parties to ensure you are catching and addressing new risks.

Many still perform this task on an ad hoc basis. "They don't have a process in place to address third-party risk from a holistic standpoint," Murphy says. "A lot of companies, for example, are managing the process on Excel spreadsheets, and it becomes very difficult to manage."

Conducting risk management from a manual process standpoint makes it difficult to capture all third parties and the level of risk that each one poses. As a result, Murphy says, "a lot of companies right now are looking to technology-enabled solutions and putting systems in place to really help take them from a manual process to an automated process."

Some third-party risk-management solutions automate the assessment and monitoring of a company's third parties, screening for issues related to sanction and watch lists, politically exposed persons lists, and adverse media, for example.

Other avenues of risk mitigation may include additional due diligence, exercising audit rights, providing third-party training on topics such as anti-bribery and conflicts of interest, and requesting annual compliance certifications. "You may decide to, in the worst case scenario, terminate the relationship," Murphy says.

Also, firms should conduct a thorough on-boarding process when going through a shift in business operations, or a merger or acquisition. A company that is expanding into an emerging market, for example, will want to ensure that it understands all the permits and licenses needed to build new facilities in that region. "Where you can run afoul of the law is by having an agent or third party do a lot of the gathering of that information for you," Murphy says.

"Companies can outsource the function, but they cannot absolve themselves of any responsibility," Murphy adds. "So you want to make sure agents and those acting on your behalf have a good reputation and prior experience." The risks associated with third parties will continue to grow more prevalent as more global firms turn to third parties.

An effective third-party risk-management program doesn't require an unlimited budget or sophisticated tools, but it does need to be tailored to the company's level and type of third-party risk. By not monitoring third parties, and failing to document due diligence processes, companies expose themselves to significant legal, financial, and reputational risk. ■

THIRD-PARTY RISK PROGRAMS

Below is an excerpt from a KPMG report titled, "Third-party risk management" (TPRM). The study highlights typical features of a well-designed TPRM process:

- Automates and stores TPI information through a Web front end, available to internal client personnel and external users as determined appropriate.
- Enables end-to-end visibility through real-time reporting and configurable dashboard capabilities.
- Facilitates a globally consistent approach to intermediary due diligence across client footprints (configured to multiple languages).
- Provides the capability to conduct risk analysis based on an established risk model and assigned scores.

In summary

- Organizations are building third-party risk management programs in response to regulatory pressures, cost reduction programs and in an overall desire to reduce risk by better understanding who they are conducting business with.
- There are certain challenges with building out TPRM programs but they are outweighed by the potential savings and benefits.

Source: KPMG.

Third-Party Anti-Bribery Compliance

By Neil Baker

As companies continue to pursue new customers in emerging markets, they must constantly weigh the benefits of expansion with the risks that lurk there, including bribery and corruption risks. Relying on multiple partners in countries where bribes, gift giving, and mutual back scratching are a normal part of every-day business culture can make the chief compliance officer's job seem impossible.

Delegates at the 2013 Compliance Week Europe conference in Brussels were frank about the challenge of working in emerging markets. But they shared their success stories, too.

Cees Klumper, chief risk officer at the Global Fund, told delegates that his organization financed health projects in 150 countries, many of which have an appalling record for bribery and corruption, lost only 2 percent of its annual budget to misuse—and 80 percent of that it recovered eventually.

"The lesson is that this risk can be managed, albeit it a cost," he said in a session titled, "How Do You Identify Third-Party Risks?"

The Global Fund runs an initial light-touch assessment on every organization it funds, then digs deeper depending on what the initial analysis reveals. Deciding how deep to probe "is an art and a science," Klumper said. With 600 staff performing this kind of work, it's also hard to ensure the assessments are consistent. Another challenge is setting up an effective program to monitor weak partners that have been told to improve.

The corruption threat needs to be seen in context, too. On the Global Fund's list of 19 serious risks, it only ranks at number ten. The organization's purpose is to tackle Aids, TB, and malaria; its biggest risk is that it won't get treatment to the people who need it most. "We have to ask ourselves, given we are there to save lives and fight disease, how much risk are we willing to accept?" he said.

Stefanie Wiegard, global compliance counsel at Johnson Controls Automotive Experience, explained how the company is getting its partners to see the value of good compliance. Johnson, which employs 110,000 people around the world to make car interiors, works with numerous emerging-market joint ventures, including 30 in China.

New partner contracts include clauses on the need to implement a compliance program. But the older contracts typically don't. Some of those agreements have been working well for over ten years, so Wiegard doesn't want to just walk in and start talking about the need to comply with bribery and corruption policies.

"It requires smooth negotiation with the partner," she said. "We show them we have a multinational program and offer them a tailored version. We explain how it helps to keep us out of trouble, and how it's good for them, too, as it could help them to work with other partners."

And what if companies refuse to get on board? "We make it clear that this is a requirement for us; it's a core element of our supplier agreement. If they don't sign, they can't do business with us."

Changing attitudes is an important part of Kyrill Farbmann's job, too. As chief EMEA compliance and ethics manager at International Paper, he has to worry about behavior in a global chain of over 100,000 suppliers.

In many countries, people accept that it's wrong to steal

Pictured above: Cees Klumper, chief risk officer of The Global Fund.

Above, Daniel Kline, managing director for EMEA at NAVEX Global, talks to the crowd at CW Europe. At left is Stefanie Wiegard, global compliance counsel at Johnson Controls Automotive Experience.

> "The lesson is that this risk can be managed, albeit it a cost."
>
> —Cees Klumper, Chief Risk Officer, The Global Fund

from their company, but think it's fine to steal for the company, Farbmann told a session on "Effective Ways to Implement Compliance in Foreign Markets. "We're trying to change that mentality," he added.

His approach is to travel frequently to overseas offices, visiting employees on the front lines. "You have to see them, talk to them, build bridges with them," he said. "And you need to build support from local management. Many of the countries high on the bribery risk indices have a hierarchical culture—if the top people respect you, others will too."

Just Saying 'No'

Sometimes you just have to draw a line in the sand. Andrew Cheung is general counsel for the U.K., Middle East, and Africa at law firm Dentons. He's responsible for Bribery Act compliance in countries where facilitation payments and bribes are endemic and culturally accepted.

He shared his experience of a country where court officials routinely demand extra cash payments for processing papers. "We decided not to do that and said we just wouldn't tolerate it," he said. "We had pushback initially, but now we are known as a firm that just doesn't pay those bribes. Things sometimes happen more slowly, but it wasn't Armageddon."

Dentons also has a comprehensive "pay-no-bribes" rule for the third parties it uses, with each of them giving a signed commitment to operate within the U.K. Bribery Act.

Does that give the firm sufficient protection? "The Act doesn't mean we have to become the enforcers of the law internationally," said Cheung. "We have contracts in place, and we offer training to some key suppliers, but I think that is enough."

The question of how much digging and monitoring is "enough" warranted a session of its own: "How Far Should Companies Go to Combat Corruption?"

Geoffrey Cruikshanks, chief compliance officer and executive vice president of legal service at logistics company DHL, makes new partners complete a due diligence questionnaire if they meet an initial screen of certain risk criteria.

"That peels the first layer of the onion," he told the conference. But Cruikshanks was frank about the limited value of the exercise. Sending out a compliance questionnaire at least shows the potential supplier that DHL takes the issue seriously. But the team sends out thousands of questionnaires each year, and it can't follow them all up. What's more, most of those forms come back "clean"—corrupt people are usually happy to lie.

"The basic problem is you can only do so much," he said. "We want to find problems, but if we miss something we also want some credit for showing that we tried. I wouldn't shy away from that." Other delegates agreed: Due diligence might be a poor way of rooting out corrupt suppliers, but it at least shows the regulators you've done something.

Some organizations push even further. David Halford is head of ethical sourcing and environmental policy at BBC Worldwide, which uses 500 suppliers in high-risk countries to make BBC-branded products, from Dr. Who toys to Top Gear soap-on-a-rope. He told a session on "Ethical Sourcing and Supply Chains" about the intensive compliance work the public service broadcaster puts into managing supplier risk.

The BBC uses local third parties to audit every new supplier and does its own forensic review of any that come back as high risk—that includes any that the initial audit identifies as "totally compliant," a rating Halford regards as too good to be true.

If a potential supplier fails on one of ten critical points—such as use of bonded labor or unsafe living quarters—then the BBC won't work with it. Apart from that, Halford's team will try to help the supplier improve its standards so it complies with the BBC's expectations.

"Many firms say you have to be compliant or we won't use you. So the only way for them to do business is to fake their records. We say we won't work with you if you are not transparent with us," he said.

"What we find in the majority of cases is we rarely come across an evil factory manager. They are good, respectable business people who are tying to do decent trade in challenging circumstances. Most of the time, when there are things that need to be put right they will engage with us." ■

THIRD-PARTY RISK STRATEGY

Cees Klumper, chief risk officer of The Global Fund, spoke at CW Europe on the best approach to identifying and managing third-party risks. An excerpt from his presentation is below.

Up-front due diligence is key

- In-country assessments of the most important third parties
- Assessing their capacities against clearly defined minimum standards
- Providing support to address 'bridgeable gaps' – and following up on a consistent basis
- Background checks of key individuals

Our main challenges

- Efficiency: determining how far to go
- Ensuring consistency
- Translating due diligence outcomes into ongoing monitoring
- Articulating risk tolerances

Source: Cees Klumper presentation.

Latest Trends in Anti-Corruption Training

By Jaclyn Jaeger

Companies are becoming more insistent that third parties they do business with provide their employees with anti-corruption training, and they want more say in exactly how that training is conducted.

The move is part of a shift where companies are increasingly turning the guidelines they have traditionally provided to third parties on anti-corruption and anti-bribery compliance into guardrails that are a condition of doing business.

Microsoft, for example, announced that as of January 2014 all of its business partners worldwide must certify that they're in compliance with Microsoft's Anti-Corruption Policy for Representatives and must further provide anti-corruption training to all their employees who resell, distribute, or market Microsoft products or services.

Companies such as BT Group, Cisco, and IBM have also made compliance training a requirement for third parties, such as resellers and joint-venture partners, if they want to do business with the companies. "Traditionally, anti-corruption and anti-bribery training of third parties has been a weakness for many compliance departments. According to an anti-bribery and corruption benchmarking report conducted by Compliance Week and Kroll Advisory Solutions, for example, 47 percent of 260 ethics, compliance, and audit executives polled said they conducted no anti-corruption training with their third parties at all.

Stephens

The move to demand anti-corruption training for third parties comes as many companies that face investigations or charges of violating the Foreign Corrupt Practices Act are finding the trouble comes not from actions of their own employees, but from actions of those at a third party they are affiliated with.

The Department of Justice and the Securities and Exchange Commission, for example, are investigating Microsoft for potential violations of the FCPA, the *Wall Street Journal* reported. The agencies are reportedly investigating allegations as to whether Microsoft partners paid bribes to government officials in several countries, including China, Russia, Pakistan, Romania, and Italy, in exchange for contracts.

In response to the allegations, Microsoft's Vice President and Deputy General Counsel John Frank, says, "We take all allegations brought to our attention seriously, and we cooperate fully in any government inquiries. Like other large companies with operations around the world, we sometimes receive allegations about potential misconduct by employees or business partners, and we investigate them fully, regardless of the source."

"In a company of our size, allegations of this nature will be made from time to time," says Frank. "It is also possible there will sometimes be individual employees or business partners who violate our policies and break the law. In a community of 98,000 people and 640,000 partners, it isn't possible to say there will never be wrongdoing."

"Our responsibility is to take steps to train our employees, and to build systems to prevent and detect violations, and when we receive allegations, to investigate them fully and take appropriate action," Frank adds. "We take that responsibility seriously."

> "The most challenging part is the preliminary stage of making the business partners aware that they have to fulfill their anti-corruption obligations."
>
> Deborah Luchetta, Compliance Officer and Head of Legal for Mercedes Benz Argentina

According to a Microsoft spokesman, "anti-corruption training is fairly common among most, if not all, IT vendors with their partner communities." If partners have not provided training on anti-corruption laws, however, they either must agree to do so, or must participate in training that Microsoft will make available to them, the company stated. Microsoft's Partner Network Disclosure Guide did not specify what specific course material will be provided to partners, or what the potential costs might be.

BT's Training Requirement

Aside from Microsoft, other companies across industries and across geographies are also now requiring their third parties to undergo anti-corruption training, including London-based telecommunications giant BT Group.

Similar to Microsoft, BT Group also provides training to its third parties on the company's anti-bribery and anti-corruption policies and practices if they do not currently have training in place. "In some cases, the third parties themselves would have good evidence of the training they have in place for anti-corruption and bribery," says Bruno Jackson, director of compliance operations at BT Group.

Cisco also has a firm requirement that third parties ensure employees get anti-corruption training that meets with the networking equipment maker's standards. Cisco "requires our channel partners, distributors, and sales-supporting consultants to complete anti-corruption training." Cisco provides the training, which is available in multiple languages, as an online course.

Then there are other companies that promote third-party anti-corruption training as a strong recommendation rather than a full-on requirement. Oracle, for example, states on its Website that, prior to executing a distribution agreement, the company "strongly encourages" its partners to confirm their understanding of Oracle's business ethics practices by taking its anti-corruption training and passing a short skill assessment.

Siemens "invites" its third parties to take part in the company's training sessions, which are conducted by compliance officers. "We are mainly focused on anti-corruption, anti-

trust, data protection, facilitation payments—all kinds of conduct that can strongly effect us in terms of reputation and financial risks, and in terms of values," says Claudia Maskin, regional compliance officer for engineering giant Siemens.

Many compliance executives say just getting third parties to voluntarily commit to a company's principles of ethics and compliance can be a challenge, never mind making it a requirement. "The most challenging part is the preliminary stage of making the business partners aware that they have to fulfill their anti-corruption obligations," says Deborah Luchetta, compliance officer and head of legal for Mercedes Benz Argentina, a subsidiary of Daimler.

Maskin agrees that the first step is getting third-party affiliates to understand the risks. "Sometimes when a global company does business in a high-risk region—such as Argentina—local business partners aren't always aware of the broader reputational and financials risks posed to a company that is found in violation of anti-corruption laws," she says.

Getting Due Diligence Started

Companies that are not yet requiring their third parties to take anti-corruption training cannot afford to do nothing at all.

Many compliance executives agree that third-party risk mitigation done right starts with the initial screening process. For example, Siemens has embedded into its business processes a "business partner compliance tool," an automated process that ranks business relationships by risk category. "We perform a very deep analysis," says Maskin.

The type of information Siemens analyzes includes former incidents of litigation, relationships with foreign government officials, whether the potential business partner has been charged with corruption in the past, and other red flags. Integrated into the compliance tool is a standard set of due-diligence questions, based on whether the business relationship is categorized as low, medium, or high risk.

BT similarly employs a thorough inspection process before bringing any business partner on board, says Jackson. One way BT achieves that is by subscribing to various third-party databases that automatically scan potential business partners against government watch lists and alerts BT whenever it comes across an entity that has been associated with corrupt activity in the past, he says.

The depth of the due diligence questions posed to a third party "depend on the risk profile of each business partner," says Jackson. Those categorized as high risk—such as the 350 agents BT engages with—go through an "enhanced due diligence" process, which involves a "deep dive to find out everything we can about those particular individuals," he says. "At times, we won't get into relationships if we're not comfortable about the risks or exposure."

Hurdles to Adoption

Before companies can begin to adopt mandatory anti-corruption training of their third parties on a widespread scale, some wrinkles still need to be ironed out. Prior to making such training mandatory, companies should consider the following questions:

- Who will be conducting the training?
- How would training be tailored to local jurisdictions, where anti-corruption laws and regulations may differ?
- Who will pay to provide the training?
- How will employees in geographically remote areas of the world be trained, where they may not have access to online learning management tools?

What will happen to employees who don't complete the training? How will the company ensure that they are being consistent in treatment and follow-up?

At a minimum, third-party risk mitigation needs to be continuously improved. ■

IMPROPER FUNDING OF LEISURE TRAVEL

Below is an excerpt from the FCPA Resource Guide in which the Department of Justice and the Securities and Exchange Commission discuss the importance of anti-corruption training:

Compliance policies cannot work unless effectively communicated throughout a company. Accordingly, the Department of Justice and the Securities and Exchange Commission will evaluate whether a company has taken steps to ensure that relevant policies and procedures have been communicated throughout the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents, and business partners.

For example, many larger companies have implemented a mix of web-based and in-person training conducted at varying intervals. Such training typically covers company policies and procedures, instruction on applicable laws, practical advice to address real-life scenarios, and case studies.

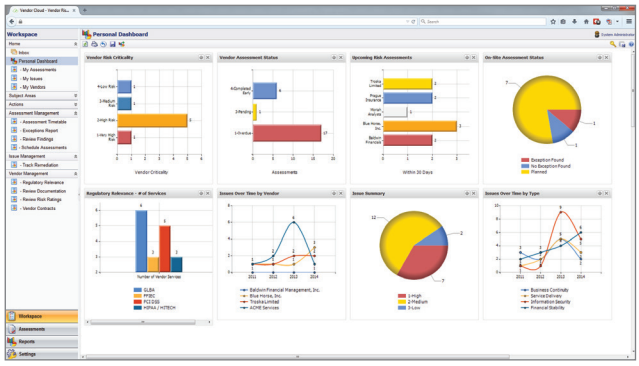
Regardless of how a company chooses to conduct its training, however, the information should be presented in a manner appropriate for the targeted audience, including providing training and training materials in the local language. For example, companies may want to consider providing different types of training to their sales personnel and accounting personnel with hypotheticals or sample situations that are similar to the situations they might encounter.

In addition to the existence and scope of a company's training program, a company should develop appropriate measures, depending on the size and sophistication of the particular company, to provide guidance and advice on complying with the company's ethics and compliance program, including when such advice is needed urgently. Such measures will help ensure that the compliance program is understood and followed appropriately at all levels of the company.

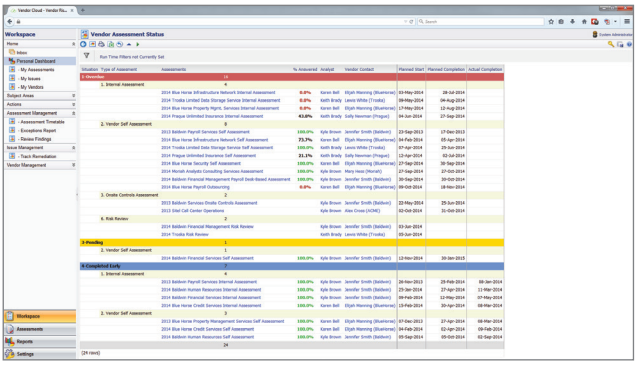
Sources: Justice Department; SEC.

DITCH THE SPREADSHEETS.

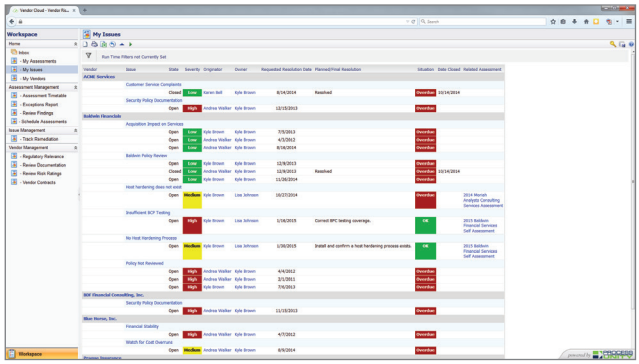
DASHBOARDS



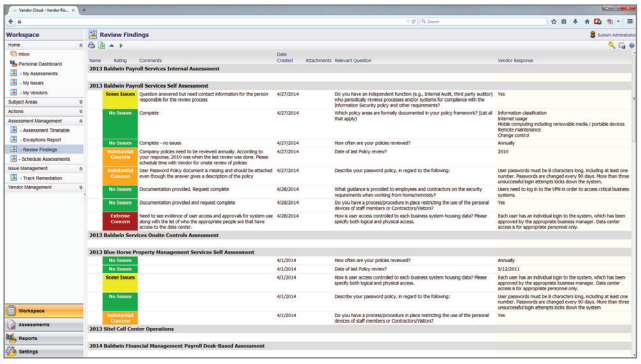
ASSESSMENT STATUS



ISSUES MANAGEMENT



FINDINGS



It’s time to up-level your third-party risk management program.

Eliminate busy work and breeze through regulatory audits with vendor risk automation. Gain real-time visibility into the state of third-party risk and demonstrate to regulators the existence of a consistent, reliable and repeatable program.

ProcessUnity Vendor Cloud effectively and efficiently manages your critical vendors throughout the entire relationship – onboarding, contracts, due diligence, performance monitoring, quality and service level management. Because it’s cloud-based, Vendor Cloud deploys in a few short weeks, complete with your existing documentation.

Learn more about third-party risk automation at www.processunity.com.

PROCESS UNITY

vendor cloud
Powered by ProcessUnity