

Vendor Landscape: Third-Party Risk Intelligence

Products Vie To Augment Your Survey-Based Program

by Claire O'Malley and Nick Hayes

October 20, 2017

Why Read This Report

Increasing business reliance on third-party ecosystems, coupled with worsening market volatility and threats, is forcing risk professionals to manage third-party risk at a new level. Point-in-time risk assessments no longer provide enough timely, relevant data to support effective risk management efforts. In response, third-party risk intelligence (TPRI) solutions enrich internal assessment data with external information and analysis. This vendor landscape examines the market for TPRI solutions.

Key Takeaways

TPRI Solutions Won't Replace A Poor Process

Risk managers should only license a TPRI solution after they've formalized a third-party risk management (TPRM) program. TPRI solutions aren't alternatives to good governance, so premature purchases will only feed data into messy, ad hoc processes.

Data Collection And Analysis Differentiate TPRI Solutions

Data capabilities separate the good from the best among TPRI vendors. After deciding which type of TPRI solution is best for your organization, pick your vendor by scrutinizing its collection and rating techniques to verify its reliability and relevance for your TPRM program.

Vendor Landscape: Third-Party Risk Intelligence

Products Vie To Augment Your Survey-Based Program

by [Claire O'Malley](#) and [Nick Hayes](#)
with [Christopher McClean](#) and Trevor Lyness
October 20, 2017

Table Of Contents

- 2 Companies Need Better Third-Party Risk Context, Faster**
Third-Party Risk Management Must Go Beyond Assessments
- 3 TPRI Vendors Analyze Your Third Parties' External Risk Data**
- 4 Three Distinct Use Cases Define TPRI Categories**
Enhanced Due Diligence Solutions Determine Whether To Engage With A Third Party
Physical And Supply-Chain Risk Monitoring Tools Help Spot And Manage Operational Crises
Third-Party Cyber Risk Scoring Tools Help Detect Risks And Prioritize Remediation

Recommendations

- 10 Use TPRI To Strengthen, Not Supplant, Your Current Approach**
- 12 Supplemental Material**

Related Research Documents

- [Assess Your GRC Program With Forrester's GRC Maturity Model](#)
- [The Forrester Wave™: Digital Risk Monitoring, Q3 2016](#)



Share reports with colleagues.
Enhance your membership with [Research Share](#).

Vendor Landscape: Third-Party Risk Intelligence Products Vie To Augment Your Survey-Based Program

Companies Need Better Third-Party Risk Context, Faster

You're only as strong as your weakest third party. Even more problematic, too many security and risk (S&R) professionals can't easily find their weakest links. For example, reports suggest that external companies had identified Equifax's poor application security as a risk factor before news of its breach went public; however, there's no evidence that the company's corporate customers broadly used that information to mitigate the risk or isolate themselves from the impact.¹ And companies that fail to establish controls to consistently detect and report illicit activities could incur major fines like McKesson's \$150 million US Drug Enforcement Administration settlement for inadequate oversight.² As business speeds up, organizations are falling even further behind in their attempts to manage and mitigate third-party risks.

Third-Party Risk Management Must Go Beyond Assessments

Point-in-time risk assessments no longer provide the right data to conduct effective TPRM. Risk managers need more reliable information to ensure that their risk assessments don't contain gaps, mistakes, or false information. More importantly, they need data to keep up with rapidly evolving business, geopolitical, and threat environments. Risk managers need to revamp their TPRM efforts with more contextual data because:

- › **Questionnaire practices are burdensome and error-prone.** Risk managers find third-party data collection increasingly difficult, even with more efficient workflow and reporting tools. This is why it's no surprise that the majority of global business and risk leaders lack confidence in TPRM processes (83%) and related technologies (91%).³ In part, this is due to the third parties themselves drowning in growing piles of longer, more detailed questionnaires. As a result, they miss deadlines, omit key information, and submit erroneous responses (whether intentionally or unintentionally). Meanwhile, risk managers make their own mistakes, word questions poorly, and fail to set and detect key risk indicators.
- › **Expanding third-party ecosystems complicate onboarding and risk prioritization.** Where do you start? With the rapid expansion of strategic partners, suppliers, vendors, affiliates, and other third parties, decisions about how to allocate limited resources become even more complex. Over 40% of global business and risk leaders believe their firms experienced meaningful increases in their level of third-party dependence over the past year alone.⁴ To make matters worse, risk managers must consider a growing set of risk issues, such as mounting cyberthreats, more severe environmental and reputational impacts, and destabilizing geopolitical and physical safety concerns with companies' global footprints.
- › **Regulatory bodies are toughening their stance on third-party accountability.** Recent regulatory developments make it clear that companies are responsible for third-party transgressions much to the same extent as their own. For example, the New York Department of Financial Services (NYDFS) Cybersecurity Regulation requires covered entities to issue and enforce cybersecurity

Vendor Landscape: Third-Party Risk Intelligence

Products Vie To Augment Your Survey-Based Program

guidelines for their third parties, including access controls, encryption standards, breach notifications, and use and protection of sensitive, proprietary data.⁵ Meanwhile, the US Office of the Comptroller of the Currency (OCC) issued detailed examination procedures that covered entities must follow as part of its “Third-Party Relationships: Risk Management Guidance.”⁶

- › **External factors are constantly altering the risk landscape.** Over the past year or so, we’ve experienced crippling ransomware attacks, the UK’s decision to leave the European Union (“Brexit”), devastating hurricanes, and one of the most egregious data breaches to date (i.e., Equifax). This small sampling of global risk events highlights just how fast our risk and business environments change, putting our business operations at heightened risk. To counter this volatile market environment, risk managers need to constantly update their third-party risk data to provide ongoing support for strategic decisions.

TPRI Vendors Analyze Your Third Parties’ External Risk Data

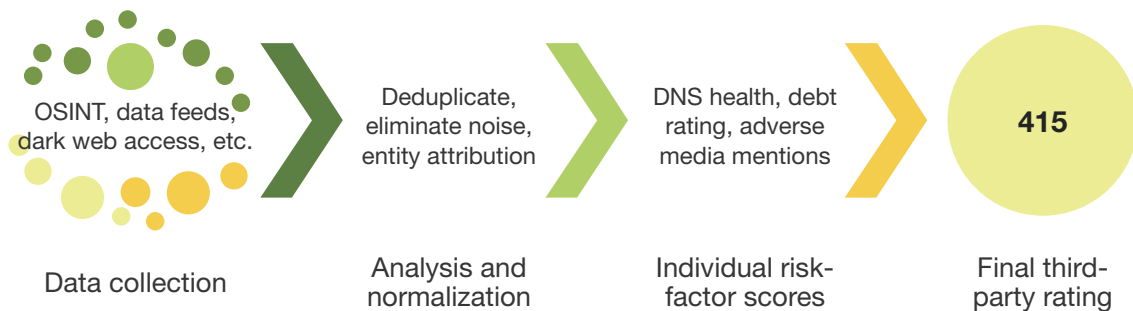
Third-party risk intelligence solutions enrich the context your firm uses to make third-party decisions by aggregating and analyzing data from a host of sources. Vendors in this space continuously update this data, often in close to real time. This helps risk managers lessen their dependence on questionnaires, validate the accuracy of vendor responses, and add detail to vendor risk profiles. TPRI solutions all provide the following core capabilities:

- › **External data collection, access, and feeds that provide risk breadth and depth.** All vendors aggregate and normalize data using a variety of proprietary techniques, public and pay-for-access APIs, web crawlers, media aggregators, threat intelligence partners, government and law enforcement watchlists, and other sources. In addition to the breadth of data these solutions analyze, their deduplication and normalization techniques are also important to consider, as they can significantly affect the relevance of results and number of false positives and negatives (see Figure 1).
- › **Risk analytics that turns raw data into scores and decision criteria.** TPRI solutions employ data science and algorithms to uncover hidden patterns and anomalies to enrich data relevance, attribution, and risk measurements. Some solutions leverage advanced data science techniques for risk analysis, such as machine learning, data clustering, and other forms of artificial intelligence (AI).
- › **Consistent risk scales and methodologies that allow critical comparisons.** A common risk framework helps users evaluate their third parties in a consistent manner. Risk scales include basic high/medium/low scores, A-to-F risk grades, more detailed 0 to 100 ranges, and even scores modeled on a personal credit score range (i.e., 300 to 850). While the varying scales aren’t differentiating features, it’s worth considering which fits better with your existing approach and, more importantly, whether the results correlate to real-world risk exposure.

Vendor Landscape: Third-Party Risk Intelligence

Products Vendors Use To Augment Your Survey-Based Program

- › **Specialized and repeatable offerings that cater to specific third-party risk initiatives.** With enough time and resources, many business intelligence (BI) vendors could tailor their solutions to identify and monitor third-party risk, but this would require a lot of upfront support, customization, and integration of new data sources. TPRI vendors allow customers to skip these steps by offering packaged solutions that specifically target TPRM initiatives, such as due diligence and risk scoring.
- › **Detailed third-party risk profiles and summary reports.** Risk managers can use these products to produce detailed profiles of individual third parties for deep review and analysis. These reports offer high-level risk analysis as well as a deeper dive into the source information to understand how the product derived the resulting score. Dashboards show risk exposure across the entire third-party landscape and allow comparisons by type of third party, region, business function, or other attributes.

FIGURE 1 Common Third-Party Risk Intelligence Data Collection Process

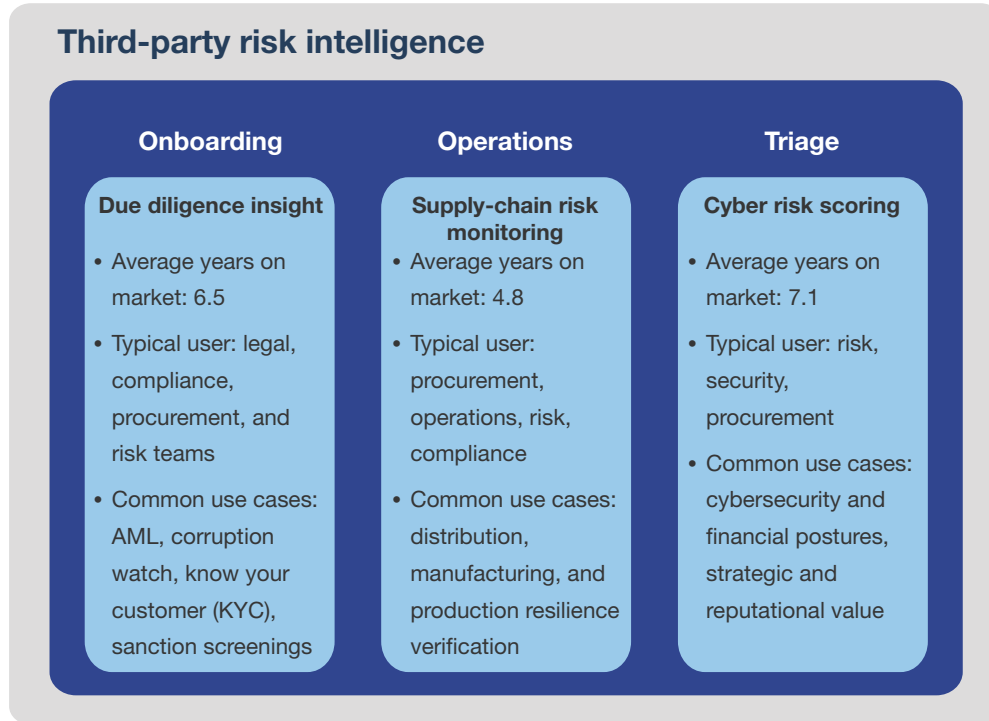
Three Distinct Use Cases Define TPRI Categories

The TPRI market covers a broad set of vendors with offerings that vary in terms of data, functionality, and targeted use cases. Here, we cover three of the most common TPRI solution categories: 1) enhanced due diligence, 2) physical and supply-chain risk monitoring, and 3) third-party cyber risk scoring (see Figure 2). Organizations often use solutions in more than one category to support the needs of different security, risk, and compliance functions.

Vendor Landscape: Third-Party Risk Intelligence

Products Vies To Augment Your Survey-Based Program

FIGURE 2 Three Of The Most Common Third-Party Risk Intelligence Solution Use Cases



Enhanced Due Diligence Solutions Determine Whether To Engage With A Third Party

Risk and compliance managers most commonly use enhanced due diligence reports to assess third-party risk before onboarding a new partner; additional use cases include merger and acquisition (M&A) analyses and financial performance reviews. Managers also validate prospective partner firms' regulatory and ethical standing relating to issues such as anti-bribery and corruption (ABAC), anti-money laundering (AML), and environment, social, and governance (ESG) efforts. The following capabilities and example vendors represent this market (see Figure 3):

- › **Core capabilities include baseline regulatory and business health data.** Solutions in this category typically collect and analyze data from a broad set of sanction lists, regulatory and law enforcement lists, government sites, business and corporate registers, and news and media aggregators. They generate detailed reports covering financial viability, possible regulatory issues, and nonfinancial risk indicators that may signal early, connected risks. Many solutions offer some degree of integration with governance, risk management, and compliance (GRC) platforms and other enterprise systems as well.


Vendor Landscape: Third-Party Risk Intelligence

Products Vendors Use To Augment Your Survey-Based Program

- › **Key differentiators include expanded data breadth and advanced risk analysis.** A core feature differentiating vendors in this space is the breadth and depth of risk data they can uncover about a particular entity. This requires not only vast data access but sophisticated link analysis and entity attribution capabilities to identify masked parent companies, subsidiaries, affiliates, and other key business relationships. Solutions that can import and analyze additional third-party data, such as financial reports of private companies, can help improve risk assessment consistency as well. Beyond financials, look for solutions in this market that can also assess reputational risk exposure.
- › **There are several vendors to consider for enhanced due diligence.** Vendors reviewed in this report include Argos Risk, Bureau van Dijk (BvD), Exiger, LexisNexis Risk Solutions, RapidRatings, RepRisk, and Thomson Reuters. Other relevant vendors include Dun & Bradstreet, Dow Jones, Kroll, and Regulatory Data Corporation (RDC).

Vendor Landscape: Third-Party Risk Intelligence
 Products Vie To Augment Your Survey-Based Program

FIGURE 3 Third-Party Risk Intelligence Enhanced Due Diligence Solution Comparison

 The spreadsheet associated with this figure contains additional data clarifying the difference between standard and extensive capabilities.

Due diligence insight	Argos Risk	Bureau van Dijk (BvD)	Exiger (DDIQ)	LexisNexis Risk Solutions	Rapid-Ratings	RepRisk	Thomson Reuters
Risk score (low-high)	100-0	AAA-D	L-M-H	N/A	100-0	0-100	N/A
Business data collection		●	●	●			●
Risk rating/index for global benchmarking					●	●	
Entity attribution and link analysis		●		●			●
Watchlists, government and regulatory feeds		●	●	●			●
Internal, private third-party data analysis			●		●		
Environmental, social, and governance (ESG) data analysis						●	
Risk analytics			●		●		
Flexible risk weightings and alerts	●				●	●	
GRC integration	●				●	●	●
Human analysis and support			●	●		●	●

LEGEND:

Limited/no capabilities Standard capabilities Extensive capabilities


Physical And Supply-Chain Risk Monitoring Tools Help Spot And Manage Operational Crises

These vendors aggregate and analyze data related to third parties’ physical operations, severe weather exposure, supply chain resilience, and workplace safety. They are essential for risk managers to prepare for and manage corporate crises, such as supplier outages, protests, and social unrest, and they offer geopolitical and regional intelligence to inform strategic planning. They also track compliance related to issues such as modern slavery, conflict minerals, and food safety. The following capabilities and vendors describe the physical and supply-chain risk monitoring market (see Figure 4):

Vendor Landscape: Third-Party Risk Intelligence
 Products Vie To Augment Your Survey-Based Program

- › **Core capabilities provide geospatial context and location-based risk monitoring.** Physical and supply-chain risk monitoring solutions all offer data for adverse media monitoring and geopolitical risk analysis, with geospatial dashboard visualization that overlays risk information on geographic maps. These capabilities help risk managers identify supply chain dependencies and simulate scenarios to determine the efficacy of contingency plans. Additionally, they can help actively monitor for risk events and send automated alerts when specified thresholds are met.
- › **Key differentiators include advanced risk analysis, visualizations, and crisis support.** Data sources are relatively diverse in this category, but the degree to which the solutions apply advanced data science techniques and measure risk exposure distinguishes competing offerings. Determine whether you plan to use the solution mainly for risk monitoring or as more of a command center during a crisis. For the former, focus on data collection, analytics, and configurability; for the latter, focus on crisis response, mobile support, and breadth of data support.
- › **There are several vendors to consider for physical and supply-chain risk monitoring.** Vendors reviewed for this report include Everbridge, KPMG, Resilinc, and riskmethods. Other relevant vendors include DHL, Elementum, Prevalent, and Supply Risk Solutions.

FIGURE 4 Third-Party Risk Intelligence Physical And Supply-Chain Risk Monitoring Solution Comparison

 The spreadsheet associated with this figure contains additional data clarifying the difference between standard and extensive capabilities.

Supply-chain risk monitoring	Everbridge	KPMG	Resilinc	riskmethods
Risk score (low-high)	N/A	0-100	1-10	0-100
Severe weather/physical safety data	●			
Adverse media feeds and analysis		●	●	
Geopolitical risk data and analysis	●		●	●
Business and regulatory intelligence		●		
Internal data integration	●		●	●
Risk analytics		●		●
Configurable tiering, risk weightings		●	●	●
Mobile support	●		●	●
Risk visualization	●		●	●
Crisis response coordination	●			

LEGEND:

Limited/no capabilities Standard capabilities Extensive capabilities

Vendor Landscape: Third-Party Risk Intelligence

Products Vendors Use To Augment Your Survey-Based Program


Third-Party Cyber Risk Scoring Tools Help Detect Risks And Prioritize Remediation

Third-party cyber risk scoring solutions aggregate and analyze external data to evaluate the cybersecurity posture of a third party. These solutions monitor a company's external network traffic and dark-web chatter to assess attributes like patching cadence, application security posture, and indications of compromise. Security and risk pros use this information to gauge vendors' security exposure, prioritize mitigation efforts, and track any significant changes. The following capabilities and vendors represent the third-party cyber risk scoring market (see Figure 5):

- › **Core capabilities gather data to evaluate how secure partners are.** All vendors in this market provide a cyber risk score to help users evaluate third-party entities on an ongoing basis. They typically gather their own data via proprietary web crawlers and other collection techniques, but a few rely on strategic partnerships with threat intelligence providers to source similar cyber risk data. To help clients encourage action, these solutions also allow customers to share individual reports with or provide a dedicated portal to the relevant third party.
- › **Key differentiators include flexibility, transparency, and the relevance of risk scores.** To select the best vendor in this market, one of the first questions to ask is whether the vendor has compared the results of its scoring methodology to historical breach data. This helps ensure that the characteristics that make up vendor scores offer relevant risk insight. Beyond that, look for vendors that are more transparent in the scoring approach, offer flexible vendor tiering and alerts, and help you work with your third parties to remediate any outstanding issues. Lastly, consider whether you will integrate these scores into your internal risk processes or use this product as your TPRM platform.
- › **There are several vendors to consider for third-party cyber risk scoring.** Vendors reviewed in this report include BitSight, CORL Technologies, CyberGRX, FICO, LookingGlass, Optiv, SecurityScorecard, and SurfWatch Labs. Other relevant vendors include Prevalent, RiskIQ, RiskRecon, and UpGuard.

Vendor Landscape: Third-Party Risk Intelligence
 Products Vie To Augment Your Survey-Based Program

FIGURE 5 Third-Party Risk Intelligence Third-Party Cyber Risk Scoring Solution Comparison

 The spreadsheet associated with this figure contains additional data clarifying the difference between standard and extensive capabilities.

Vendor cyber risk scoring	BitSight Technologies	CORL Technologies	Cyber-GRX	FICO	Looking-Glass	Optiv	Security-Scorecard	Surf-Watch Labs
Risk score (low-high)	250-900	A-F	1-100	300-850	0-100	1-1,000	A-F	0-100
Web data collection	●				●			●
Dark web and threat intelligence	●				●		●	●
Business intelligence			●			●		
Risk assessment/questionnaire builder		●	●			●		
GRC platform integration	●	●					●	
Configurable tiering and alerts	●			●		●		●
Risk analytics	●			●			●	
Proven score-breach correlation	●			●				
Vendor review and collaboration	●		●	●		●	●	

LEGEND:

 Limited/no capabilities  Standard capabilities  Extensive capabilities

Recommendations

Use TPRI To Strengthen, Not Supplant, Your Current Approach

Third-party risk intelligence solutions will add value to security and risk pros’ existing third-party risk management efforts by improving process efficiency, reducing the risk of losses and fines, and providing insight to guide partnership decisions. Most importantly, they offer you an impartial lens to better identify and manage threats, vulnerabilities, and business risks so you can protect your organization. But before you set out to select a TPRI solution, make sure that you:

Vendor Landscape: Third-Party Risk Intelligence

Products Vendors Use To Augment Your Survey-Based Program

- › **Mature your internal TPRM efforts first.** TPRI tools can help you reach new levels of program maturity and efficiency, but only if you have the right foundation in place. It doesn't matter that you've identified new risks if you have no consistent way to document or address them. Assess the maturity of your risk and compliance program and make sure you have well-established workflows and objectives.⁷ Once your team is comfortable with the program for managing third-party risk, look to TPRI solutions to make further improvements.
- › **Scrutinize TPRI vendors' data collection and risk-scoring techniques.** Force vendors to pull back the curtains so you feel comfortable with the way their solution collects data and confident that their risk-scoring methodology is reliable. Then ask vendors to demonstrate that their scoring methodology correlates with a higher probability of data breaches. If the vendor conducted the analysis itself, request a copy of the analysis to verify it. Lastly, require that you speak to at least one customer reference about their experience and the results they've seen.
- › **Verify that your vendor follows core principles for cybersecurity risk ratings.** The US Chamber of Commerce announced in June 2017 that a consortium of public and private companies established the "Principles for Fair and Accurate Security Ratings," whose tenets encourage many best practices, such as transparency, dispute and correction rights, independence, and confidentiality.⁸ This is important guidance not just for selecting the right vendor but also to maintain valuable third-party relationships by giving partners ample opportunity to clarify and resolve any potential issues.
- › **Reconcile how you'll manage TPRI data with existing risk technologies.** If you're like a lot of S&R pros, you already use a GRC platform to manage third-party risk for your organization. If you do, you're well positioned to make use of TPRI right away. However, as you select and implement your TPRI solution, consider how existing processes will change. Thankfully, many of the TPRI vendors already have strategic partnerships with GRC platforms, and if they regularly work with yours, all the better.

Vendor Landscape: Third-Party Risk Intelligence

Products Vies To Augment Your Survey-Based Program

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

[Learn more.](#)

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

[Learn more.](#)

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

[Learn more.](#)



Forrester's research apps for iOS and Android.

Stay ahead of your competition no matter where you are.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Argos Risk

Exiger

BitSight

FICO

Bureau van Dijk (BvD)

KPMG

CORL Technologies

LexisNexis Risk Solutions

CyberGRX

LookingGlass

Everbridge

Optiv

Vendor Landscape: Third-Party Risk Intelligence

Products Vies To Augment Your Survey-Based Program

Rapid Ratings

SecurityScorecard

RepRisk

SurfWatch Labs

Resilinc

Thomson Reuters

riskmethods

Endnotes

- ¹ Source: George V. Hulme, "Equifax Rated 'F' in Application Security Before Breach," Security Boulevard, September 11, 2017 (<https://securityboulevard.com/2017/09/equifax-rated-f-application-security-breach/>).
- ² Source: Jeanne Whalen, "McKesson to Pay \$150 Million for Failing to Report 'Suspicious' Drug Orders," The Wall Street Journal, January 17, 2017 (<https://www.wsj.com/articles/mckesson-to-pay-150-million-for-failing-to-report-suspicious-drug-orders-1484699478>).
- ³ Source: "Third-party Governance and Risk Management," Deloitte, 2017. (<https://www2.deloitte.com/uk/en/pages/risk/articles/third-party-risk.html>).
- ⁴ Source: "Third-party Governance and Risk Management," Deloitte, 2017. (<https://www2.deloitte.com/uk/en/pages/risk/articles/third-party-risk.html>).
- ⁵ Source: Maria T. Vullo, "23 NYCRR 500: Cybersecurity Requirements For Financial Services Companies," New York State Department Of Financial Services, March 1, 2017 (<http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>).
- ⁶ Source: "OCC Bulletin 2017-7: Supplemental Examination Procedures for Risk Management of Third-Party Relationships," The US Office of the Comptroller of the Currency, January 24, 2017 (<https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html>).
- ⁷ The Forrester GRC Maturity Model helps risk management professionals objectively assess their GRC efforts to identify areas of weakness as well as centers of excellence, then outline a strategy to make appropriate improvements. The model consists of 14 functions and 59 components within the domains of oversight, technology, process, and people, each with detailed assessment criteria to provide a consistent and objective method of assessment. See the Forrester report "[Assess Your GRC Program With Forrester's GRC Maturity Model.](#)"
- ⁸ Source: "Principles for Fair and Accurate Security Ratings," U.S. Chamber of Commerce, June 20, 2017 (<https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings>).

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- › Core research and tools
- › Data and analytics
- › Peer collaboration
- › Analyst engagement
- › Consulting
- › Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
› Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.