

Brought to you by the publishers of **COMPLIANCE WEEK**



Top TPRM priorities in 2023

An e-Book publication sponsored by **dun & bradstreet**

About Us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a quarterly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

Dun & Bradstreet, a leading global provider of business decisioning data and analytics, enables companies around the world to improve their business performance. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to accelerate revenue, lower cost, mitigate risk, and transform their businesses. Since 1841, companies of every size have relied on Dun & Bradstreet to help them manage risk and reveal opportunity. For more information on Dun & Bradstreet, please visit www.dnb.com.

Cybersecurity, regulatory risks lead TPRM priorities in 2023

Respondents to a survey from Compliance Week and Dun & Bradstreet overwhelmingly indicated cybersecurity to be the most important compliance-related area affecting third-party risk management in the new year, though fraud and other risks should still be on their radar.

BY AARON NICODEMUS

Compliance professionals will be most focused on addressing cybersecurity and regulatory compliance risks contained within their third-party relationships this year, according to the results of a new survey from Compliance Week and Dun & Bradstreet.

Out of 179 total respondents to the “State of Third-Party Risk Management in 2023” survey conducted online between October and November, 41 percent said cybersecurity was their top risk management priority. Second was regulatory compliance at 27 percent, followed by supplier risk at 15 percent; environmental, social, and governance (ESG) at 9 percent; and combating business fraud at 8 percent.

Approximately 37 percent of respondents said ESG was the least of their concerns of those five issues, followed by combating business fraud at 29 percent.

Another question asked which compliance-related area would be most important in 2023. Cybersecurity was the clear favorite among options provided at 65 percent, followed by anti-bribery/anti-money laundering (13 percent), climate-related risk disclosures (12 percent), and ISO frameworks (6 percent).

Survey respondents represented industries including fi-

nancial services (19 percent); healthcare (8 percent); manufacturing (6 percent); real estate, education, and technology (all 5 percent); and automotive, food and beverage, retail, pharmaceuticals, construction, and government (all 3 percent).

That cybersecurity is the top concern in assessing third-party relationships does not come as a surprise, said Paul Westcott, Dun & Bradstreet’s product director for know your customer/know your business (KYC/KYB).

“Cybersecurity can become a large reputational risk,” he said. “The results of a cyberattack can appear in the media much more quickly than many other types of risks.”

Regulatory compliance in 2022 was increasingly complicated by Russia’s war against Ukraine, a trend likely to continue in 2023. Many countries are continually adding companies and individuals to sanctions watchlists, creating a regular stream of potentially problematic new connections to third parties.

The key with assessing the risks these events pose is to determine ahead of time whether certain changes in your firm’s relationships with particular third parties are material to your operations, Westcott said.

“Fraud peaks under times of economic stress. That’s when good people do bad things. From my point of view, it’s going to be a tough year for fraud.”

– Brian Farley, VP, Business Segment Manager, Third-Party Risk and Compliance, Dun & Bradstreet

Survey respondents, when asked which third-party data they are most reliant on to assess their business relationships, said financial (55 percent), company principals/employees (52 percent), legal (50 percent), watchlists and sanctions (40 percent), and corporate linkage (31 percent). Respondents could choose more than one type of data. Less popular answers included firmographic/corporate entity and ultimate beneficial ownership, which both came in at 22 percent.

Some firms are moving away from only using data to drive decision-making about their partners and vendors, which can track patterns that are not material to the business relationship, Westcott said. Instead, they are transitioning to an event-based model, in which a change of ownership or significant shift in business model are more relevant, he said.

“It’s determining how material that risk is to my organization, in context to all of the other risks,” he said.

ESG being ranked so low by survey respondents is likely because of multiple factors in the market, said Brian Farley, Dun & Bradstreet’s vice president, business segment manager, third-party risk and compliance.

The first factor is companies are bracing for a recession, and efforts to measure, for example, the greenhouse gas

“Cybersecurity can become a large reputational risk. The results of a cyberattack can appear in the media much more quickly than many other types of risks.”

Paul Westcott, Product Director for KYC/KYB,
Dun & Bradstreet

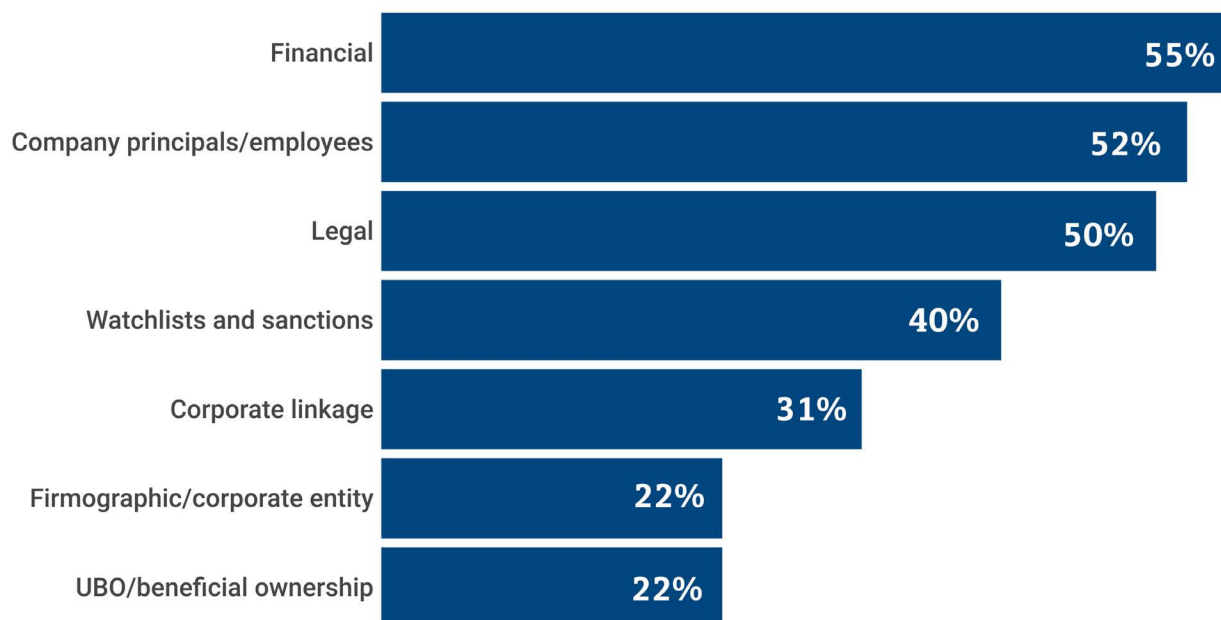
emissions of suppliers, are being pushed off.

Another factor is while regulators in Europe have begun requiring ESG-related disclosures, the climate-related disclosure rule proposed by the U.S. Securities and Exchange Commission has not been finalized.

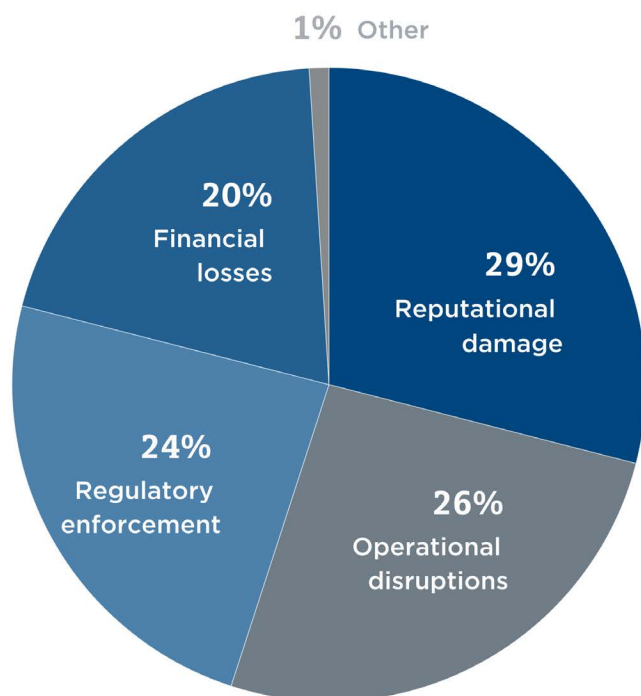
“The regulatory framework isn’t baked yet. People don’t want to invest in something, then learn they need a totally different solution,” Farley said.

Survey respondents said reputational damage is the most important consequence for not managing third-party risk

What types of data will you be most reliant on to perform customer and third-party due diligence? Choose all that apply.



What are you most concerned about if your compliance team is not effectively managing risk?

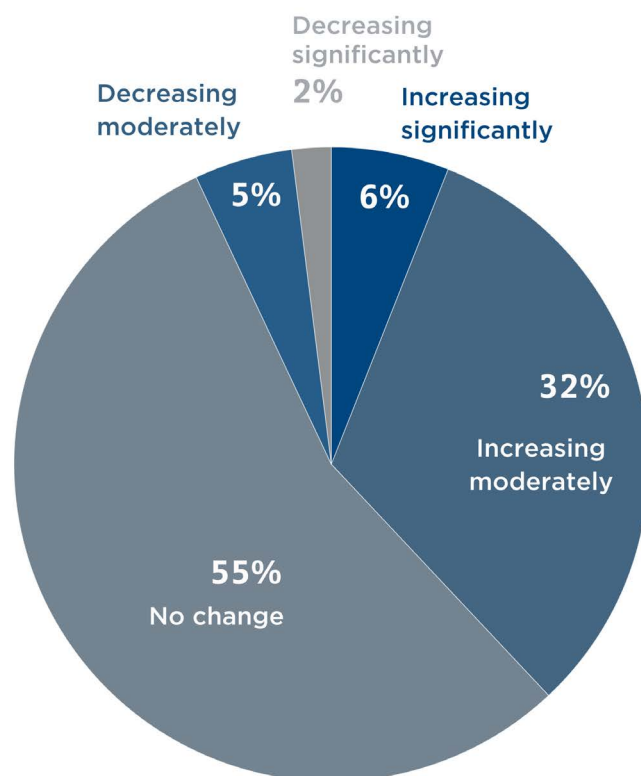


(29 percent), followed closely by operational disruptions (26 percent), regulatory enforcement (24 percent), and financial losses (20 percent).

More than half of survey respondents (54 percent) reported increasing vendor/third-party due diligence in response to global disruption, while 45 percent reported increasing their ongoing monitoring of their third parties. Respondents could choose as many responses as applied. Nearly two in five (39 percent) reported an increased reliance on risk data and analytics to drive decision-making. Only 18 percent reported no change to their third-party risk management priorities because of global disruptions.

When asked to choose all the ways their firm has reacted to increased scrutiny of sanctions compliance, one in three respondents said they invested or planned to invest in more standardized/actively monitored data. Nearly as many respondents (30 percent) reported their firms had enhanced

Have you observed B2B fraud increasing or decreasing in the past year?



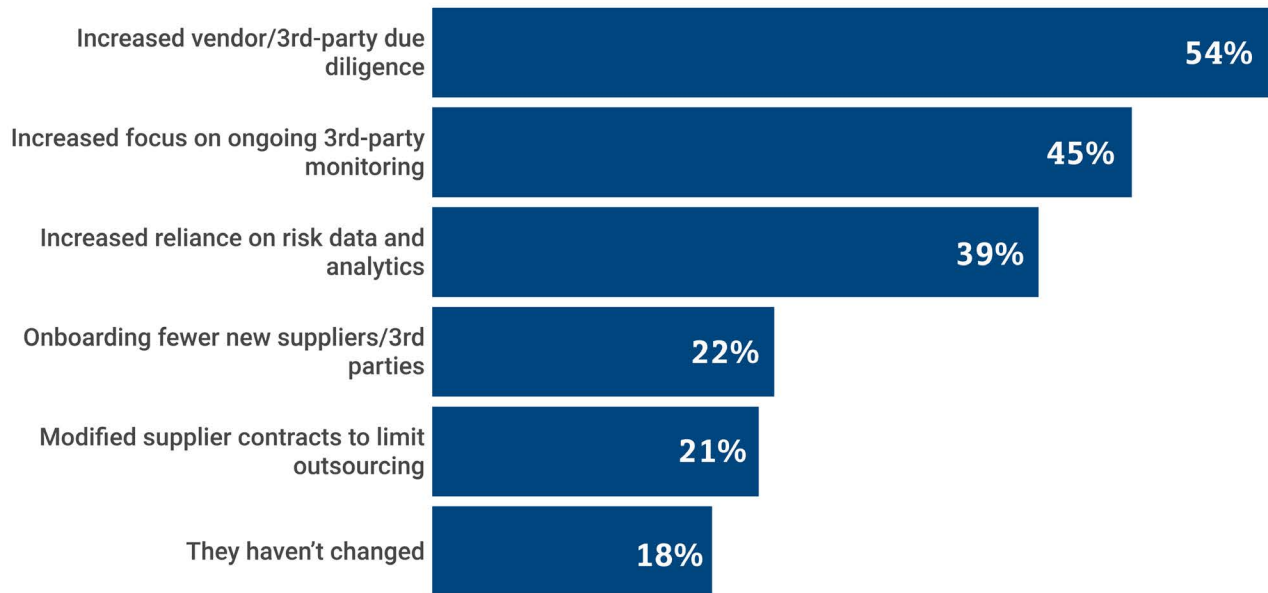
screening technology or implemented new sanctions compliance programs. Other responses included increasing sanctions screening frequency (29 percent) and ending high-risk relationships (22 percent).

Nearly a third (29 percent) of respondents said their business had not been impacted by sanctions.

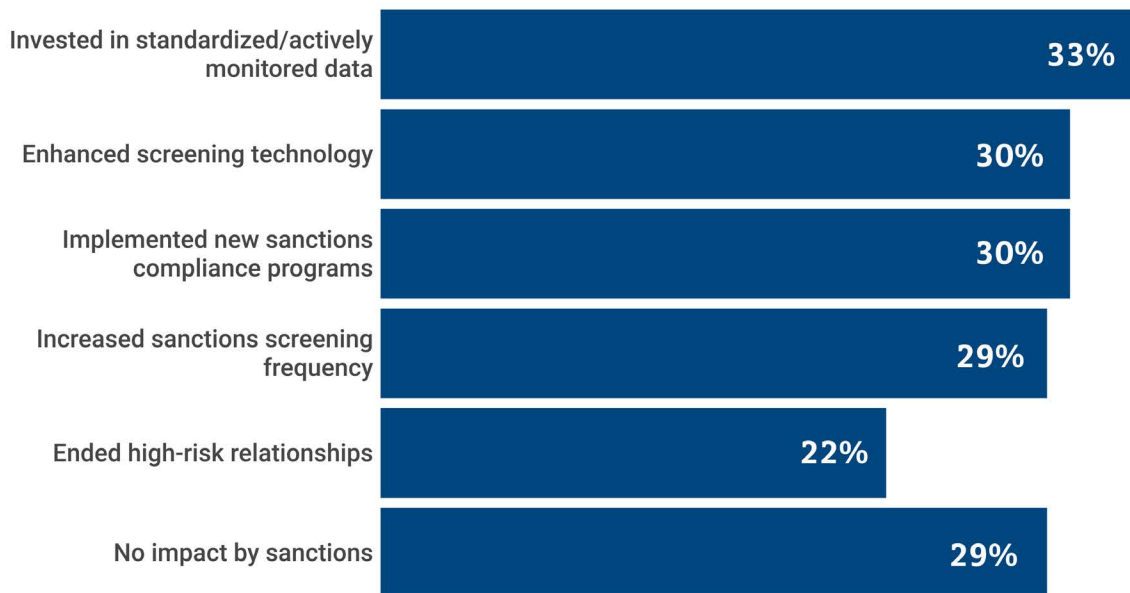
One question asked respondents if they have seen an increase or decrease in business-to-business fraud in the past year. More than half (55 percent) said they experienced no change. Nearly a third (32 percent) said it increased moderately. Six percent said such fraud increased significantly, while 7 percent said it was decreasing.

“This surprised me a little bit,” Farley said, particularly since there are signs of a recession coming in 2023. “Fraud peaks under times of economic stress. That’s when good people do bad things. From my point of view, it’s going to be a tough year for fraud.” ■

How have your TPRM priorities changed considering global disruption/instability? Choose all that apply.



How has your team responded to increased scrutiny of sanctions compliance? Choose all that apply.



Conclusion

The end in mind

Collectively, data is often cited as the missing element that will help finance and risk teams — including procurement and compliance — to “reimagine” risk management and achieve the upper hand in this climate of volatility and unpredictability. But more data isn’t necessarily good enough; the focus needs to be having the right data in the right places. When you start by defining the outcomes your data-driven organization requires, you’ve taken a critical first step that will serve as the north star, a directive, of your data strategy. This will clear the way for the necessary interrogation of processes and data completeness that will expand data value and eliminate the blind spots in your risk management efforts.



Learn more about why and how businesses can become more resilient and *future-ready* through better integration of finance and risk data.

ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of B2B data, insights and AI-driven platforms, helps organizations around the world grow and thrive. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to grow revenue, increase margins, manage risk, and help stay compliant—even in changing times. Since 1841, companies of every size have relied on Dun & Bradstreet. Dun & Bradstreet is publicly traded on the New York Stock Exchange (NYSE: DNB). Twitter: @DunBradstreet

© Dun & Bradstreet, Inc. 2023. All rights reserved. (CR-1203792219440615 01/23)

dnb.com

