



How to light the path to best practices
when managing third-party risk

SPECIAL REPORT:

Third-party risk management

As firms increasingly turn to external partners, the risks they acquire can become an internal problem.

Joe Mont has more.



How to insulate your company from **THIRD-PARTY RISK**

As if compliance officers don't have enough on their plates, their responsibilities frequently extend beyond the bubble of their own companies and into the ever-expanding, increasingly risky world of third parties, vendors, service providers, and supply chain partners.

As the business world diversifies and goes global, companies more and more are turning to specialized firms to fulfill complicated niche services and meet product needs. Examples include cloud services, emerging technologies, payment services, licensees, and providers of commodities, parts, and

finished products.

Although vital, the extended enterprise is nonetheless ripe with escalating risk. A recent Deloitte report detailed some of the reasons why: "During the recession, we saw many organizations push more of their business out to third parties in an effort to reduce internal costs across the extended enterprise. Higher volume, of course, can mean higher risk."

There is also an increasing focus by regulators. Outsourcing doesn't allow you to export your compliance obligations, they say. Guidance issued by the Office of the Comptroller



in 2013, for example, laid out its expectations regarding third-party relationships for financial institutions.

It “expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party,” OCC examiners wrote. “A bank’s use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.”

Institutions, it added, “should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.” An effective risk management process throughout the lifecycle of the relationship includes plans that outline the bank’s strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.

The Securities and Exchange Commission and Department of Justice have similarly issued guidance and advisories on the importance of assessing third-party risk, with the latter agency focusing on bribery and violations of the Foreign Corrupt Practices Act.

Steve Klemash, who leads the EY Center for Board Matters, says a starting point for assessing vendor risk starts, quite logically, with an inventory of the third parties partnered with a company.

“Then the assessment gets back to what is the risk appetite, how material are these third parties, and what is the likelihood that something could go wrong? How are they connected to our systems? It actually comes down to just classic business management,” he says. “A lot of these organizations are extensions of the enterprise, but it’s easy to kind of forget about them when you’re just thinking about management and the people you’re seeing, day to day, reporting to the board.”

Third-party risk must be understood as just another facet of overall, ongoing risk assessments. “It’s another risk in the universe,” Klemash says. “[These risks] continue to grow given the nature of how businesses are creating more agility through outsourcing and a contingent workforce. You need to understand it from that perspective.”

ALSO IN THIS SECTION

Results from the Compliance Week third-party risk management survey p4, 7

Five-step lifecycle of third-party risk management p6

Best practices in preventing a third-party data breach p9

How to break up with a third party the right way p13

The risks of outsourcing compliance p16

Why continuous monitoring is crucial for TPRM p19

Boards, more so than ever before, need to consider whether third-party risk should fall under their purview. “If something is material, and it has a high likelihood of having a negative impact on the organization, the board is going to spend more time in that area,” Klemash says. “If it’s not, you’re going to let management do their thing. It all depends upon materiality. The more material and significant a vendor is, then boards are more likely to go in and try to understand the contractual terms, understand security, and what happens if something goes wrong.”

Tom Grundy, senior director of Wolters Kluwer’s U. S. Advisory Services, stresses the importance of managing the “entire lifecycle of the relationship.”

“You’ve got to be able to envision that relationship when it’s in place and plan for all aspects of the lifecycle,” he says. “Are they a good fit in terms of strategy? Are you going to be able to achieve shared goals? There needs to be a quali-

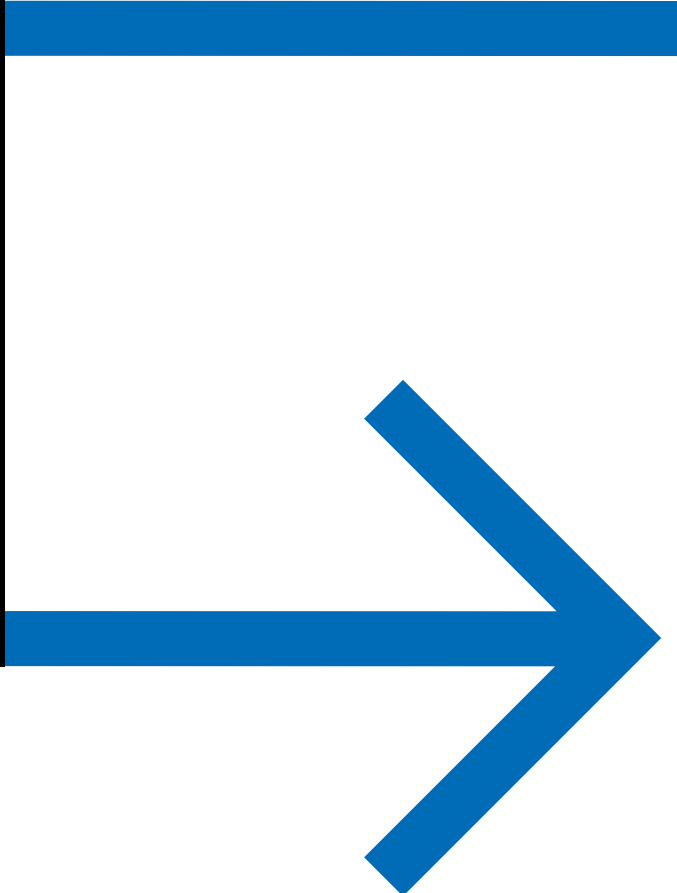
“There needs to be a qualitative and quantitative risk assessment of the relationship. You’ve got to look at the inherent risk that that third party is bringing to the table and into the relationship. If you don’t, you’re going to wind up in a relationship where maybe you’re managing issues that you should have already thought through.”

Tom Grundy, Senior Director, U.S. Advisory Services, Wolters Kluwer



WE ARE REFINITIV

CONNECTING THE
FINANCIAL COMMUNITY
TO WHAT'S NEXT.



We equip a network of over 40,000 global institutions with best-in-class data, technology, and expertise that helps support new, more agile ways of working. From trading to investing, from market regulation to risk, our insight drives the financial industry forward.

Find out how our insight can inform – and transform – your business.

refinitiv.com

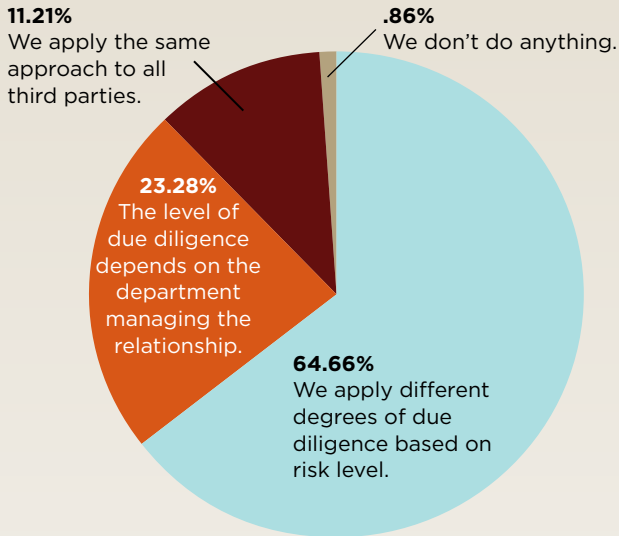
The Financial and
Risk business of
Thomson Reuters
is now Refinitiv.

REFINITIVTM

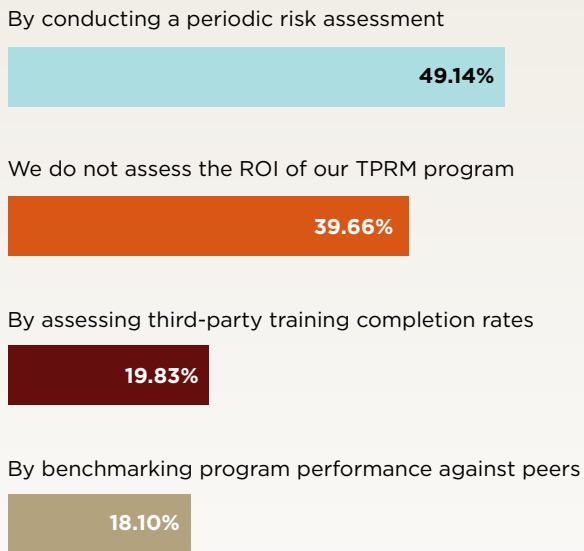
{CW'S THIRD-PARTY RISK SURVEY}

In partnership with Refinitiv, CW asked more than 100 compliance professionals involved with managing third-party relationships at their companies 12 questions related to their TPRM programs.

How does your organization manage third-party risk?



How do you measure the return-on-investment (ROI) of the TPRM program?
(Top four answers)



tative and quantitative risk assessment of the relationship. You've got to look at the inherent risk that that third party is bringing to the table and into the relationship. If you don't, you're going to wind up in a relationship where maybe you're managing issues that you should have already thought through."

"Third-party risk is getting more complex because it bleeds into so many other areas," says Kristy Grant-Hart, founder and CEO of Spark Compliance and author of "How to be a Wildly Effective Compliance Officer."

"There can be cyber-security risk, modern slavery and supply chain risk, and reputational risks surrounding shareholder activism and social media, particularly around political statements," she says. "If you're closely involved with a company that is making political statements and choices, that can be risky as well."

"The lack of centralized systems is really problematic, and mergers and acquisitions make that even harder. Data doesn't work together."

Kristy Grant Hart, Founder & CEO, Spark Compliance

The biggest challenge Grant-Hart sees is in-company compartmentalization and the "silo effect that has made it so that you really don't get the sort of joined-up due diligence that is required, particularly for big companies in this day and age."

"Moving forward, that will be the biggest push and the biggest requirements as we continue to build compliance and develop more mature systems," she says. "The lack of centralized systems is really problematic, and mergers and acquisitions make that even harder. Data doesn't work together."

Contractual language laid out at the start of a vendor relationship and during renewals can provide a framework for the relationship. The requirement for certain risk-related disclosures should be a key element of that process.

"The contract has to be very clear in establishing expectations," Grundy says. "It's a whole laundry list of things. If you look across industries, there are a lot of common elements that go into these. You've got to have a right of access to data and reporting, so that you can understand what they're doing and what they've promised to do for you. You need to have an



understanding about data security standards.”

A company should establish service-level agreements to set expectations, including those for a reporting cycle, Grundy says. You can, for example, set expectations for ensuring consumer complaints are handled according to the agreement.

“If you think you have a problem or even if you get the whiff of a problem you haven’t confirmed yet, you have to tell us,” Grant-Hart says of the preemptive language in a contract that can clarify expectations regarding data breaches, FCPA violations, and sanctions-related problems.

“You try to put the onus on the third party to tell you,” she says. “That’s pretty effective because then it is the obligation of the third party to proactively tell you. You can put damages clauses in there, attorney’s fees, and all sorts of things that make it ugly for the third party if they don’t follow through.”

Contractual language can also impose audit and termination rights. “When getting audit and termination rights, really think about how they are going to work in practice,” Grant-Hart says. “One of the challenges that compliance folks deal with is they need to talk to the business units. It is all well and good to have audit and termination rights, but if it is your most important supplier and it’s going to take six months to get a new one, what are you going to do? Are you really going to terminate that contract right now? Do you have a backup supplier? What would that mean in terms of operations, as well as for the compliance and legal team, and prosecution risk?”

Those conundrums tie into another best practice: assessing critical suppliers as part of a risk assessment. “It is important to assess who you can really not manage without,” she says.

Grant-Hart stresses the importance of internal auditors when vetting third parties.

“Internal audit is often underutilized, compared to the expense of hiring an external audit firm to go in for a two-week-or-longer assignment. Let’s say that there is a requirement for training from your third party, or that they need to submit an annual attestation,” she says. “That is a basic internal audit function checkbox. You can see if they’re not doing a training every year, for example. If you look for the small things, you can sometimes be clued in that maybe you should look for the bigger ones as well.”

A common practice is for companies to send their third-party partners periodic questionnaires and surveys that are intended to better understand their operations, commitment to regulatory compliance, and potential red flags.

Five-step lifecycle of third-party risk management

The management of third parties is absolutely critical in any best practices compliance program, as third parties continue to be the highest risk under the Foreign Corrupt Practices Act (FCPA). The five-steps lifecycle below separates the third-party risk management process into actionable items.

1. Business justification

The purpose of the business justification is to document the sufficiency of the business case to retain a third party. The business justification should be included in the compliance review file assembled on every third party at the time of initial certification and again if the third-party relationship is renewed.



2. Questionnaire

The term “questionnaire” is mentioned several times in the Justice Department FCPA Guidance. It is generally recognized as one of the tools that a company should complete in its investigation to better understand with whom it is doing business. This requirement is not only a key step but also a mandatory step for any third party that desires to do work with your company.



3. Due diligence

Most compliance practitioners understand the need for a robust due diligence program to investigate third parties. You must evaluate the information and show you have used it in your process. If it is incomplete, it must be completed. If there are red flags, they must be cleared or you must demonstrate how you will manage the risks identified.



4. The contract

In compliance terms and conditions, there are a few basic minimum clauses required. These include right to audit, certifications and training clauses, and the right to terminate for an FCPA violation. The 2012 FCPA Guidance intones: “Additional considerations include payment terms and how those payment terms compare to typical terms in that industry and country, as well as the timing of the third party’s introduction to the business.”



5. Management of the relationship

This is where the real work begins, for if you do not manage the relationship it can all go downhill very quickly and you might find yourself with a potential FCPA or U.K. Bribery Act violation. There are several different ways that you should manage your post-contract relationship: auditing, monitoring, training, and ongoing communications, among them.

—Tom Fox

{CW'S THIRD-PARTY RISK SURVEY}

In partnership with Refinitiv, CW asked more than 100 compliance professionals involved with managing third-party relationships at their companies 12 questions related to their TPRM programs.

What due diligence measures do you take to manage third parties? (Top four answers)

We pre-screen our third parties

74.14%

We monitor our third parties

69.83%

We send questionnaires and collect other documentation

69.83%

We require our third parties to attest to our company's policies

47.41%

What third-party due diligence processes, procedures does your firm automate? (Top six answers)

Contract management

43.10%

Collection of questionnaires from business partners

37.93%

Continuous monitoring of third parties against watch lists, etc.

37.93%

Vendor onboarding

34.48%

Everything is done manually/we don't automate our TPRM program

31.90%

Tracking third-party certifications as it concerns acceptance of policies

31.03%

Grant-Hart is not a fan of how these questionnaires are traditionally deployed. The idea is good, she says, but forms overthink and overcomplicate the process. "Most of them are far too long and make my head spin," she says.

Expect pushback from vendors, frequently along the lines that certain disclosures could compromise data privacy laws, especially when employee information comes into play.

"There are really good arguments about why due diligence complies with GDPR and why it's necessary," she says. "Then there are people who feel very differently, and we don't really have a good answer from the EU's [statute]. There definitely are divergent opinions about that."

Nevertheless, the exercise can be an informative one, Grant-Hart says, even as she urges that the questions be streamlined. It is important to ask for information about beneficial ownership, for example, although it may require an outside form to properly confirm the provided information for high-risk parties.

Grant-Hart recently published a list of potential questions on her firm's blog.

Sought-after information should include basic company background: the name of key leaders, whether any executives are current or former government officials, the percentage of ownership of each owner, and whether the company is wholly or partially state-owned.

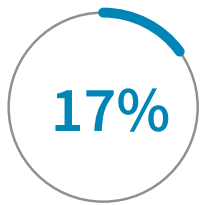
Will the third party be hiring sub-contractors? Is it going to be reimbursed for gifts, hospitality, or entertainment it gives on your behalf? Will the third party be dealing with government officials on your company's behalf?

Other questions to ask:

- » Has the third party or its executives ever been convicted of a crime?
- » Has anyone associated with the third party been indicted, plead guilty to, or been convicted of a crime related to bribery or corruption?
- » Has the company ever been under a consent decree, corporate monitorship, deferred prosecution, or non-prosecution agreement related to bribery or other compliance-related failures?
- » Has the third party been included on a sanctions list?
- » Is anyone at the third party related to or in an intimate relationship with a person at your company?

A questionnaire can also assess other areas of corporate concern, such as modern slavery prevention, data privacy, information security, anti-trust, and confidentiality, Grant-Hart says. ■

MANAGING THIRD-PARTY RISK IS CRITICAL



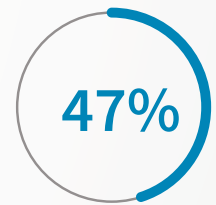
Only 17% of businesses feel they are **highly effective** at mitigating third-party risk*



More than half of businesses have had a third-party **data breach***



63% of data breaches are **linked to** a third-party vendor*



47% said their organization **does not** have a technology solution to help manage vendors**



Get the oversight solutions you need now and let Vendorly® help manage your third-party risk

- Pre-Contract Due Diligence/Contract Management
- Ongoing Monitoring
- Periodic and/or Annual Assessments
- Financial Health Reviews
- Cyber Security Ratings
- Performance Management
- Dashboard Reporting



* According to Ponemon Institute

** According to Vendorly's 2018 Vendor Management Survey

Best practices in preventing a third-party data breach





Examining how “high-performing” organizations handle their third parties lights the path for companies looking to strengthen the weakest links in their data chains. **Jaclyn Jaeger** has more.

A benchmark report reveals some stark differences in governance practices between companies who were able to avoid a third-party data breach in the past year (or ever) versus those who failed to prevent such a breach.

At a time when massive data breaches continue to make headlines, the findings from “Data Risk in the Third-Party Ecosystem” provide some powerful insight into how leading companies are detecting, mitigating, and minimizing data risk associated with third parties and their third parties (so-called Nth parties). The results were based on a survey of more than 1,000 IT and IT-security practitioners in the United States and the United Kingdom who are directly involved in their organizations’ approach to managing data risks.

The study was created by the Ponemon Institute, a research think tank dedicated to advancing privacy, data protection, and information security practices, and sponsored by Opus, a global provider of compliance and risk management solutions. Since 2016, when the study was first conducted, the number of companies to have suffered a third-party data breach increased from 49 percent to 61 percent in 2018. Moreover, third-party data breaches over a 12-month period increased from 34 percent to 45 percent in 2018.

“While corporate executives understand the implications of a data breach or cyber-attack to their business, far fewer are aware of the source of these attacks and the vulnerabilities that their organizations need to address to properly secure their data,” Larry Ponemon, founder of the Ponemon Institute, said in a statement.

In just the latest example, hotel chain Marriott announced on Nov. 30 that its guest reservation database may have compromised the personal information of upwards of 500,000 customers. Marriott determined that the pilfered data was from the Starwood guest reservation database and that there had been unauthorized access to the Starwood network since 2014.

In another recent example, Dunkin Brands reported a security incident, in which a third party attempted to access customer profiles and personal data. “Although Dunkin did not experience a data-security breach involving its internal systems, we’ve been informed that third parties obtained usernames and passwords through other companies’ se-

curity breaches and used this information to log into some Dunkin’ DD Perks accounts,” the company stated.

“Considering the explosive growth of outsourced technology services and the rising volume of third parties, companies need to take control of their third-party exposure and implement safeguards and processes to reduce their vulnerability,” Ponemon said.

Leading practices

Companies that are looking to reduce their exposure to a third-party data breach will want to parse the findings of the Ponemon and Opus study, which conducted a special analysis on “high-performing” organizations, defined in the report as those who were able to avoid a third-party data breach in the past 12 months (36 percent of responding organizations) or that have never experienced one at all (32 percent of responding organizations). The survey then compared these high-performing organizations to those who have experienced a third-party data breach in the past 12 months (42 percent) or ever (59 percent).

Overall, the report found that high-performing organizations have more robust governance practices in the way they manage outsourced relationships. Such practices include, for example, executive-level support, sufficient resources, the evaluation of third parties’ security and privacy practices, and the regular review of third-party management policies and programs.

Any company seeking to better detect, mitigate, and minimize data risk associated with third parties and Nth parties should adopt the following governance practices that, according to the report, high-performing organizations share:

Communicate regularly with senior management and the board. According to the report, 53 percent of respondents within high-performing organizations said they have board- and executive-level engagement, compared to just 25 percent of respondents among organizations that have experienced a third-party data breach. Because the sample size of respondents is so large, even just a five percent variance is “statistically significant,” Ponemon said in a Webinar discussing the results.

A key part of board- and executive-level engagement is



regular communication with the board and senior management. High-performing organizations regularly report, for example, on what steps have been taken to protect sensitive and confidential information from a third-party data breach and the effectiveness of these programs based on how they are assessing, managing, and monitoring third-party security practices and policies, according to the report.

Findings from the report further indicate that having board- and executive-level engagement tends to make it easier to get the sufficient amount of resources necessary to allocate toward managing outsourced relationships, which is critical considering that 60 percent of high-performing organizations said sufficient resources are allocated to managing outsourced relationships, versus just 15 percent of all other organizations.

“That finding seems to indicate that having necessary resources directly correlates to high performers’ success at preventing a third-party data breach,” says Lee Kirschbaum, senior vice president and head of product, marketing, and alliances at Opus. Moreover, simply having board engagement demands that data risk in the third-party ecosystem gets the attention it deserves, Kirschbaum says.

Evaluate security and privacy practices of all third parties.

Although most companies rely upon contracts to ensure that their third parties have appropriate security practices and controls in place, “they don’t necessarily follow through in terms of assessing the security stance and practices of third parties,” Kirschbaum says. According to the findings, only 40 percent of respondents said their organizations evaluate the third parties with whom they share information.

In a contract, for example, some companies might require their third parties to disclose their most critical vendors; show evidence of a vendor management program; and/or include the right of the company to receive fourth-party audit reports. High-performing organizations, however, go one step further by following up on these contractual obligations.

According to the Opus and Ponemon Institute report, 50 percent of respondents from high-performing organizations said, in addition to having in place a contractual arrangement, they further conduct audits and assessments to evaluate the security and privacy practices of their third parties, compared to 31 percent of all other organizations who said they take such measures.

Take an inventory of all third parties and Nth parties with whom the organization has a relationship.

“Ultimately, the only way you can assess risk is if you know who you’re doing business with,” Kirschbaum says. Forty-five percent of high-performing organizations said they create

an inventory of third parties who have access to confidential information and how many of these third parties are sharing this data with one or more of their contractors. In comparison, just 22 percent of all other organizations said they take such an inventory. “A pretty stark difference,” Kirschbaum notes.

When asked why they do not have such an inventory, 69 percent of respondents that did not cited a lack of centralized control over the management of third-party relationships as the reason, and another 48 percent cited the complexity of third-party relationships as another barrier to creating a comprehensive inventory of all third parties.

Require notification from third parties when they share data with an Nth party.

Another stark difference to come from the report is that 38 percent of high-performing organizations, versus just 18 percent of all other organizations, include in their vendor contract a requirement that third parties provide information about possible third-party relationships with whom they will be sharing sensitive information.

“When vendors have access to sensitive information, you can put in place controls to manage it, monitor, and track it,” Kirschbaum says. Being able to track sensitive data handled by the company is not just best practice, it’s a regulatory mandate under data protection laws like the EU’s General Data Protection Regulation. Thus, requiring notification from third parties when they share data with an Nth party is one way to track sensitive data.”

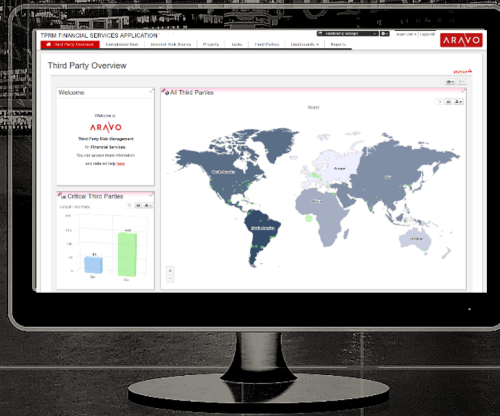
The overarching message to come from this report is that high-performing organizations not only have the internal support that they need, but also are able to keep their finger on the pulse of their outsourced relationships to a far greater degree than their peers with less mature programs. Such high-level governance practices are demonstrated through a strong showing of executive-level support and sufficient resources, the close and consistent evaluation of third parties’ security and privacy practices, and the regular review of third-party management policies and programs.

High-performing organizations will also have in place a third-party risk management committee; greater visibility into all parties with whom they do not have a direct relationship; and some formal level of accountability for the proper handling of the third-party risk management program to keep the program in check moving forward.

For some boards, the risk of a third-party data breach may not currently be top-of-mind, especially if it’s not part of an audit, but Kirschbaum foresees that changing. Even if it’s not a standalone risk, he says, “it may be part of a broader set of risk and compliance discussions and reviews with the audit committee in the future.” ■



ARAVO



FROM RISK TO READINESS

Aravo Solutions delivers award-winning, cloud-based solutions for managing third-party governance, risk and performance.

We help companies protect their business value and reputation by managing the risks associated with third-parties and suppliers, and to build business value by ensuring that their third-party relationships are optimized.

The world's most respected brands count on Aravo for their third-party management programs. Our unrivaled combination of technology and domain expertise helps firms accelerate and optimize their programs, delivering better business outcomes faster and ensuring the ability to adapt as programs evolve.

Built on technology designed for usability, agility and scale, even the most complex organizations can keep pace with the high velocity of regulatory change and achieve a complete view of their third-party ecosystem throughout the lifecycle of the relationship.

Our suite of rapid-time-to-value applications means organizations of any size can stand up a best-practice program, quickly, cost effectively and confidently.



Recognized as a Leader in the Forrester Wave™: Supplier Risk And Performance Management Platforms, Q1 2018.



Recognized as a Category Leader in the Chartis Research RiskTech Quadrant® for Third Party Risk Management Systems 2017.



Awarded the GRC 20/20 Innovator Award for Aravo for GDPR, and the 2016 Value Award for Third Party Management.

"The efficiency, effectiveness and agility Aravo provides demonstrates the advantages of a dedicated third party management platform to meet the needs of a growing, complex and dynamic business environment."

Michael Rasmussen, GRC 20/20

Learn more at: aravo.com



How to break up with a third party the right way

Not all business relationships have a happy-ever-after ending, but there are things both parties can do to mitigate the risks of a third-party breakup.

Jaclyn Jaeger has more.

Breaking up is hard to do—but when it comes to ending a business relationship, it doesn't have to be. All it takes is some careful planning and a little finesse.

Ending a relationship with a third party is in many ways not unlike a personal breakup. Sometimes it ends badly, with one party walking away hurt. Sometimes it ends amicably, with no hard feelings. In both cases, all must eventually come to terms with the reality that the relationship has simply run its course.

There are things that can be done to reduce the risk of such an outcome, however. First, be honest about expectations upfront, and put those expectations in writing. Elements of a third-party contractual agreement should include, for example:

- » The circumstances under which the company can execute a right-to-audit clause;
- » The company's expectations concerning anti-bribery and anti-corruption compliance with corporate policies and procedures, and laws and regulations;
- » What sort of notice the third party must give for sub-contracting out work;
- » The range of commissions or other types of payment that can be made to a third party without extra approvals being needed.

"All of those areas of risk should be contemplated in the contracting process," says Bill Pollard, a partner in Deloitte's Risk and Financial Advisory practice.

Then comes the prenuptial agreement—a contract termination clause, in business speak. The basic elements of a termination clause should stipulate the circumstances under which a termination may be warranted; how many days of notice must be provided; in what form that notice should be provided and to whom; processes and procedures for retrieving proprietary data, documents, and equipment, or for destroying and disposing of sensitive information; and a

timeline for that termination. In short, it's a means to mitigate any risks associated with terminating the relationship, should it come to that point.

As with any relationship, it's best to start off on the right foot, not going into it thinking a breakup is inevitable. "Be mindful of what you can do to keep it a positive relationship," says Dennis Frio, a managing director in Grant Thornton's Financial Services Advisory practice.

Transparency is an important factor in building and keeping trust. "The more transparent the relationship is between the company and its third party, usually the more effective the relationship," Pollard says.

When that transparency starts to dissolve is when red flags can start to crop up, resulting in a potential cause for termination. Pollard cites the following red flags as examples: detailed invoices that become less detailed over time; third parties that start sub-contracting out to sub-vendors; subtle changes in terms and conditions to the contract; or requests for larger discounts.

"A third-party risk management program really should have an element of ongoing monitoring," Woodbury says. As part of that, relationship managers working with third parties on a day-to-day basis should be conducting periodic reviews of the third party.

Those periodic reviews should assess things like the quality, cost, and timeliness of the third party's work, so that the company can get a clearer picture of how well that third party is performing over the course of the contract, Frio says. It's also a good idea to monitor news feeds for any adverse media on that third party, whether there is known litigation or IP infringement cases that may serve as warning.

Finally, where more and more third parties are handling sensitive and confidential employee and customer information, it's also important to monitor any potential data breaches.

"The key is to make sure that whomever is engaging with that third party is making sure they are actively managing the third party and paying attention to these issues," says Gayle

Woodbury, a managing director at Crowe, an accounting, consulting, and technology firm. From there, the company can better assess whether this is a third party that it wants to continue doing business with, she says.

Another question the company should consider: “Is there a reputational risk to making that change? If so, how do we mitigate that risk?” says Woodbury.

Not every situation is so dire that it warrants the termination of a third-party relationship. Some trigger points are obvious, like a breach of contract, or serious concerns about the third party’s ability to perform. If the third party is involved in some type of fraudulent or corrupt behavior or has been named in a government investigation, the likelihood of the company continuing to use them diminishes significantly, Pollard says.

Another obvious trigger point is breach of a confidentiality clause. Some companies stipulate in their contracts that a breach in confidentiality will result not only in termination of the relationship, but further requires the third party to pay back any punitive damages in some cases, Frio says.

Outside of certain egregious situations, the real struggle over whether to terminate a third-party relationship concerns behavior in the gray—for example, a third party that isn’t necessarily in breach of a contract but is being delinquent about its compliance obligations.

The decision becomes even harder when you have the sales and operations teams pressuring others in the company to maintain the relationship if that third party is integral to the company’s bottom-line success. Faced with such pressure, it helps to have full visibility into the third party from all business units, including compliance, legal, finance, sales, and marketing. “If the company doesn’t connect the dots across the organization about a third party, that’s when it’s hard to figure out where to draw the line,” Pollard says.

Providing notice

“You’d want to make sure you have your ducks in a row well in advance of providing notice,” Woodbury says. As part of that, all parties involved in dealings with that third party should be notified, including the relationship owners themselves, other business units, business partners, and customers of that third party.

Just be careful not to forget to provide notice to the third party with whom you’re ending the relationship. There have been situations where companies have gone through the whole internal process of preparing to terminate a third party



but forget to inform the third party itself. “As silly as that sounds, that happens,” Woodbury says.

Another common mistake companies make is to provide a termination notice to a third party, only to realize that they’ve underestimated the time and effort it takes to onboard a replacement third party. “You’ll want to work through your transition plan and have a good estimate on what that’s going to take before you provide notice,” Woodbury says.

Once you’ve provided notice, the next step should be following through with an exit strategy to ensure that activities are transitioned without disruption. An exit strategy should consider things like whether you’re going to bring the services in-house, transfer them to another third party, or discontinue them altogether. If you bring it in-house, you’ll also need to ensure you have the right skillsets and resources in place or figure out how long it will take to put those skillsets and resources in place.

Alternatively, if you’re switching third parties, it’s always good if you can identify in advance who your alternate third parties would be; how much time will be needed to make that transition; and what steps are necessary to onboard that new third party.

It’s also important to ensure that you’ve cut off access to any assets or data that you’ve provided the third party and, furthermore, that you have a plan in place to safely and securely transfer that data either internally or to the new third party. If you have any outstanding invoices, you’ll want to make sure those are all paid off as well.

The company should continue with ongoing monitoring of the third party, keeping in mind that claims can still arise with a third party even after the contract has ended. “Certainly, in the financial services industry, we have seen enforcement actions where that type of situation has happened and the regulators have held banks accountable,” Woodbury says. ■



GET STARTED

As reliance on third parties increases, so does risk. Get started on the path to effective third-party risk management with Lockpath's Keylight Platform.

Request your 14-day free trial at
lockpath.com/vendor-risk

The risks of outsourcing compliance

Using external firms and consultants can bolster the effectiveness of certain compliance functions. Abdicating too much responsibility, however, could draw the ire of regulators. **Joe Mont** has more.

There is no denying that third-party relationships require careful and ongoing compliance reviews. But what if your compliance functions—up to and including the CCO—are themselves outsourced?

The answer depends on what specific compliance initiatives are shuffled off to an outside vendor, why, and whether doing so affects a firm's risk weighting and tolerance.

Does outsourcing compliance make your company better? Or does it run contrary to best practices and open new risks? Those are the questions regulators are asking.

In 2017, the Office of the Comptroller of the Currency issued this warning: "Banks may outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations."

The Securities and Exchange Commission has also cast a critical eye upon outsourced compliance arrangements. In August 2017, it reached a settlement with a third-party chief compliance officer and the firms that retained him for filing incorrect and misleading data. It came to light that neither the outsourced CCO, nor the internal chief investment officer, took "sufficient steps to ascertain the accuracy" of those disclosures.

It is not the first or only time the SEC has chimed alarms.

A 2015 risk alert issued by the Office of Compliance Inspections and Examinations noted that, faced with budget constraints and a shallow talent pool, financial firms were more frequently turning to external professionals to supplement—if not entirely run—their compliance programs. Updating firm policies and procedures, preparing regulatory filings, and conducting annual compliance reviews were

among the services increasingly farmed out to external consultants and law firms.

Examination scrutiny

As part of what it called the Outsourced CCO Initiative, OCIE evaluated these arrangements at nearly 20 firms. "Significant issues" were identified at registrants with an outsourced CCO who also served that role for multiple firms or that "did not have sufficient resources to perform compliance duties."

Several of the examined outsourced CCOs, for example, used standardized, generic checklists that did not fully capture business models, practices, strategies, and compliance risks. Others infrequently visited registrants' offices, conducted only limited reviews of documents and training on compliance-related matters while on-site, and had limited visibility into, and authority within, the organization.

"A CCO, either as a direct employee of a registrant or as a contractor or consultant, must be empowered with sufficient knowledge and authority to be effective," the OCIE said, adding that a firm is ultimately "accountable for its own deficiencies."

Although the risk alert was intended to nudge firms that outsource the role of CCO, by further clarifying a view of what a robust compliance program must exhibit, the SEC offered advice and potentially a safe harbor for less comprehensive arrangements.

"The SEC has not banned outsourced compliance in any way or said it is presumptively disfavored, but reading between the lines you get the feeling that, in an ideal world, it is not how they would like to have regulated entities go about things," Jason Halper, a partner at Cadwalader, Wickersham & Taft, told Compliance Week when he was a partner at Orrick, Herrington

"The purpose of the whole outsourcing platform is really to handle all the low-hanging fruit out there in terms of tasks for a compliance department."

Jennifer Kopcsik, Managing Director of Client Development, ACA

& Sutcliffe in December 2015. “If you do delegate, you need to understand who the vendor is, their relationships with your company, and potential risks associated with that firm.”

There are, despite certain risks, aspects of a compliance program that do benefit from an external assist. A common use of third parties in this context is to help improve training programs. They can also facilitate employee “helplines” by impartially gathering and reporting employee concerns about workplace practices.

The view from consultants

ACA Compliance Group is a provider of governance, risk, and compliance advisory services. The firm was founded in 2002 by former SEC and state regulators and has since grown to more than 700 global employees.

“The purpose of the whole outsourcing platform is really to handle all the low-hanging fruit out there in terms of tasks for a compliance department,” says Jeremy Kopcsik, managing director of client development at ACA. “A typical client for us is a smaller department of five or fewer people. They just don’t have the bandwidth to deal with a lot of things. We take on these tasks for them, so they can then focus their attention on the more high-profile tasks they need to address internally.”

Among the increasingly in-demand services that might otherwise tax both internal manpower and expertise: social media reviews, e-mail surveillance, and marketing reviews. “There are compliance departments that have two or three dedicated individuals where all they do is review that firm’s marketing material, just a very time intensive task,” Kopcsik says.

Among the touted benefits of third-party compliance advisors is speed. “There’s no ramp-up time, there’s no training, there’s no implementation delay,” Kopcsik says, adding that “outsourcing allows firms to scale their compliance department” without the added costs and training that come with a new hire.

Guy Talarico sees third-party compliance services as a means to keep pace with the complex regulatory landscape that has constantly evolved since the 2008 recession and passage of the Dodd-Frank Act. He is founder and CEO of Alaric Compliance Services, a firm that provides outsourced

compliance solutions for the financial services industry.

The firm provides outsourced CCOs in addition to preparing disclosures, firm monitoring and testing, and mock audits.

“The dust is still settling,” Talarico says, reciting an alphabet soup of domestic and international rules and issues firms must consider, from FCPA and FATCA to Brexit and GDPR. “It’s harder and harder to be an expert.”

“[The regulatory landscape] really is so diverse, and so complex, that unless you’re a JP-Morgan with thousands and thousands of people in all kinds of specialized roles, you need to have outside support to effectively get these things done,” he adds. “Every day, there’s something in the news” for advisors to pay keen attention to.

In Talarico’s view, despite accessional risk warnings, the SEC has actually validated the value of outsourced compliance services.

“You often see, in enforcement actions, that the Commission requires firms to hire independent consultants as part of the remediation to fix what they found,” he says. “Even the SEC is explicitly dictating the hiring of third-party compliance, consulting firms to help registrants meet their demands.”

What are firms looking for as they consider these services? Among the attributes they seek: knowledge, experience, and interpersonal skills, the latter vital to ensure open lines of communication.

Firms, according to Talarico, also typically ask—or at least should—for specific details about the engagement. How much time are they going to spend on site? How will they interact electronically with the firm? Do they have the necessary resources?

“This has to work both ways. The [external] CCO has got to feel comfortable that the firm is being open and honest and giving them all they need,” he says. “They need to know that the firm is going to listen to them when they raise an issue, and management doesn’t just say, ‘Oh, don’t worry about it.’ You don’t want to be in that role.” ■

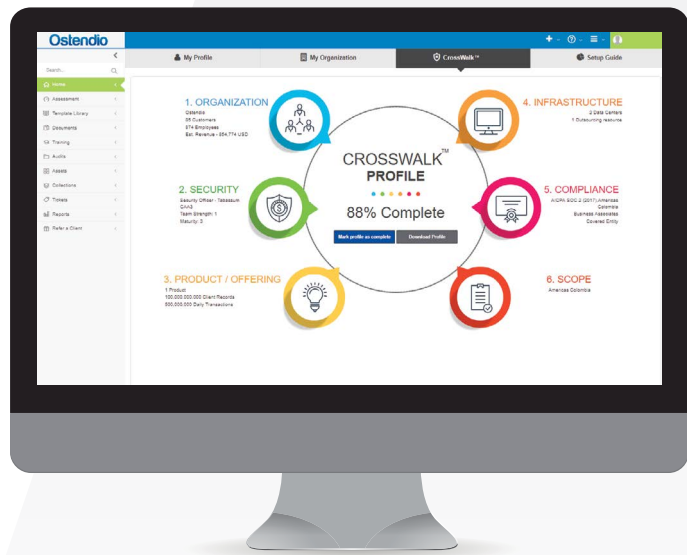


Automate your compliance and risk management program.

Organizations of all sizes are struggling to manage data security and privacy compliance challenges. Ostendio offers a comprehensive solution to effectively manage over 100 global privacy and security standards and regulations.

Ostendio's MyVCM saves you time and money by streamlining your processes with:

- ✓ Workflow management
- ✓ On-boarding
- ✓ Contract management
- ✓ Vendor and employee training
- ✓ Document management
- ✓ Asset management
- ✓ Vendor audits
- ✓ Self-assessments



Request a free demo of our software at www.ostendio.com/request-a-demo

Why continuous monitoring is crucial for TPRM

Three cautionary tales demonstrate the potential trouble a company can find itself in when third parties are not actively monitored, writes **Tom Fox**.

Your corporate compliance program requires all third parties to be certified through a rigorous five-step process that is renewed every two years. But what happens during the interim period? If you are not actively monitoring your third parties at all times, you could be setting the organization up for a Foreign Corrupt Practices Act (FCPA) violation. Consider these three examples:

1. Let's say you have assured yourself that your third-party agent does not have any politically exposed persons as owners, beneficial owners, or principals. You're confident of this fact at the start of the relationship, but are you monitoring it via public data resources on an ongoing basis? If you're not, what happened to Hitachi in South Africa about a decade ago could happen to you. In that case, Hitachi's third-party agent brought on board a member of the African National Congress and transformed the nature of the relationship, which ultimately led to an FCPA enforcement action.
2. Beyond a change in ownership or in the principals, what happens if there is a change in the commission rate paid to a previously approved third-party agent? Consider Hewlett-Packard and its 2014 FCPA enforcement action. One of the three bribery schemes unearthed on the company occurred in Mexico, where HP-Mexico wanted to use a corrupt agent involving a deal with Pemex, because he had a very close relationship with the Pemex official who would be making the decision on the contract. HP-Mexico even signed a contract with this agent that detailed his description of services included an "influencer fee" for which he would receive a 25 percent commission. This agent apparently could neither meet the company's due diligence requirements nor accept its mandatory commission rate, or both. Whatever the reason, the corrupt agent was not approved as an agent on the Pemex deal. So HP-Mexico simply sub-contracted this agent to an existing, previously approved HP channel partner. HP-Mexico then said it needed to raise the commission rate of this channel partner from 1.5 percent to 26.5 percent because this channel partner was now "managing discounts with Pemex," which, not

so coincidentally, this channel partner had never done. Because this channel partner was previously approved by compliance, the request for an increase in commission rate was never submitted to compliance for approval.

3. Now consider this scenario on a much grander scale, as outlined in Panasonic Avionics' 2018 FCPA enforcement action. The company had 13 corrupt agents in its Asia region, which had engaged in bribery in the past and could not pass due diligence scrutiny under the company's compliance regime. So what did the employees in its Asia region do to get around this problem? According to the deferred prosecution agreement, after these corrupt agents were formally terminated by the company, Panasonic Avionics employees secretly continued to use the agents by having them rehired as sub-agents of a previously approved third party, which had passed PAC's due diligence checks. Through this fraudulent process, Panasonic Avionics employees hid more than \$7 million in payments to at least 13 sub-agents, which were used to facilitate bribery and corruption. Similar to Hewlett-Packard, the Panasonic Avionics compliance function did not have any mechanism to detect or prevent this subterfuge, such as effective internal controls over the lifecycle of third parties within their organization. At Hewlett-Packard, there were no internal controls in accounting, finance, or accounts payable that could have alerted the compliance function when a previously approved third party had its commission rate increased by 25 percent. In addition, at Panasonic Avionics there was apparently no red flag raised when a previously approved third party's total commission payments jumped more than \$7 million in one year.

There must be ongoing monitoring, communication, and functioning internal controls of third parties. The compliance function should have visibility into internal controls around third-party payments. If there is a big increase in a commission rate, it should be investigated before it is approved. If there is a spike in annual commissions paid, it should be investigated after the fact. And, as always, document everything! ■



Third-Party Risk: Are you scoring an own goal?

What are the main challenges around ensuring bribery and corruption does not impact your business through your third-parties and counterparties? Also, what steps can you take to understand these hidden third-party risk factors, no matter where they may lie?

1. Companies say that tackling bribery and corruption in their global operations is one of their biggest challenges.
2. We have outlined some of the steps required to implement a successful anti-corruption compliance program.
3. A third-party risk assessment should involve constant monitoring and input, as a company's risk profile can change at any point in time.

With a surprising 92 percent of respondents to our recent True Cost of Financial Crime survey saying that they viewed bribery and corruption as a common practice, it's clear that alarm bells should be ringing for regulators and legislators across the globe.

According to the report, an estimated US\$309 billion is lost in turnover to bribery and corruption each year. That's bigger than the \$239 billion lost to fraud and \$267 billion for money laundering.

In contrast, it is encouraging that 94 percent believe that tackling bribery and corruption throughout their global operations is important, and one of the two areas that companies find the most challenging.

However, it is an area that most companies have said they find challenging to prevent in their global operations. This makes it essential that they identify ways to get a clearer picture of their risks.

In a separate third party-risk survey conducted in late 2017, we asked which top three regulations had the most impact on a company's operations.

In North America and Europe, anti-bribery and corruption legislation was at the top, while it was second on the list in Asia Pacific.

The good, the bad and the ugly

Robert Barrington, Executive Director of Transparency International UK, said there was often a mis-match between corporate and public views of the financial crime problem.

In an article for the True Cost of Financial Crime report, he said: "The key point is that companies think of themselves as victims; the public think of them as perpetrators."

The usual defense of the 'rogue employee' somewhat neglects the concept of corporate accountability and responsibility.

Is it a coincidence that more of these rogue employees are apparently found in companies with poor governance, weak compliance, a culture of misaligned incentives and over-aggressive sales targets?"

In order to fight corruption and bribery in business, it is crucial to have the support from the leadership right down to the far reaches of its upstream and downstream associations.

Third party risk assessment

We have outlined some of the steps required to implement a successful anti-corruption compliance program.

1. COMMITTING TO COMPLIANCE

- Top down commitment
- Financial commitment
- Anti-corruption policy objectives
- Employee guidance

2. RISK ASSESSMENT OBJECTIVES

- A good risk assessment involves a process of constant monitoring and input which should consider:
 - third-parties location
 - business sector
 - business partners
 - transaction types
- A risk assessment document should be:
 - constantly revised
 - kept up-to-date
 - is benchmarked against

3. RESEARCH & REPORTING

- Relevant and regularly reported metrics
- On going due diligence
- Undertake added measures for third-parties that are deemed to be higher risk

One part of a sound anti-corruption program is a thorough risk assessment of the third party, involving constant monitoring and input, as a company's risk profile can change at any point in time.

This could be due to many factors, ranging from operational difficulties and financial troubles through to associations with "bad actors."

Over the last two decades, there has been substantial progress by companies in developing and implementing anti-corruption programs. Such programs are vital to the success of international efforts to combat corruption.

TRANSPARENCY INTERNATIONAL

Some of the points to consider during onboarding are the third-party's geographic location, the business sector it operates in, their business partners and the type of transactions they undertake. Also, when conducting a refresh: has anything changed?

One way or another?

From recent reports, it seems that organizations can be too complacent when it comes to putting safeguards in place to avoid being part of the problem.

On the other hand, they also realize the extent of the challenge it brings and are keen to find solutions.

It is safe to say that the problem of corruption is not going away any time soon.

Partnering with an organization like ours can provide you with a clearer picture of the risks facing your business and deliver insight towards what you need to focus on most.

Our risk intelligence helps you make the best possible decisions, given what is known, at any point in time.

Discover World-Check, the trusted and accurate source of risk intelligence: refinitiv.com/en/products/world-check-kyc-screening

Visit refinitiv.com

