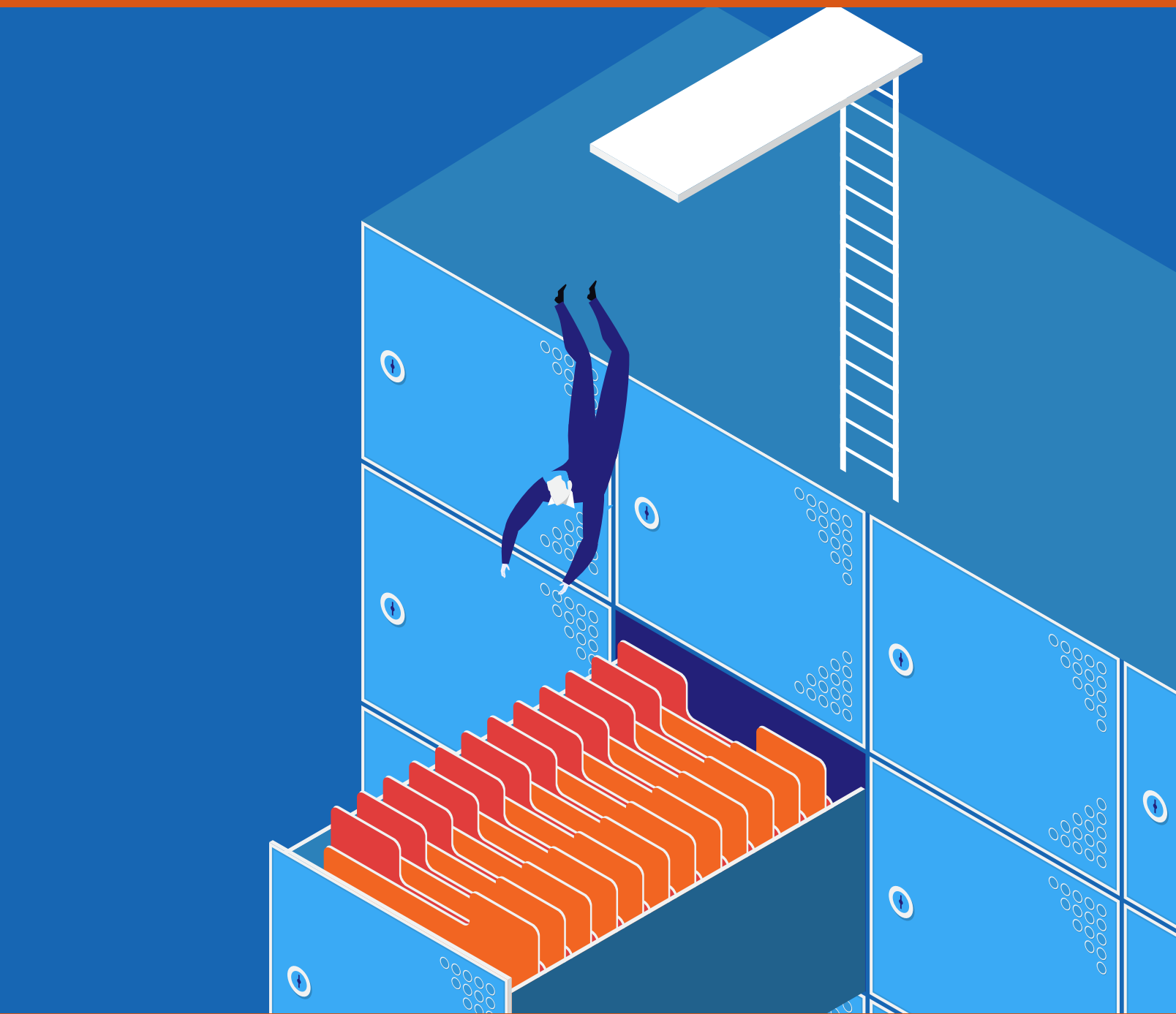
Brought to you by the publishers of COMPLIANCE WEEK



Reducing third-party risks with eyes wide open

A report sponsored by

opus

RAPIDRATINGS™

COMPLIANCE WEEK
THE LEADING RESOURCE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Recent analyses show that many companies don't have adequate visibility into their third parties, and even less so their third parties' third parties and beyond (so-called Nth parties). **Jaclyn Jaeger** has more.

For most global companies, the ability to identify, assess, and manage risks posed by third parties is challenging enough without having to worry about their extended corporate families. But by ignoring these third parties, companies today are increasingly exposing themselves to a whole new level of financial, regulatory, and reputational risk.

Recent analyses show that many companies still don't even have adequate visibility into their third parties, and even less so concerning their third parties' third parties and beyond (so-called Nth parties). These findings were highlighted in a new survey by Opus Global and RapidRatings, in partnership with Compliance Week.

According to the findings, 33 percent of 102 respondents said they have "limited or no visibility into fourth-party/Nth-party risks," and another 32 percent said they require their third parties to manage their own suppliers. Others responded that they either "don't know" (15 percent) or that they encourage (but don't require) their third parties to manage their third-party universe (7 percent). Just 13 percent said they take "an active approach to assessing fourth/Nth parties."

The findings were consistent with a recent global survey conducted by Deloitte. In Deloitte's survey[1], just 2 percent of 975 respondents said they regularly identify and monitor their third parties' sub-contractors, while another 10 percent do so only for those sub-contractors identified as critical. Other respondents said they either rely on their third parties to do so (44 percent); have an unstructured/ad hoc approach (18 percent); or do not do so at all (17 percent).

Global companies whose procurement, compliance, and risk management teams are looking to take their third-party and fourth-party risk management efforts to the next level will want to consider the following best-practice measures:

Build the case for a bigger budget. Whether talking about cyber-security risk, data-privacy risk, or bribery and corruption risk, the common denominator is third-party risk exposure. Some of the biggest challenges in managing third-party risk is lack of staff and lack of budget. According to the Opus and RapidRatings survey, 36 percent of respondents said they lack staff to manage all of their third parties, and another 24 percent said they lack the budget to invest in the necessary tools and technologies.

"That's problematic," says RapidRatings Chief Executive Officer James Gellert. "Companies have to prioritize risk management. They have to resource it. They have to fund it. If they can't do those things, they're taking on risk that they don't need to be."

These findings correlate with another finding in the Opus and RapidRatings survey, in which just 10 percent said that they measure the success of their third-party risk management program with quantitative metrics, such as by calculating lost revenue and returns on investment. "It's hard to make the case for a bigger budget without having that quantifiable data," says Lee Kirschbaum, senior vice president and head of product, marketing, and alliances at Opus.

Before a company can tackle its fourth-party and Nth-party risks, it must first have a firm grasp on its third-party universe: Who are your third parties? What services are they providing? What is the nature and level of risk posed by each third party? What adequate protections, if any, does the company have in place to manage those relationships? How often are third-party due diligence management policies assessed?

> "The reason most companies don't properly manage their Nth parties is because they don't have the system capability to do it."
>
> Mark DeLuca, Senior Vice President, Worldwide Sales, Opus

This process takes quite a bit of time. "Typically, companies will do that successively over a period, eventually getting to all their third parties," says Mark DeLuca, senior vice pres-

1 Deloitte: Focusing on the climb ahead: Third-party governance and risk management – Extended enterprise risk management global survey 2018'

ident of worldwide sales at Opus.

Automate monitoring and auditing controls. Companies with mature risk management programs use automated systems to manage third- and fourth-party risk. By automating risk management processes, a company can more quickly and efficiently screen third parties and their sub-contractors; conduct enhanced due diligence; and manage the exercise and oversight of audit rights.

"The reason most companies don't properly manage their Nth parties is because they don't have the system capability to do it," DeLuca says. Manually monitoring third-party risks or using an off-the-shelf solution that is not purpose-built is not going to do the job effectively or efficiently.

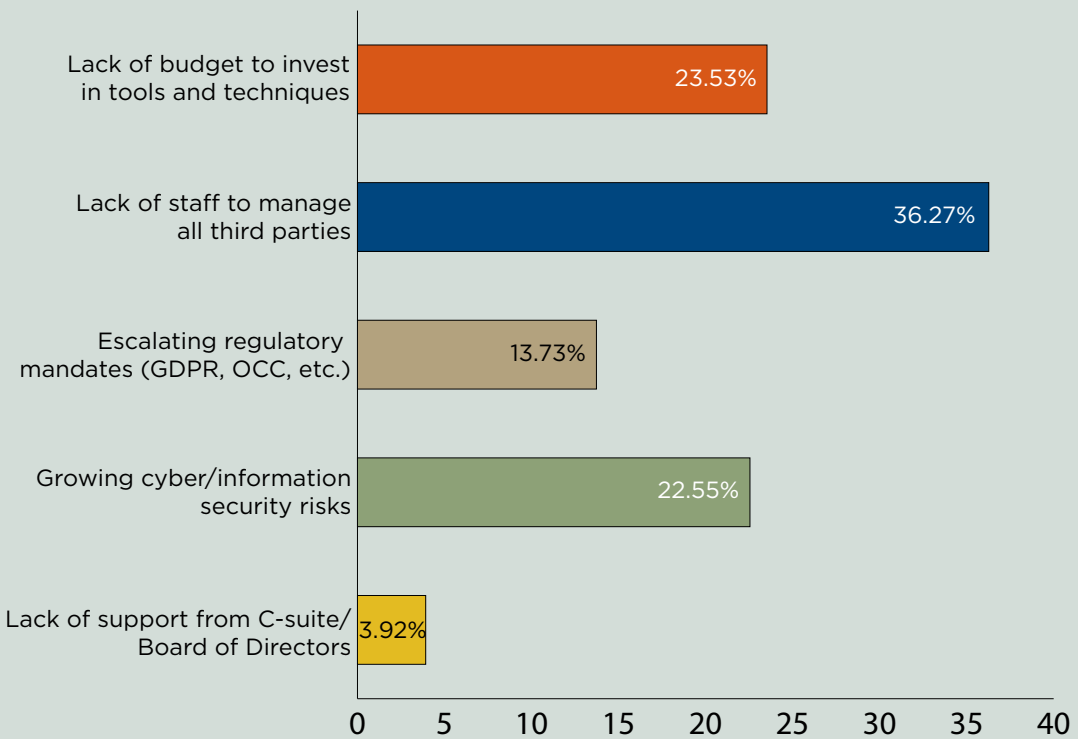
As just one example, Opus's SaaS third-party risk management solution, Hiperos 3PM, enables companies to segment third parties by criteria—such as by customer impact, geography, and spend. From there, users can assign and automate controls for each third-party relationship. Third-party performance can also be managed through ongoing assessments and results reporting, information that can then be shared with boards, critical business partners, and even enforcement authorities.

"Once you have things centrally managed and stored, it helps drive automation, because then you have one place that houses everything and you get a clear view and visibility into everybody who has access to the information," Kirschbaum says. "Until you identify it, you really can't manage it."

Monitoring should be in line with the language in the contract that you've agreed to at the beginning, either with your third party or even directly with the sub-contractor.

Focus on critical or high-risk third parties. Once the business has a firm grasp on its overall universe of third parties,

What are your organization's biggest challenges when it comes to third-party risk management?



Source: Compliance Week in partnership with OPUS and RapidRatings

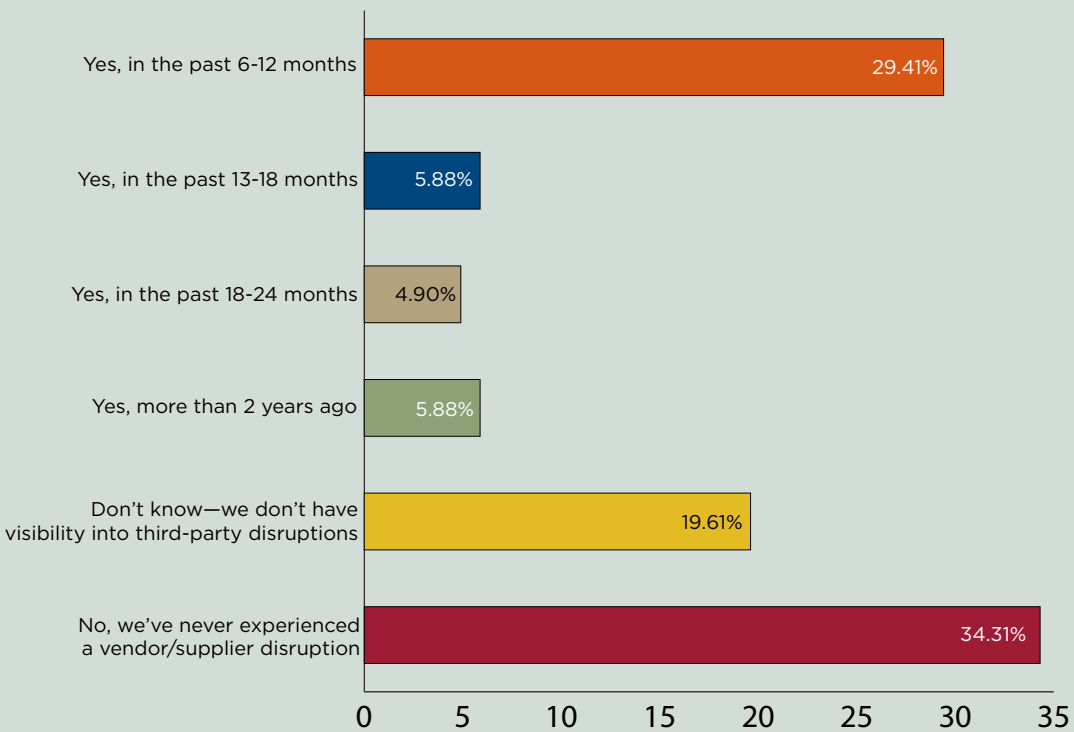
"Companies have to prioritize risk management. They have to resource it. They have to fund it. If they can't do those things, they're taking on risk that they don't need to be."

James Gellert, CEO, RapidRatings

that's when you can take a deep dive to identify your most critical or high-risk third parties. Respondents to the Opus and RapidRatings survey said they use a variety of criteria to determine the criticality of a third party, including whether the third party is a sole-source provider (45 percent) or a dominant supplier (41 percent) or if the service is client-facing or product-facing (40 percent). Other considerations cited include whether the third party is a high-spend third party (38 percent) or whether multiple departments or business units have the same vendor (34 percent).

The financial health of a third or fourth party can also pose a threat. That is where RapidRatings comes into play. Its Financial Health Rating provides forward-looking and actionable insight into the financial stability of third-party vendors, suppliers, and counterparties by using quantitative methods and machine learning techniques to analyze relevant financial data, rating private financial statements and public company filings. The financial reports that are generated facili-

Has your organization experienced a disruption caused by a third party (vendor or supplier?)



Source: Compliance Week in partnership with OPUS and RapidRatings

"Once you have things centrally managed and stored, it helps drive automation, because then you have one place that houses everything and you get a clear view and visibility intoeverybody who has access to the information. Until you identify it, you really can't manage it."

Lee Kirschbaum, SVP and Head of Product, Marketing, and Alliances, Opus

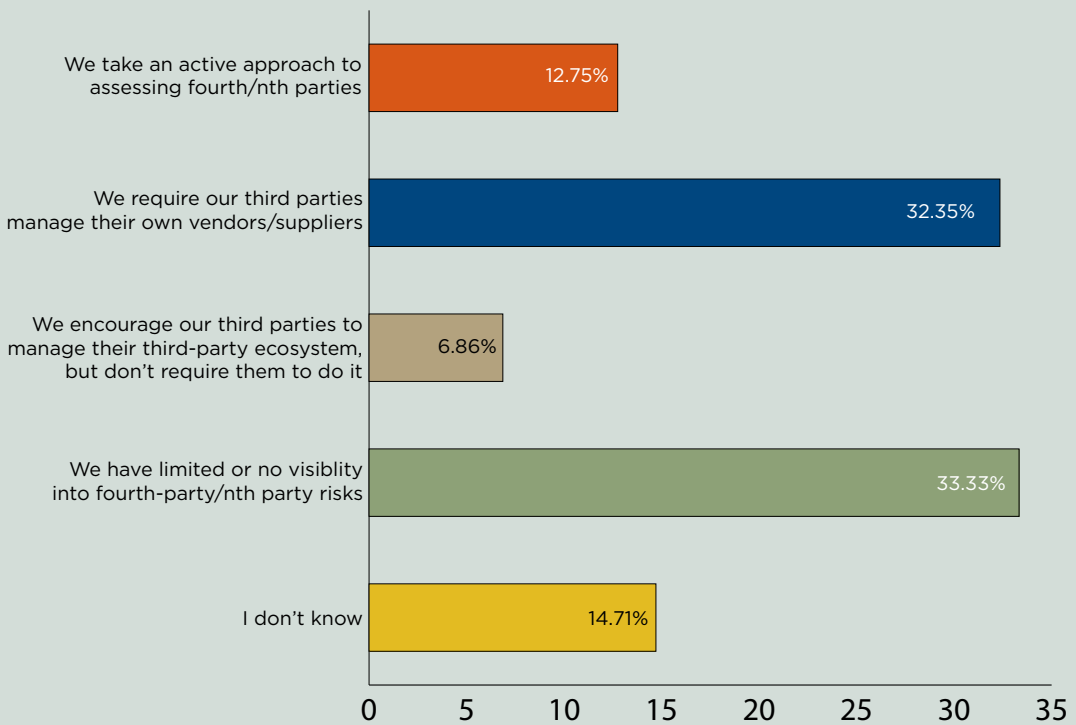
tate conversations between companies and their third parties concerning financial health and, thus, facilitate greater transparency between these business relationships.

Asked what actions they take when they identify a high-risk vendor or supplier, most respondents said they conduct an in-depth analysis and/or discuss potential steps to mitigate the risk. Other responses included scheduling a conversation with vendor/supplier executives; creating an action plan with the vendor/supplier; and/or conducting a site visit.

Whatever measures the business as the end customer uses to mitigate its own third-party risks, third parties can flow those same expectations down to their sub-contractors.

Centralize the risk management process. The Opus and RapidRatings survey revealed mixed results when it came to

To what degree does your organization monitor fourth-party/ nth-party risks/tier 2 and beyond suppliers?



Source: Compliance Week in partnership with OPUS and RapidRatings

centralized versus decentralized programs, with 44 percent saying they have a centralized model; 37 percent saying they have a decentralized model with centralized policies; and 19 percent saying they have completely decentralized model (separate polices and decisions at the department or regional level).

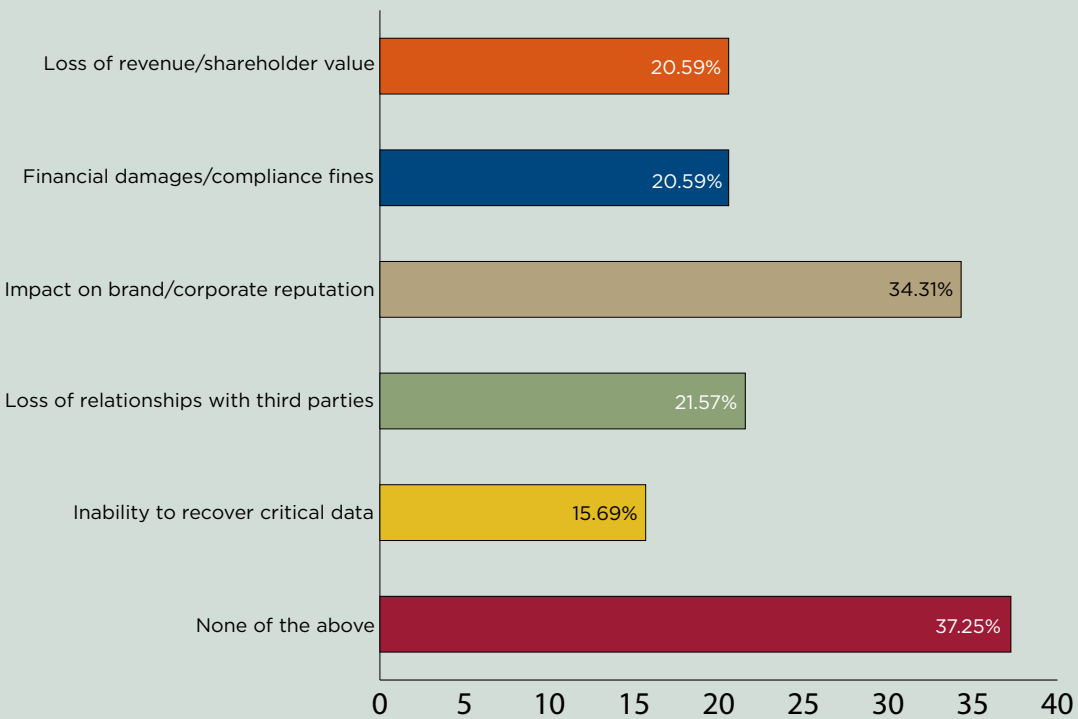
"I would hope and expect over the next few years to see more companies moving toward centralization," Gellert says. A centralized model drives efficiency not just from a cost perspective, but also in the quality of the analyses being performed, he says.

Make risk management a cross-functional effort. Some companies promote the sharing of their third-party risk data on vendors, suppliers, and partners more than others, depending on the maturity of the risk management program. According to the Opus and RapidRatings survey, responses varied from "partially, across some departments" to "completely, across the entire enterprise" to "not at all." Others said information-sharing is limited to a certain department or function.

Information-sharing is a critical aspect of a robust third- and fourth-party risk management program. "While it's important for a centralized group to control processes and policies, it's also important to collaborate," Kirschbaum says.

The need for business functions to join forces continues to grow dire, as third- and fourth-party risks continue to evolve, both in their scope and complexity. External factors like growing cyber-security risk and escalating regulatory mandates, like the EU's General Data Protection Regulation, are placing an enhanced emphasis on procurement, compliance, and risk management teams playing a leading, collaborative role. Ultimately, those with more mature risk management programs will not only reduce their financial, regulatory, and reputational risk, but gain a leg up in the marketplace as well. ■

What impacts from third-party risks have affected your organization most? Select all that apply.



Source: Compliance Week in partnership with OPUS and RapidRatings

ABOUT OPUS

Opus is a global risk and compliance SaaS and data solution provider founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace. Today, the world's most respected global corporations rely on Opus to free their business from the complexity and uncertainty of managing customer, supplier and third-party risks. By combining the most innovative SaaS platforms with unparalleled data solutions, Opus turns information into action so businesses thrive. For more information about Opus, please visit www.opus.com.

ABOUT RAPIDRATINGS

RapidRatings® is transforming the way the world's leading companies manage enterprise and financial risk. RapidRatings provides the most sophisticated analysis of the financial health of public and private companies in the world. The company's analytics system provides predictive insights into third-party partners, suppliers, vendors, customers and securities issuers. Every business conversation becomes more productive, transparent and efficient with the RapidRatings Financial Health SystemTM. For more information, visit ww.rapidratings.com.

COMPLIANCE WEEK

ABOUT COMPLIANCE WEEK

Compliance Week, published by Wilmington Group 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. Our mission is to help our subscribers comprehend and comply with the constantly evolving global regulations and standards to which public companies must adhere.