Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Data breaches impart third-party risk lessons

3M's John Ostergren on supply chain, third-party risk management

How do your risk oversight processes stack up?

Collaboration enhances risk management in financial services

Elements of a best-in-class TPRM program

New cyber-rules coming for defense contractors

More firms exiting third-party vendor relationships

Taking the pulse of third-party Risk Management Policies

PROTECT YOUR BRAND AND STRENGTHEN THIRD-PARTY COMPLIANCE

Innovative Solutions for Compliance and Procurement Professionals

ComplianceDesktop®
COMPLIANCE TECHNOLOGY PLATFORM

Integra Check®
Integrity due diligence

Supplier Integrity®
Supplier Management Platform

- Manage the full spectrum of your global compliance and integrity risk program, including third-party management
- Take advantage of a single, innovative platform with holistic and robust reporting
- Make the most of your existing technology investments with easy integration capabilities and an anytime, anywhere mobile solution
- Receive report analysis that is relevant, current and accurate with local insight and global expertise
- Have access to on-the-ground resources in over 145 countries
- Make informed decisions from relevant information produced by a Professional Services team composed of lawyers, accountants, auditors, certified compliance and fraud experts
- Complement existing third party management tools with compliance and integrity risk protection
- Quickly assess the risk of prospective suppliers and identify potential issues
- Efficiently perform screening and due diligence based on the supplier risk
- Easily integrate the automated workflow into any existing process

Red Flag Group®

Turning Compliance Into A Competitive Advantage®

www.redflaggroup.com | info@redflaggroup.com

Inside this e-Book

Data breaches impart third-party risk lessons 4

3M's John Ostergren on supply chain, third-party risk management 8

How do your risk oversight processes stack up? 12

Collaboration enhances risk management in financial services 17

Elements of a best-in-class TPRM program 22

New cyber-rules coming for defense contractors 27

More firms exiting third-party vendor relationships 31

About us

COMPLIANCE WEEK

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

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

Data breaches impart third-party risk lessons

The data breaches at Yahoo, Equifax, and the SEC send a collective warning to organizations everywhere to improve their own third-party risk assessment. **Joe Mont** reports.

In terms of infamous data breaches, the past year has a bad one on the cyber-security battlefront.

In recent days, we learned that a 2013 data breach at Yahoo was underreported. The reality: every single user, all three billion of them, had their information compromised.

Watching the watchman, over at the Securities and Exchange Commission, it announced that an incident previously detected in 2016 provided the means for illicit trading gains. A software vulnerability in the test filing component of the Commission's EDGAR system was exploited and resulted in access to non-public information.

And, of course, there was the headline-feeding revelation that a massive data breach that hit consumer credit rating firm Equifax, potentially exposed the personal information of 143 million customers.

While each of these parties struggles with internal investigations and external scrutiny, the rest of the corporate world needs to be on their guard. We look at three ways the recent breaches should resonate with all companies that are serious about compliance and cyber-security.

Given the regulatory refrain that companies inherit the sins of their third parties, intriguing (and frightening) risk dilemmas emerge.

Where the Equifax breach can get really scary is that its partner companies need to assess whether when their customers' data was similarly compromised.

As for the SEC, given that its collection of confidential, soon-to-be material data shared through EDGAR's pre-filing functionality was compromised, it may be wise to think of it as a third party and not just a regulator.

All of these incidents shed a light on the much broader picture of third-party data risks. A recent study, released in September 2017, underscores the dangers.

Opus, a provider of global compliance and risk management solutions, partnered with the Ponemon Institute for a study, "Data Risk in the Third- Party Ecosystem." It uncovered the security risk companies face when sharing sensitive information with third parties.

Among the findings: 56 percent of businesses have had a third-party data breach (a seven-percent increase from last year); 84 percent lack a complete inventory of third parties; 63 percent don't know when a third party shares data with a fourth party.

The survey also found that 42 percent of companies experienced cyber-attacks against third parties that resulted in the misuse of their company's sensitive or confidential information.

The survey found that the effectiveness in managing third-party risks remained low. Fewer than one-in-five companies (17 percent) felt their organizations effectively managed third-party risk. Less than half of all respondents agreed that managing outsourced relationship risks is a priority in their organization.

A key deficiency identified in the study was that "companies lacked visibility into their third-party relationships." More than half of the respondents said they do not keep a comprehensive inventory of all third parties with whom they share sensitive information. Only 18 percent of respondents know how external parties access and process data.

"Cyber-criminals continue to target weak links because companies are failing to successful manage risk," says Dov Goldman, vice president of innovation

& alliances at Opus. "Smart companies are learning from those that have implemented clearly defined third-party risk management programs supported by good governance and robust technology."

The study noted a strong correlation between implementing governance and IT security practices and a reduction in breaches. These practices include: evaluating security and privacy practices of all third parties; supplementing contractual agreements with audits and assessments; creating an inventory of all third parties with whom information is shared; and ensuring oversight by the board of directors.

Organizations whose board of directors requires assurances that third-party risks are effectively being managed were 10 percent less likely to experience a breach, the report says.

"It is critical for organizations to actively manage their third-party interactions by implementing standard processes, including inventory and policy review and documentation, senior leadership, and board member oversight, as well as other safeguards to reduce their vulnerability," says Dr. Larry Ponemon.

Do you understand your holistic population of third parties? That is among the crucial questions a company much ask, according to Daniel Maloney, senior manager at Accenture and an expert in third-party risk management.

Questions include: What data is accessed and by who? Is there a segregation of duties and controls? Who has access to servers and why? Why do they need this data? Are they collecting too much data?

"A third party is basically anyone you have a contract with," he says. "It is not just vendors or people you pay. It is anyone who you might be doing business with. It includes anyone working on commission, debt collectors, charitable organizations, marketing partnerships, joint ventures, and things like that."

Maloney adds: "You need to understand which third parties have access to your data. Once you understand, for example, that 2,000 out of 10,00 parties have access to your data, then you need to understand where that data is, including which country because each one has different data regulations."

With that roadmap, it is time to ensure that those parties have proper controls. Maloney says most firms do a good job initially. Where they start to fail is ongoing maintenance. "In year three, four, or seven of the contract, are the controls still up to speed, or have they not kept up with the times? Controls, even three years ago, did not take into account cyber-security," he says.

A risk-based approach to assessing the inventory of third parties is another priority. "A cloud computing vendor is going to be treated differently than an office supply vendor you buy pens from," Maloney says. "A particular firm may have no access to data but is critical to the business. You might, in that case, care more about business continuity and financial liability."

A company, based on its size and influence, might consider being a cyber-security evangelist to its family of partners, because relationship management, when it comes to information security, can be vital.

"A lot of third parties and vendors are very small companies," Maloney says. "When you want to go and review their cyber-security and information-security policies you are actually telling them things that also help yourself. Yes, you are protecting your data, but you are also helping them because they may not have the resources, skills, or breath of knowledge needed to know what they are missing. Treat them more as a partner and you help them as well as yourself."

"The big thing is understanding third parties, understanding who has access to data, and where their risk exposure is, from a data perspective or not," Maloney says. "It may be geopolitical or maybe reputational, but understand that risk exposure and where it is coming from. Make sure that when you review your third parties you do it initially and then on an ongoing basis that corresponds to the risk of the activity, knowing that the risks may change over time. You could have somebody critical today who becomes non-critical tomorrow, or vice versa."

And if dealing with those regulators who are collecting data, Maloney has some key advice: "Treat them just as you would anybody else," he suggests. "You have a program and should do the same things for everybody; you shouldn't do anything different." ■

Crowe Horwath

Crowe Horwath

Recognized Leadership in Third-Party Risk Management Services

In today's complex business environment, organizations are expected to provide innovative solutions quickly and with precision. In order to remain competitive, your organization probably works with more third parties – and in different ways – than ever before. Third-party relationships, which include suppliers, vendors, joint ventures, and others, are intricately involved in ongoing operations, and they form the new ecosystem of organizations today. Such relationships can complicate your organization's risk profile and expose it to third-party risks from sources around the globe. At the same time, new types and categories of risk continue to emerge, so staying ahead of the game is challenging.

Crowe Horwath can help your organization assess and manage risks and maintain successful third-party relationships across the ecosystem. With more than 1,000 risk consultants around the globe, Crowe risk specialists combine risk management expertise and real world experience in a broad range of industries with a deep knowledge of third-party risk, related risk and compliance disciplines, and supporting technology systems.

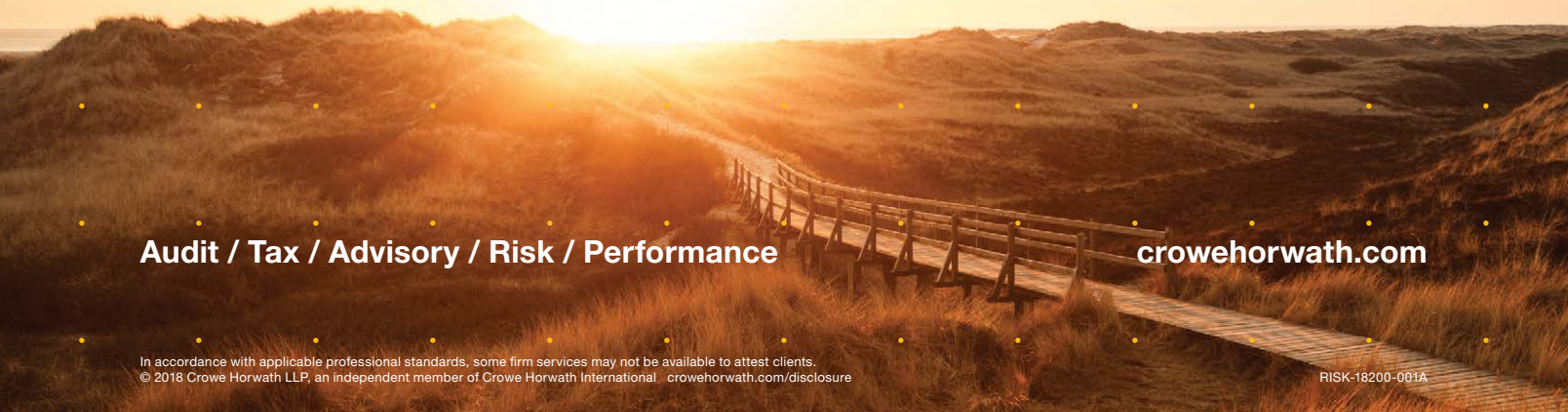
Crowe offers a comprehensive portfolio of third-party and vendor risk management services, including:

- **Program consulting:** We assess all program areas to identify maturity levels and compliance gaps, and we develop practical ways to advance program capabilities.
- **Independent program reviews:** We provide assurance through independent testing, monitoring, validation, and audit of third-party risk management activities.
- **Third-party and fourth-party assessments:** We execute on-site and remote assessments of third parties located across the globe and spanning multiple risk domains.
- **Technology enablement:** We offer a robust third-party management solution, aligned to regulatory guidance and best practices, that can help organizations manage risk, compliance, and performance across their third-party and fourth-party populations.
- **Managed services:** We bring people, process, and technology together to provide a managed service to support third-party risk management programs.

To learn how your organization can experience the Crowe difference, visit crowehorwath.com/tpr or contact:

Michele Sullivan
+1 574 235 6824
michele.sullivan@crowehorwath.com

Gayle Woodbury
+1 630 586 5325
gayle.woodbury@crowehorwath.com



Audit / Tax / Advisory / Risk / Performance **crowehorwath.com**

RISK-18200-001A

3M's John Ostergren on supply chain, third-party risk management

Smart companies understand which risks to take on in the interest of growth and which ones must be shunned, says John Ostergren, director of environment, health and safety at 3M. **Joe Mont** talks more with Ostergren on managing risk.

The idea of knowing and wantonly taking chances would seem to run counter to most corporate cultures. For most businesses, however, doing nothing is the biggest risk of all.

That is the message from John Ostergren, director of environment, health and safety at 3M. It is important to take a longer-term view of risk, he says.

We chatted with Ostergren about risk management, corporate and shareholder debates over "long-termism" and short-termism" and taking a

quarter century view when it comes to assessing the value of an investment, not just results over a financial quarter.

3M is a global science company with $30 billion in sales, and 90,000 global employees.

CW: What path led to your career specialty at 3M?

JO: I'm a lawyer by training and a scientist at heart. I did my Ph.D in environmental geochemistry before I went to law school.

That's the foundation that helps me connect with a science-based company, and that connection is pervasive for anything I'm doing here, more so than just wearing a legal hat.

I was most recently leading our supply chain legal team and now I lead our EHS (environment, health and safety,) team. As you can probably appreciate; there is a lot of natural synergy between the legal and the EHS functions, particularly in the area of holistic risk management.

If I wind my career clock back to the beginning, I was originally an environmental scientist. One of the things I quickly learned is that, typically, you can't be an environmental scientist without the experience of something becoming a so-called legal issue at some point if it is of any significance.

So, I became a lawyer, came to 3M as a lawyer, and am now having the chance to go back to my first passion, environmental sciences.

CW: How helpful is it to have scientific background as well as legal expertise?

JO: It is essential. That is the word I would use, recognizing, of course, that I work with a lot of people at 3M who have scientific bona fides with less formal training. You cannot work at 3M without being grounded in scientific ideas and disciplines, and be ready willing and able to engage in discussions with highly trained specialists. Science applied to life is a very real thing at 3M, and it starts with our scientists, who do some of the most important and interesting things that fuel the rest of the company. Being able to, literally, speak the same language has been essential for me and it is what makes my job fun.

ABOUT JOHN OSTERGREN

John leads 3M's Environment, Health, and Safety (EHS) organization, responsible for the company's global EHS programs and performance – ensuring safe & healthy workplaces, environmental performance, and compliance. He earned his JD and Ph.D. (geochemistry) from Stanford University. Prior to his current role, John served as 3M's General Counsel for Supply Chain and EHS, and previously as General Counsel for operating units in 3M's Industrial, Electronics, and Safety & Graphics business groups. Before 3M, Mr. Ostergren was an attorney at Dorsey & Whitney in Minneapolis, Minnesota, where his practice focused on environmental and technology litigation, and regulatory matters. He served as Editor-in-Chief for the Stanford Environmental Law Journal, and his doctorate research focused on molecular-scale surface chemistry and the fate and transport of environmental contaminants.

Prioritization is essential for risk management, and it is essential for virtually everything we do at 3M. It is one of the fundamental leadership behaviors we identify at the company.

CW: Over the years, disclosures of risk factors at public companies keep growing and multiplying. How can a company prioritize the risks that truly need attention in an age where nearly anything can be counted as a risk factor? How can a company prioritize the risks that really need attention?

JO: Prioritization is essential for risk management and it is essential for virtually everything we do at 3M. It is one of the fundamental leadership behaviors we identify at the company. We all need to demonstrate it in any of the topic areas or silos we are working. The litmus test for effective prioritization is effective execution.

From my perspective, one of the most important things about prioritizing for risk management is that we recognize that it is not just defense. Risk management is about, in frequent cases, risk optimization. You can manage yourself to zero risk by certain behaviors that would be commercial suicide. Knowing the difference between good risk and bad risk is critical, and that is one of the primary criteria for prioritization.

The core is making sure we have compliance nailed down for zero tolerance, must-do activities. There are certain areas where we have to get it right and compliance is one of those.

Beyond that core, we are most often talking about risk where optimization is essential and trade-offs need to be done in an orderly manner. I tend to think of that in my world as the distinction between effective risk management and overall good management. It is a distinction that is subtle at best and they are nearly identical. That is especially the case when you recognize risk management from an optimization standpoint.

We have to, with equal vigor, find those risks we are interested in taking in order to do things differently and pursue opportunities that will, with the first step, be a risk. You could be thinking of doing something differently than you have in the past as defensive risk management, but you also can, and must, also think of it as risk optimization and the pursuit of growth.

Putting risk management together with good management comes back to prioritization. To be tautological about it, you have to prioritize. You cannot do everything.

You need to fundamentally understand your business and customers. You need to understand what market you are working in, your supply chain, and what your customers are demanding in order to optimize the value stream and balance those zero-tolerance compliance components with the optimization of risk management components for commercial success.

CW: The idea of wantonly taking chances would seem to run counter to most corporate cultures. For most businesses, however, doing nothing is the biggest risk of all, you say. Can you explain and defend that viewpoint?

JO: It is about continual, creative destruction. There needs to be a very serious commitment to continuous improvement that includes fundamentally doing things differently. Not just incremental improvements on what you did yesterday, but with real rigor making a programmatic commitment to ensuring we are taking a hard look at what things we should be doing differently to succeed tomorrow.

Yes, almost by definition, when you frame the question that way there is risk. All you know is that things are going to be different from what you did yesterday. There will be some uncertainty and that uncertainty is the source of risk. There is a chance it

will go well. There is a chance it will not go well. You need to be realistic about what your odds of success are and, most importantly, map out the risk profile to, obviously, improve your chances of success and choose your targets well.

It is all on a foundation of needing to do things differently. If you don't do things differently, all you are going to get is the same result. That might work for a little while, but it isn't going to work in the long term.

CW: How does this approach to risk fit within the debates between corporate short-termism and long-termism? You advocate a longer-term view of risk and the potential it offers for business growth. You say that can include a quarter century view when it comes to assessing the value of an investment, not a just financial quarter. Can you discuss that philosophy at 3M?

JO: When companies do well, as this one has for more than 115 years, you have both the privilege and the urgency to consider both short-term and long-term objectives.

There is a chicken or the egg question. You might not be around for 100 years, but you will increase your odds for being around by thinking long-term out of the gate. The fact of the matter, however, is that a start-up company does not have the latitude that we have, or the same urgency around balancing those often-competing perspectives. We, no question, have both.

We have to meet both financial quarter expectations and maintain a rigorous focus on the much longer term in order to do our strategic planning and look around corners that we otherwise wouldn't even see coming.

We talk sometimes about the microscope and the telescope and taking both of those views. You absolutely need to understand the landscape right under your feet in gory detail. You really do need to see that most distant horizon as best you can to understand what the ground is going to look like tomorrow, because all you know is that it is going to be different than it is today. The better you can predict that future, the better you will be positioned for success in it.

CW: How do third parties complicate risk mitigation? How to you make sure third parties and vendors embrace the same values as 3M?

JO: There are very tactical aspects for how we do that through vetting business partners in various ways, whether it is suppliers or other service providers.

More broadly than those tactical pieces, we need to look at our third-party partners as part of our solution, not our problem. Yes, they do complicate things, but done well it delivers more value to the end customers than we would absent the collaboration. That is how we look at it. Those third parties have to be accretive to value in the whole. We have to create situations where the reason we are not doing all of this ourselves is because we do it better together.

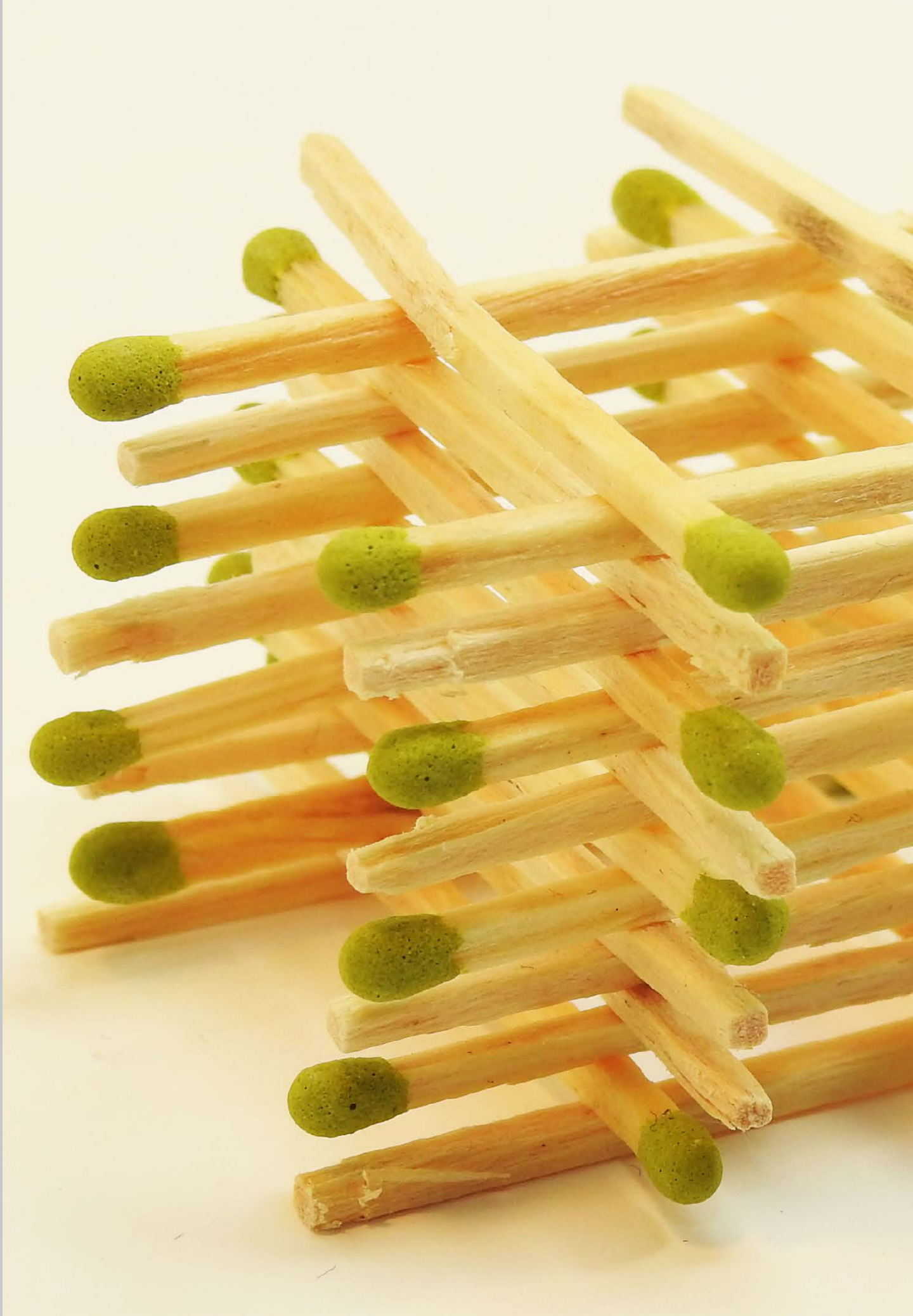
We need to recognize that we are not working with third parties to offload the stuff that we don't want to do or we don't know. We are offloading, so to speak, and partnering with those third parties so we can be greater than the linear sum of our parts.

Part it is risk management. We have to understand how they manage their risks because in value streams their risks become our risks. We need to understand that and find ways to manage it.

That's not to say we take managerial control of our third parties' operations, but we do have a need to understand how they are managing the risks that will become our risks.

CW: What advice might you have for those who, like you, are in the role of evaluating supply chain risk?

JO: Find ways for your risks to be your opportunities. Make risk management another way to think about good management, and vice versa. Management discussions and decisions that are disconnected from risk management can be dangerous. ■



How do your risk oversight processes stack up?

A pair of recently published reports draw a straight line between strong enterprise-wide risk management and strategic execution. **Jaclyn Jaeger** reports.

The global business risk environment is growing more complex, making it more important than ever that companies can effectively predict and respond to disruption. And yet, it seems that most organizations' risk oversight processes are not quite up to par.

Those are some of the key findings from a new report, the "2017 Global State of Enterprise Risk Oversight," released jointly by North Carolina State's Enterprise Risk Management (ERM Initiative) and the Association of International Certified Professional Accountants—a global accountancy body formed by members of the AICPA and the Chartered Institute of Management Accountants.

The report is based on a survey of 586 respondents in senior accounting and finance roles to gather insight on the current state of enterprise-wide risk oversight in four global regions: Europe and the United Kingdom; Africa and the Middle East; Asia and Australasia; and the United States.

One of the main findings from that study is that respondents around the globe overwhelmingly believe the volume and complexity of risks today has grown much over the past five years. An offshoot of this business environment are the unexpected risks that emerge.

"The increase in risks and the operational surprises are tied to the dynamic global business environment," says Mark Beasley, director of the Enterprise Risk Management Initiative at North Carolina State University and co-author of the report. "For example, Europe and the U.K. have seen issues ranging from the Brexit vote to immigration challenges, while Africa and the Middle East have dealt with a wide variety of challenges, such as disruptions caused by the ongoing war in Syria and conflicts with ISIS."

"The United States has been comparatively stable, but we seem to have entered a period of domestic political uncertainty, which is not reflected in the survey, and of course issues abroad can have significant effects on U.S. organizations," Beasley adds.

Even as the risk environment grows more complex, most companies' risk management practices still need significant improvement. "We're seeing a major disconnect between how organizations perceive their challenges and how they are responding to them," Beasley says.

Less than one-third of respondents in all four regions believe they have "complete" enterprise-wide risk management (ERM) processes in place. In all regions of the world, too, less than a quarter of respondents described their risk management oversight as "mature" or "robust."

The survey also examined what techniques companies use to identify, assess, and monitor their key risk exposures. Roughly one-quarter of respondents in each region said they don't maintain risk registers of their top risk exposures.

Furthermore, 57 percent of companies in Asia and Australasia and 47 percent in Africa and the Middle East have formal risk management policy statements, compared with 36 percent in Europe and the United Kingdom, and 39 percent in the United States.

The survey further found a disconnect between risk oversight and strategy execution. A higher percentage of respondents in two regions—Asia & Aus-

"We're seeing a major disconnect between how organizations perceive their challenges and how they are responding to them."

Mark Beasley, Director, Enterprise Risk Management Initiative, North Carolina State University

tralasia (34 percent) and Africa & the Middle East (53 percent)—believe their risk oversight provides a competitive advantage, compared to a very small percentage in Europe and the United Kingdom (18 percent) and in the United States (19 percent).

About half the respondents believe that their senior executive teams consider existing risk exposures when evaluating possible new strategic initiatives. Higher percentages were reported by respondents in Europe & the United Kingdom (53 percent) and in Africa & the Middle East (also 53 percent). Only 44 percent of U.S. companies, however, hold a similar belief.

FERF Findings

Another report, "The Strategic Financial Executive: Managing Risk in a Disruptive World," conducted by the Financial Executives Research Foundation (FERF) in partnership with accounting firm Grant Thornton revealed similar findings. In that report, just 25 percent of financial leaders said that they feel they're able to execute a proper response to risk, and 57 percent admitted they were too late in recognizing changes.

"Organizations of all kinds face new risks from the fast rate of change in regulation, competition, technology, and other factors," says Andrej Suskavcevic, CEO of Financial Executives International and FERF. "[F]inancial executives are integral to advising CEOs and boards of directors on these changes and partnering across their organizations to help identify and manage these risks."

Risk management vs. strategy. The FERF and Grant Thornton report spoke about the need for a more sophisticated process in managing risk. "Leaders can help their organizations reduce risk by looking not only at financial indicators, but at other metrics that measure business health," says Bailey Jordan, risk advisory services partner at Grant Thornton. "Risk can even drive opportunity."

Some companies, for example, are "now dedicating time to understanding change by monitoring macro factors, regulatory issues, cyber-risk, and other data to understand how these changes may affect their organizations," the report stated. "These companies are building processes to identify disruption, black swan events, new competitors, and other emerging risks."

The report also noted that financial executives are continually moving toward aligning risk with strategy and performance. "This shift begins with focusing more on business objectives and the risk surrounding the achievement of those goals, and on aligning with the overall execution in performance, with accountability structures and plans," the report stated.

Integrating risk management processes with strategic planning is still an area in need of improvement, however. According to the ERM Initiative report, fewer than 20 percent of companies in the European Union, United Kingdom, and United States companies believe that their risk management processes are providing a unique competitive advantage. Only half of respondents in all regions indicate that they "mostly" or "extensively" consider risk exposures when evaluating new strategic initiatives.

The overall gap between the complexity of today's risk environment and the risk processes in place come at a time when boards are placing more pressure on management to enhance their risk oversight. In the United States, audit committees are the ones pushing most aggressively for senior

executives to be more involved in risk oversight, which contrasts with the other regions of the world where the greatest amount of pressure is coming from boards or chief executives, the ERM Initiative report stated.

The ERM Initiative report additionally found that, among companies in the United States, boards of directors are more likely to delegate risk oversight to the audit committee, whereas boards of non-U.S. companies are more likely to delegate it to a board risk committee. In addition to pressure coming from audit committees and boards, regulators around the world are also calling for enhanced risk oversight.

In most regions of the world, too, boards of directors formally direct risk oversight. This response was given by 71 percent of respondents in Asia and Australasia; 59 percent in Africa and the Middle East; and 53 percent in Europe and the United Kingdom, as well as the United States.

The ERM Initiative report also found that more companies have risk committees than chief risk officers. About one-third of companies have appointed a chief risk officer, whereas more than half—except respondents in Europe and the United Kingdom—have risk committees.

Numerous barriers appear to impede the progress of ERM practices. Outside the United States, most respondents feel that they don't have sufficient resources to invest in ERM, whereas many respondents of U.S. companies feel that ERM takes a back seat to other priorities.

A lack of perceived value from enterprise risk oversight also impedes progress. This lack of value is most prominent in Africa and the Middle East (41 percent), followed by the United States (37 percent); Europe and the U.K. (34 percent); and Asia and Australasia (27 percent).

The ERM Initiative report from North Carolina State concludes, "The more that executives recognize how robust risk insight increases the organization's ability to be agile and resilient, the greater progress they can make in expanding their risk oversight infrastructure." ■

CALLS TO ACTION

The findings from the 2017 Global Risk Oversight report give rise to the following calls to action.

1. 1. The increasing complexities in today's business environment mean risk management is unlikely to get easier. Senior executives and boards of directors benefit from honest and regular assessments of the effectiveness of the current approach to risk oversight in the light of the rapidly changing risk environment.
2. Given the fundamental relationship between "risks" and "returns", most business-unit leaders understand that taking risks is necessary to generate higher returns. The challenge for management is to genuinely consider whether the process used to understand and evaluate risks associated with the organization's strategies actually delivers any unique capabilities to manage and execute their strategies.
3. Given the intricacies of managing risks across complex business enterprises, organizations may need to strengthen the leadership of their risk management function. Appointing a risk champion—for example, a chief risk officer—or creating a management-level risk committee may help to ensure that all risk management processes are appropriately designed and implemented.
4. Most organizations have tremendous amounts of data that might provide insights about emerging risks. Most of these, however, have not analyzed that data with a risk perspective in mind. They may need to add key risk indicators (KRIs) to management's dashboard systems and reports.

Source: Global Risk Oversight Report

AUTOMATE YOUR THIRD-PARTY RISK PROGRAM

Assess More Vendors…
More Thoroughly…
In Less Time.

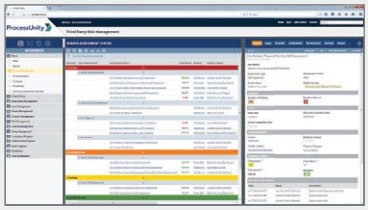
ProcessUnity Vendor Cloud is a software-as-a-service application that automates the third-party risk management lifecycle. Organization of all sizes use Vendor Cloud to streamline key processes including vendor onboarding, pre-contract due diligence and ongoing vendor reviews.

Vendor Cloud significantly reduces the "busy work" associated with manual third-party risk processes, freeing teams to spend more time on strategic risk mitigation. The easy-to-use system can be configured to match an organizations' unique program requirements. Automated notifications, interactive reports and personal dashboards help reduce operational exposures while ensuring results stand up to regulatory scrutiny.

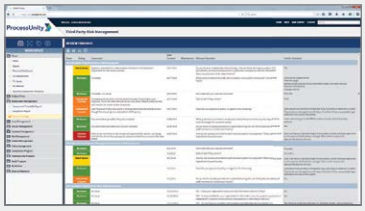
Get started on the road to automation at www.processunity.com/automate

ASSESSMENT SCHEDULES

ASSESSMENT STATUS



FINDINGS



INTERACTIVE REPORTS

ProcessUnity

Collaboration enhances risk management in financial services

The Office of the Comptroller of the Currency has endorsed collaboration between banks as a way to reduce costs on managing third-party risk, and compliance officers are more than ready for it. **Jaclyn Jaeger** explores.

Collaboration among financial institutions is how many banks today are enhancing their third-party risk management programs.

Although collaboration is not a new concept among banks, the Office of the Comptroller of the Currency (OCC) recently endorsed it as an acceptable means for banks to alleviate the significant cost burdens associated with a third-party risk management (TPRM) program. That endorsement came in the form of a supplemental guidance (Bulletin 2017-21) the OCC issued in June, which discussed, among other areas, the use of collaboration for managing third-party relationships.

The OCC guidance should come as a welcome development for compliance and risk officers in the financial services industry, as it provides banks substantial flexibility to enhance their own individual third-party risk management programs. "They're really embracing a best-practices approach and one that gives us all more guidance and instruction on what we need to be doing to make sure the regulators are happy," Brad Keller, senior director of third-party strategy at Prevalent, said during a 2017 Compliance Week Webinar on the OCC guidance.

OCC Bulletin 2017-21 was issued in response to questions submitted by banks as a follow-up to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance." Issued in 2013, Bulletin 2013-29 provides a comprehensive framework for banks for assessing and managing risks associated with third-party relationships.

In Bulletin 2017-21, in response to questions about collaboration, the OCC responded that when banks use the same service providers to secure or obtain like products or services, they may collaborate to meet certain expectations described in OCC Bulletin 2013-29—such as performing due diligence, contract negotiation, and ongoing monitoring responsibilities. "Collaboration can leverage resources by distributing costs across multiple banks," the OCC stated.

The OCC further stated that banks may take advantage of various tools designed to help them evaluate third-party service provider controls. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. Once third parties complete the questionnaires, the results can be shared with banks.

To gauge how banks are embracing collaboration as outlined in Bulletin 2017-21, Compliance Week conducted an online poll during the Webinar. In that poll, the plurality of respondents (44 percent) said their institution "fully understands the benefits of a more collaborative approach and is investigating how to leverage them in our TPRM program."

The second highest number of respondents (33 percent) said that their "institution is unsure how to utilize/execute a collaborative approach in our TPRM program," while another 15 percent answered that their institution is "actively engaged in collaboration with other banks with whom we share common third-party service providers." Nine percent said their institution is "unsure of the actual benefits from a collaborative approach."

Executing collaborative efforts. Compliance officers and risk officers at banks seeking guidance on how to execute a collaborative approach in their TPRM program may want to check out a policy paper issued by the OCC in 2015. That policy paper described a variety of ways that banks currently collaborate, including through the exchange of information and ideas.

Other collaborative efforts used by banks, the OCC said, include:

- Jointly purchasing materials or services;
- Sharing back-office or other services;
- Sharing a specialized staff member or team;
- Jointly owning a service organization;
- Participating in disaster mitigation agreements; and
- Jointly providing/developing products and services.

"Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems."

Office of the Comptroller of the Currency

OCC Bulletin 2017-21 also discussed collaboration opportunities to help mitigate cyber-threats to banks, as well as to their third-party relationships, including engaging with information-sharing organizations. "Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems," the OCC noted.

The OCC cited a variety of information-sharing organizations that help banks monitor cyber-threats and vulnerabilities and enhance risk management and internal controls. These organizations include the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), and InfraGard, among others. Banks also may use the FS-ISAC to share information with other banks, the OCC said.

Bank-specific responsibilities. The OCC has repeatedly warned, however, that collaboration cannot be used to satisfy all oversight responsibilities, particularly third-party risk management processes that must be tailored to each bank's specific needs. Examples of individual bank-specific responsibilities include:

» Integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
» Assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
» Implementing information technology controls at the bank.
» Ongoing benchmarking of service provider performance against the contract or service-level agreement.
» Evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
» Monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
» Monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

Furthermore, the OCC stressed that any collaborative activities among financial institutions must comply with antitrust laws, and that banks should take appropriate steps to ensure compliance with these laws. In this regard, financial institutions should review the Federal Trade Commission and U.S. Department of Justice's joint "Antitrust Guidelines for Collaborations Among Competitors."

Ongoing monitoring. Another focus area for examiners is what banks are doing from an ongoing monitoring standpoint for each of the bank's third-party service providers that support critical activities, which Bulletin 2017-21 also discussed in broad detail.

OCC's 2013 guidance provides specific criteria that a bank's board and management may use to identify its critical activities, but some examples can include significant bank functions—such as payments, clearing, settlements, and custody—or significant shared

services, such as information technology.

Other potential critical activities may be those that:

» Could cause the bank to face significant risk if a third party fails to meet expectations;
» Could have significant bank customer impact;
» Require significant investment in resources to implement third-party relationships and manage risks; or that
» Could majorly affect a bank's operations if the bank must find an alternative third party or if the outsourced activities must be brought in-house.

When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC said it expects the bank's board of directors and management to:

» Develop alternative ways to analyze these critical third-party service providers;
» Establish risk-mitigating controls;
» Be prepared to address interruptions in delivery—multiple payment systems and multiple telecommunications lines in and out of critical sites, for example;
» Ensure that contracts meet the bank's needs; and
» Retain appropriate documentation of all related decisions and efforts to obtain information.

Ongoing monitoring involves looking at not just the bank's third parties' threat environments concerning areas outside of contractual requirements, but also the threat environment of the third parties' sub-contractors. Areas to monitor could include legal activity that could impair the third party's ability to deliver services; regulatory actions; financial viability; operational issues like a merger or acquisition or any senior-leadership changes; or brand and reputational issues.

"Ongoing monitoring lets you address issues before they become events," said Keller, who has been developing and leading risk management programs for more than 25 years. For example, a third-party vendor doesn't have to alert a bank to a data breach that occurred at a data center other than where the bank's sensitive data is stored, but that's something the financial institution ought to know, because both locations likely employ the same IT security controls, he said. Thus, the bank's chief compliance or risk officer should have that conversation with that third-party vendor to determine what they're doing to address that threat.

Another critical piece to ongoing monitoring is documentation. Examiners are going to want to see how the bank's compliance function is executing ongoing monitoring and evaluating third parties' processes against the bank's specifically identified criteria, Keller said.

"No matter how robust the bank's third-party risk management processes are, if those efforts are not documented and compliance cannot provide actual evidence of that process, the OCC, for all intents and purposes, will treat those efforts as non-existent. It becomes something they view more as aspirational on behalf of the institution, as opposed to something they can say the institution is, in fact, actually doing," Keller said.

A third helpful guidance for compliance and risk professionals in financial services to peruse is OCC Bulletin 2017-07, because it describes what examination procedures OCC examiners may use during the examination of a bank's risk management of third-party relationships. "If you haven't looked at 2017-07, I would suggest you do, particularly if you think you're up for an examination soon," Keller said.

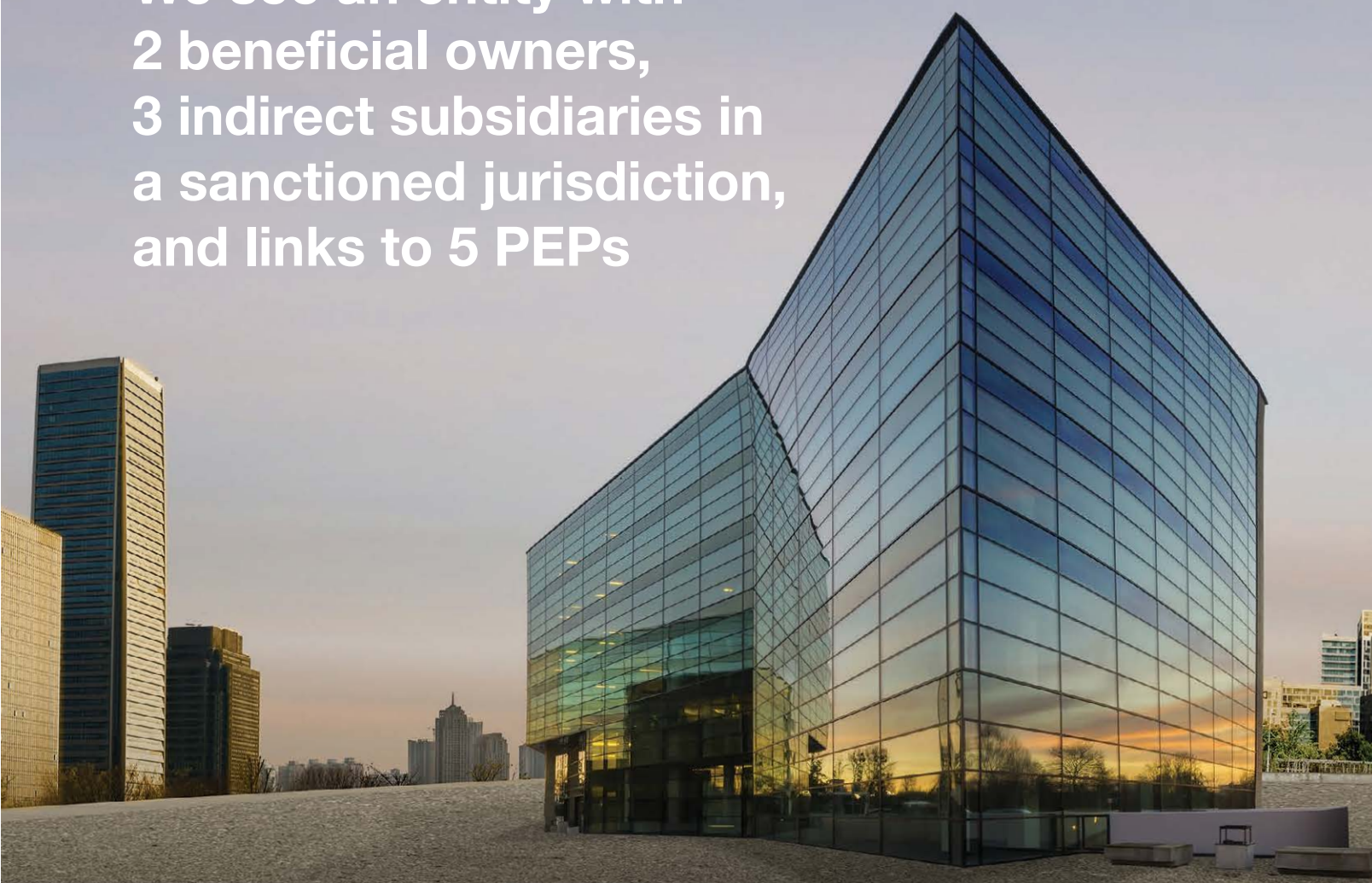
In another polling question provided during the Compliance Week Webinar, respondents were asked to describe their financial institution's response to OCC examination procedures. Most (52 percent) said they treat them the same as any other regulation, while 32 percent said they treat them as an "indication of preparedness."

Another 16 percent of respondents said they treat OCC examination procedures as informational, rather than as a regulatory requirement. "The best approach," Keller said, "is to treat it as any other regulation." ■

Some just see a company

BUREAU VAN DIJK
A Moody's Analytics Company

We see an entity with 2 beneficial owners, 3 indirect subsidiaries in a sanctioned jurisdiction, and links to 5 PEPs



Download our free white papers

Really getting to know your third parties
The definitive guide to beneficial ownership

Register for your free trial
bvdinfo.com
bvd@bvdinfo.com

Welcome to the business of certainty

orbis

compliance catalyst

Elements of a best-in-class TPRM program

Prudent ethics and compliance officers will want to check out a new third-party risk management benchmark report from NAVEX Global to gauge how their programs compare against their peers. **Jaclyn Jaeger** reports.

Companies with robust third-party risk management programs clearly distinguish themselves in many ways from those whose programs lack maturity.

Those best practices were recently analyzed in NAVEX Global's third consecutive report on third-party risk management (TPRM). Prudent ethics and compliance officers will want to check out the new report to gauge how their TPRM programs stack up against their peers.

In its 2017 "Ethics & Compliance Third-Party Risk Management Benchmark Report," 427 survey respondents rated the maturity of their TPRM program based on the following four categories:

» **Reactive** (13 percent of respondents): We address issues as they arise with no formal pro-gram in place.
» **Basic** (29 percent of respondents): We are seeking to develop procedures to manage third-party engagements, but due diligence efforts lack consistency and uniformity between business units or geographies. We send questionnaires and screen a limited number of third parties. Management of third-party engagements lacks centralization, and we have an in-complete understanding of organizational exposure to risk associated with third parties.
» **Maturing** (44 percent of respondents): We understand our organizational exposure to risks associated with our third parties, have some level of uniform policy, and are moving toward a centralized third-party risk management system. We are identifying internal stakeholders who will be accountable for defining risk and owning third-party engagements. We per-form audits and require training and policy attestation from a limited set of third parties. We have confidence that we're taking a risk-based approach to third-party due diligence but still have gaps to cover.
» **Advanced** (14 percent of respondents): We have consistently identified and stratified potential exposure to risk across the organization and have a clearly defined global policy. We regularly perform audits, train third parties on our policies, and gain attestation at clearly de-fined intervals. Key internal stakeholders are informed and involved in the entire third-party risk management lifecycle. We measure program success and KPIs and adapt our program based upon results. We have confidence that our program is defensible and would with-stand enforcement action.

New in this year's report, the program maturity definitions were adjusted to more closely align with the FCPA Guidance and best practices, including performing audits, requiring training, and centralizing risk management operations. Additionally, much of the maturity-scale criteria was based on process, structure, and alignment—not on budget, number of full-time employees, or number of third parties, the NAVEX report stated.

Using the four categories as a baseline, the report provides a clear picture of what distinguishes mature and advanced TPRM programs from those that are reactive or basic. The core elements that define mature and advanced TPRM programs from basic and reactive are explored in greater detail below.

Due diligence and policy assessments. Overall, the data revealed that most companies (57 per-cent)

conduct third-party due diligence by pursuing a risk management program that corresponds to the nature and level of risk that their third parties represent. Moreover, 55 percent of respondents indicated that their companies use formal processes—such as capturing business rationale and con-ducting screening to vet third parties and filter-out high -risk engagements.

"This reflects the kind of program criteria you see not only in the FCPA Guidance and other recognized guidance around third parties, but also the recent Evaluation of Corporate Compliance Programs from the Department of Justice," Randy Stephens, vice president of advisory services for NAVEX Global, said during a recent Webinar discussing the findings.

Mature and advanced TPRM programs assess their third-party due diligence policies more often than reactive and basic programs. In the NAVEX report, 49 percent of companies with maturing and advanced programs assess their third-party due diligence management policy on an annual basis, 44 percent of reactive and 28 percent of basic programs indicated that they don't even have a policy in place.

Third-party risk classification. Sixty-two percent of respondents, overall, said they use specific criteria to classify third-party risk as high, medium, and low. A significant 87 percent of respondents with maturing and advanced programs, however, are more likely to use specific criteria to classify risk, compared to 52 percent of both reactive and basic programs. "Your third-party risk management program should be consistent, but adaptable," Stephens said.

Among those that classify third parties by risk level, the main criteria assessed are the type of third party (82 percent); amount of the contract (62 percent); and geography of the third party (61 per-cent). A risk-based approach includes applying different degrees of due diligence based on these classification criteria.

Another important classification consideration is to tie a third party's risk level to the amount of revenue that it generates. "For example, you may have a high-risk third party in China who generates $5,000 in revenue versus a mid-risk third party that generates $1 million revenue through government interactions," Michael Volkov, a former federal prosecutor and a white-collar defense attorney with the Volkov Law Group, said during the Webinar.

TPRM through automation. Mature and advanced TPRM programs are more likely to use au-tomated systems to manage third-party risk, 43 percent compared to 30 percent of respondents overall. Automated systems are mainly used to help screen third parties (72 percent) and to conduct enhanced third-party diligence (60 percent).

Automation also helps when it comes to exercising audit clauses. "There is no better way to do that than to start with the data you have in your automated program," Volkov said.

Across all aspects of program execution, companies that use automated systems perform signifi-cantly better, especially when it comes to screening third parties, the report found. Mature and ad-vanced TPRM programs tend to screen all their third parties, while reactive and basic programs tend to screen only select third parties—such as those that are crucial to their business or those in high-risk industries or geographical locations. "Not doing at least some basic level of screening for every third party is going to open you up to greater risk," Stephens said.

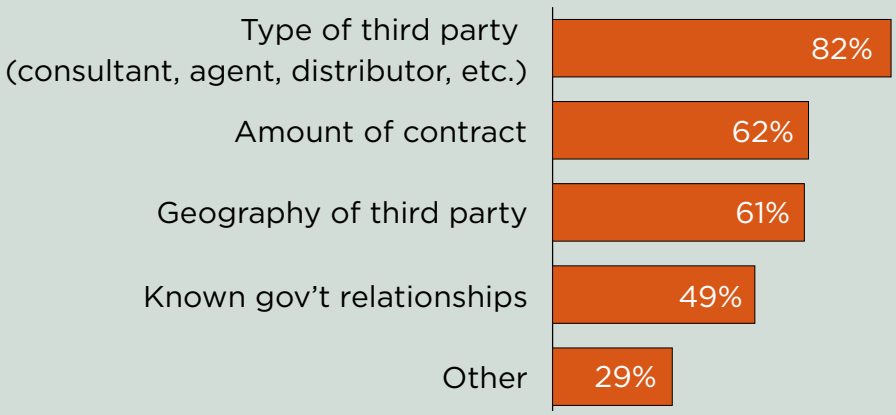
Furthermore, 92 percent of mature and advanced TPRM programs said they continuously monitor third parties, including 37 percent that monitor all third parties. In comparison, nearly one-third of respondents with reactive and basic programs said they do not continuously monitor third parties.

Overall, companies that use automated systems are more likely to continuously monitor all third parties than those not using automated systems (41 percent vs. 23 percent, respectively). "It's easier to conduct due diligence and monitor when you're using automation, particularly where an organization engages thousands or tens of thousands of third parties," Stephens said.

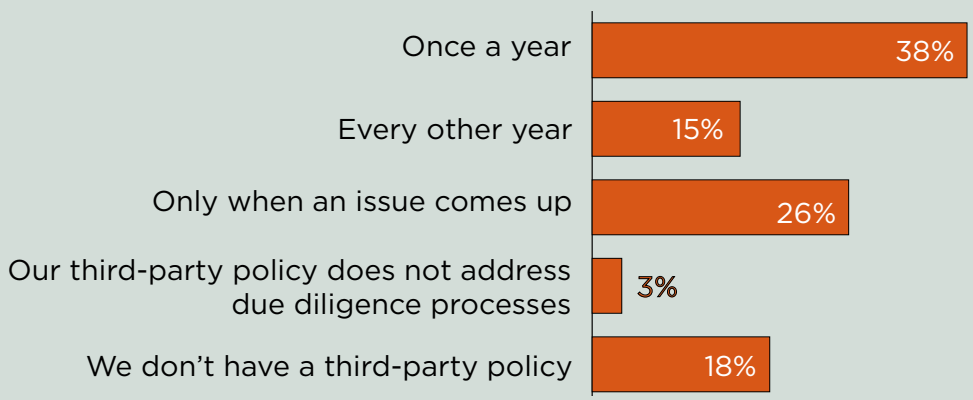
Program effectiveness assessments. The

TPRM SURVEY RESULTS

NAVEX Global asked respondents to its "Ethics & Compliance Third-Party Risk Management Benchmark Report," a third-party risk management survey: What criteria does your organization use to classify third parties as high, medium, and low risk? Respondents' answers are below.



NAVEX asked respondents to its TPRM survey: When do you reassess or update your third-party policy, including your third-party due diligence policy? Results are below.



Source: NAVEX Global

most common approaches used to assess effectiveness of third-party due diligence programs, particularly among maturing and advanced programs, are periodic risk assessments and audits. "This best practice ensures the program is working as intended and can also be an early warning sign for gaps or opportunities to improve," the report stated.

> "Not doing at least some basic level of screening for every third party is going to open you up to greater risk."
>
> Randy Stephens, Vice President, Advisory Services, NAVEX Global

Almost half of organizations with reactive programs (48 percent) and more than a third of those with basic programs indicate that they don't assess program effectiveness, compared to 11 percent of maturing programs and eight percent of advanced programs.

Those with maturing and advanced programs are likely to assess the effectiveness of their TPRM program using a variety of approaches, including:

» Periodic risk assessments (56 percent vs. 36 percent of reactive and basic programs);
» Onboarding and screening efficiencies (32 percent vs. 13 percent);
» Ability to proactively identify and mitigate third-party risks (36 percent vs. 19 percent);
» Third-party training completion and attestation rates (13 percent vs. six percent);
» Audits (53 percent vs. 36 percent); and
» Benchmarking program performance against peers (20 percent vs. six percent).

The report highlighted that, surprisingly, 22 percent of respondents do not measure effectiveness using any means whatsoever. "You can't improve what you can't measure; the strongest compliance programs will be able to rely on data, metrics, and outcomes to measure effectiveness and apply resources accordingly," the report stated.

Overall performance. Across all aspects of program execution, performance significantly improves with maturity. Respondents with advanced programs said they are able to do the following:

» Implement a risk-based program (87 percent);
» Comply with laws and regulations (87 percent);
» Conduct deeper dives where needed (82 percent);
» Defensibility of program with enforcement agencies (83 percent);
» Accurately define risk (84 percent); and
» Determine the ROI of the program (50 percent).

Beyond performance, the report showed that the less mature a TPRM program, the greater the likelihood of facing an enforcement action. In the report, 46 percent of those respondents with reactive programs faced legal action in the last three years where less than 30 percent of those with basic, maturing, and advanced programs faced legal or regulatory enforcement actions over the same period.

In sum, key findings from NAVEX Global's 2017 TPRM benchmark report shows ethics and compliance professionals that today's best practices include applying program diligence and consistency across all third parties; defining business justification for engagements; continuously monitoring higher-risk third parties; and applying due diligence analysis when and where it's warranted.

Lastly, companies that use an automated third-party management solution to manage the scale and scope of their third-party risk profile enjoy improved program performance on multiple levels, helping to better protect both their legal and financial risk, as well as their reputational risk overall. ■

New cyber-rules coming for defense contractors

New, potentially overlooked government-issued cyber-security demands for defense contractors extend into their network of suppliers as of Dec. 31. **Jaclyn Jaeger** explores.

An ever-increasing array of cyber-security demands are being placed upon companies in all sectors—from rules specific to firms doing business in New York state to Europe's General Data Protection Regulation.

Potentially lost amid those frequently spotlighted demands are strict, sweeping, and imminent regulations for contractors with the Department of Defense.

In an effort to protect Covered Defense Information—unclassified data categorized as sensitive because it was provided by, or generated for, the Government and not intended for public release—comes Defense Federal Acquisition Regulations Supplement 252.204-7012 and rules pertaining to "Safeguarding Covered Defense Information and Cyber Incident Reporting." Yes, it is as complicated as it sounds.

The DFARS supplement applies to all Department of Defense solicitations other than procurements for "commercial off-the-shelf items." Defense contractors possessing or transmitting CDI must implement the 110 security controls itemized in the cyber-security framework crafted by the National Institute of Standards and Technology, a measurement standards laboratory and non-regulatory agency of the U.S. Department of Commerce.

The NIST document, specifically, is "Special Publi-

cation 800-171," also known as "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

The deadline for adapting these now-mandated controls is fast approaching: Dec. 31, 2017.

Experts warn that many contractors may not be fully cognizant of how broad and complicated the requirements are, especially as they extend deep into the supply chain to all sub-contractors and suppliers. Smaller companies will, as expected, face a disproportionate challenge. Suppliers and sub-suppliers may be unaware of the rules passed on to prime contractors and poorly positioned to assist them by proving their own cyber-readiness.

"Implementation of the NIST standards and other requirements of DFARS 7012 can be challenging for even the most experienced contractors," says Nelson Kanemoto, founder of eResilience, a division of Referentia Systems that specializes in commercial cyber-security and DFARS compliance services.

"For small- and medium -sized businesses it's even more difficult because of limited time and resources," he says. "It is critical for contractors to get started ASAP, especially since it's not guaranteed that government contract officers will accept a System Security Plan and Plan of Action and Milestones for implementing DFARS regulations as an alternative to timely compliance. If you're non-compliant at the end of the year you risk having to stop work."

Not only is losing government contracts a concern, compliance failures could trigger civil and criminal liability if inaccurate security assurances fall under "misrepresentation" for purposes of the False Claims Act.

"Implementing NIST guidelines and other requirements of DFARS 7012 is much more complicated than many companies realize," says Kanemoto. "It goes way beyond the average IT skillset, and government-issued guidelines often have gray areas that require careful interpretation."

Among DFARS 7012's key requirements to meet by the end of the year: comprehensive reporting requirements for cyber-incidents and discovery of malicious software; meeting security standards for cloud-stored CDI data (including those of the Federal Risk and Authorization Management Program; providing the government on-demand access to any information and equipment needed to conduct a forensic analysis; and providing the Department of Defense, upon request, damage assessment information.

Other mandates include the use of digital rights management technology to encrypt documents, and requiring multi-factor authentication to access documents.

"Threat actors are launching increasingly sophisticated and potent cyber-attacks that target the most vulnerable points in an organization's global, multi-tiered supply chain," said Vijay Takanti, senior vice president of product development for Exostar. "Supply chain risk mitigation and management is a top priority for the aerospace and defense industry, particularly with the Dec. 31st deadline looming."

Exostar is a provider of Software-as-a-Service offerings for companies in aerospace and defense, life sciences, and healthcare industries. Clients include Northrop Grumman, Huntington Ingalls Industries, Airbus North America, Rolls-Royce, and BAE Systems.

"When you are working through a global multi-tiered supply chain with potentially tens of thousands of suppliers in that supply chain, how do you know and how do you trust the level of security and data hygiene of all of those partners," says Tom McHale, Exostar's director of risk management product development, on the new rule's difficult demands. "A chain is only as strong as its weakest link. There are a lot of people who are scrambling now to be able to demonstrate this level of compliance, especially if you are a large organization with thousands of suppliers."

The large prime contractors understand what is at stake, he added, but "they have a wide and deep supplier network and don't necessarily have visibility much below their top level of suppliers. They may not know all the players."

A common procedure for many firms is using questionnaires and self-certifications to assess supply chain risks and regulatory compliance down through supply chain partners. With the new NIST standards

in play, additional pressure is on prime contractors to identify suppliers that are having problems and either help them improve their security posture or reconsider their use as a supplier.

Among the specific challenges for contractors is adapting to two-factor authentication and encryption demands.

"When CDI data is either moved to them or they are holding it for their own purposes, that information—schematics, technical drawings needed for manufacturing purposes—must be encrypted," McHale says. "There is technology required that they are probably not familiar with and companies may have problems with that level of control."

The NIST standards "are the correct bar to be shooting for," says Larry Lieberman, business development manager and "cyber-security evangelist" for eResilience and Referentia.

Nevertheless, it won't be easy. "Prime contractors are, as we speak, going through the process of parsing out who they are going to need to drop from their roster of sub-contractors and their teams," he says.

Compliance now, Lieberman says, will pay off later. "The DoD is the top of the iceberg," he says. "Everyone is going in that direction, including the rest of the federal agencies. This, we suspect, is going to be wrapped into the Federal Acquisition Regulation by next year. It will be not just for anyone doing business with the DoD, but if you are doing business with any federal agency that you will need to adapt these same standards. Then, the commercial world is not too far behind that."

The hardening of federal cyber-security standards is underway. In 2017, the Trump regime announced an executive order mandating agencies submit updated cyber-security risk management plans designed to safeguard controlled unclassified information.

"The government is going to go after the prime sub-contractor, but if a sub-contractor is the one causing all their problems, they are going to be ostracized by prime contractors and probably other sub-contractors as well," says Tim Williams, eResilience's technical director.

The rule change is a "wake-up call" to act now or risk having to find other sources of business, he says. "An entire organization needs to buy in and understand what is going on." Williams suggests key steps for DFARS 7012 compliance:

» perform a content audit to understand what information you need to protect;
» conduct an assessment to identify the gaps in your organization's DFARS 7012 compliance;
» provide adequate security controls to protect the CDI;
» create an incident response plan;
» train employees;
» and institute continuous monitoring and improvements.

As for challenges, McHale agrees that multifactor authentication may be a "culture change for people."

"Another thing that people don't necessarily understand is the monitoring piece that has to go along with all of this," he says. "It is not just that you are supposed to be collecting all the log data, you are supposed to be going through that log data to look for indications of compromise. You can't just wait for the FBI to come along and tell you there was a breach. You need to find that breach ahead of time."

Another suggestion: Document and maintain a backup of everything you do. "When all is said and done, if there is an incident and the government comes in, they are going to ask, 'Why did you implement this required control the way that you did.?' If there is an issue, it won't be the Department of defense on the other side of the table, it is going to be the Department of Justice and they are going to be looking at your reasoning," McHale says. "If you don't have good reasoning for things, that's where you are going to run into trouble."

"A good, documented approach will keep you off the bad side of the road," he adds. "So, document why you are doing things and have good backup of the reasoning behind why you implemented controls the way you did." ■

RAPIDRATINGS®

Pioneering Financial Health.
We See What Others Don't.

ASSESS THE FINANCIAL HEALTH OF YOUR THIRD-PARTY BUSINESS PARTNERS

- Accurately assess risk each third party poses to your organization
- Effectively evaluate partners in due diligence & monitor throughout the lifecycle
- Easily meet compliance requirements, including privately-held vendors
- Proactively avoid business disruption and support business continuity initiatives

How will the Financial Health Rating help you protect your brand?

REQUEST A FREE FHR REPORT

More firms exiting third-party vendor relationships

More firms are leaving or changing third-party vendor relationships, says a new study. **Jaclyn Jaeger** has more.

An increasing number of companies across nearly all industries expect to exit or change relationships with third-party vendors due to heightened risk levels. That was one key finding to come from the fourth annual "Vendor Risk Management Benchmark Study" from Protiviti and the Santa Fe Group. In this year's benchmark report, 53 percent of 539 compliance, risk, audit, and IT executives surveyed said that their companies are plan to "de-risk" (by either exiting or changing) their third-party vendor relationships that pose the highest risk.

Respondents said it has "become imperative from a risk and regulatory standpoint to also assess or our vendors' sub-contractors." Put another way, it's becoming increasingly difficult for firms to get their arms around fourth parties—their vendors' vendors. "Often, we find that companies don't even know that their vendor has outsourced part of the work that it's doing on its behalf," Gary Roboff, a senior adviser to the Santa Fe Group, said in a podcast discussing the results.

Other reasons cited include cost concerns associated with assessing vendors (29 percent), and a lack of internal support and skills for the sophisticated forensic control testing required of vendors (24 percent).

A wave of new cyber-security-related regulations—such as the EU's General Data Protection Regulation,

China's complex Cyber Security Law, and the New York Department of Financial Services Cybersecurity Requirements—are creating additional pressure from a regulatory and compliance standpoint.

"Even though companies have made strides in their vendor risk management practices as evident in this year's survey results, many organizations may not have access to enough vendor risk management expertise to mitigate their risks," said Cal Slemp, a managing director with Protiviti, leading its security and privacy solutions consulting business globally.

Respondents were benchmarked against the "Vendor Risk Management Maturity Model," developed by the Shared Assessment Program, comprised of financial institutions, Big 4 firms, and third-party risk management executives in the brokerage, healthcare, insurance, retail, and telecommunications industries.

"When it comes to pressing issues ... one of the major concerns for organizations today is vendor risk," said Kevin Donahue, a senior director with Protiviti. "They can manage these risks very well within their own organizations, but may have a lot of trouble figuring out how to manage them with their vendors."

Respondents were asked to rate their firm's maturity level (on a 0 to 5 scale) under eight categories of vendor risk management, and under roughly 130 controls within these categories: policies, standards and procedures; contracts; monitoring and review; vendor risk identification and analysis; program governance; communication and information sharing; tools, measurement and analysis; and skills and expertise.

One positive finding to come from the report: Five out of the eight vendor risk management categories showed improvements in average maturity on a year-over-year basis. "The first few years, in 2014 and 2015, we didn't see a lot of progress," says Roboff. "We began to see more forward movement in 2016, and that movement continued in 2017."

Vendor risk identification and analysis, and skills and expertise demonstrated the greatest gains in maturity level overall. Under vendor risk identification and analysis, for example, the three sub-categories to show the biggest year-over-year improvements were supporting information-gathering in vendor reviews; executing a formal vendor assessment process; and formally documenting assessment roles and duties.

The sub-category with the lowest maturity level was "having a process in place to determine if a vendor utilizes sub-contractors whenever a vendor contract does not include vendor outsourcing requirements." This finding "represents a clear call to action, given the critical need to understand and monitor fourth-party risk," the report stated.

With a maturity score of 2.6, the "skills and expertise" category continued to show the lowest level of vendor risk maturity, and yet its maturity level has improved more than any other category in the past two years. In this specific category, four components show the largest year-over-year improvements:

» Annually measuring employee understand of vendor risk management accountabilities and reporting results to management;
» Providing training for assigned vendor risk management resources to maintain appropriate certifications;
» Routinely measuring or benchmarking the organization's vendor risk management budget with management report to demonstrate return on investment; and
» Implementing metrics and reporting for compliance to required training and aware of vendor risk policies.

But more fixes are needed, given that three vendor risk components in this category received the lowest maturity level scores in the entire survey. These categories were routinely measuring or benchmarking the organization's vendor risk management budget with management report to demonstrate return on investment; annually measuring employee understand of vendor risk management accountabilities and reporting results to management; and integrating vendor risk management functions and tools sufficiently into business lines so that overall costs and budget for dedicated risk management budgets are reduced. ■

RISKRATE®
Enterprise Due Diligence

Effectively Manage Third-Party Risks

Protect your organization against legal, operational and reputational risk with RiskRate

- Automated third-party onboarding and risk-based stratification
- Analyst reviewed screening and continuous monitoring for adverse media, sanctions and PEP lists
- Integrated enhanced due diligence
- Globally accessible

NAVEX GLOBAL®

Learn more about RiskRate today **www.navexglobal.com/RiskRate**