Building trust with your third parties in a technology-driven and disruptive world

EY Global Third-Party Risk Management Survey 2019–20

Overall survey results
Disclaimer

- EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.
- This presentation is © 2020 EYGM Limited. All Rights Reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form or by any means, electronic or mechanical, including by photocopying, facsimile transmission, recording, rekeying, or using any information storage and retrieval system, without written permission. Any reproduction, transmission or distribution of this form or any of the material herein is prohibited and is in violation of US and international law.
- These slides are for educational purposes only and are not intended, and should not be relied upon, as accounting advice.
- Percentages are shown as whole numbers. As a result, some percentages may not sum to 100%
Table of contents

03 Global results
05 Survey respondent demographics
08 Third-party risk management program/function organization, governance and oversight
14 Third-party population breakdown/risk tiering
18 Assessments
25 Issue management/risk treatment
28 Fourth-party management
31 Technology
34 Reporting
36 Cybersecurity and threat intelligence
39 Inbound requests
42 Privacy regulations
44 Regulatory and internal audit exams
46 Nontraditional third parties
48 Concentration risks (financial services only)
50 Affiliate management (financial services only)
54 Innovation
56 Areas of investment
Global results
From July through September of 2019, EY professionals conducted a survey of 246 organizations of various sizes and maturity levels from around the globe and across a variety of industries. Although the executives who completed the survey were from various functions within each organization, all functions had a role in third-party risk. These functions included, but were not limited to, enterprise risk management, procurement, cybersecurity, internal audit and finance. The purpose of the survey was to address the distinctive nature of third-party risk across industries.

Industries in the survey included, but were not limited to, financial services, consumer products and retail, health care, life sciences, media and entertainment, technology, power and utilities, diversified industrial products, and government and public sector.

In this survey, we asked participants to respond to questions within several key areas of their respective third-party risk management (TPRM) programs. Topics included:

- Third-party risk management program/function organization, governance and oversight
- Third-party population breakdown/risk tiering
- Assessments
- Issue management/risk treatment
- Fourth-party management
- Reporting
- Technology
- Cybersecurity and threat intelligence
  - Inbound requests
  - Privacy regulations
  - Regulatory and internal audit exams
  - Nontraditional third parties
  - Concentration risks (financial services only)
  - Affiliate management (financial services only)
- Innovation

This document includes the results aggregated for each question across all industries. For any questions, support for data interpretation or specific data requests, please reach out to tprm@ey.com.
Survey respondent demographics
Of the 246 survey participants, the largest number of respondents came from the banking and capital markets sector, a result of the tenure of programs and regulatory pressures. This group was followed by insurance; technology, media and entertainment, telecommunications; advanced manufacturing and mobility; and consumer.

### Respondent profile (Q1) number of respondents

<table>
<thead>
<tr>
<th>Industry</th>
<th>Number of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking and capital markets</td>
<td>73</td>
</tr>
<tr>
<td>Insurance</td>
<td>37</td>
</tr>
<tr>
<td>Technology, media and entertainment, telecommunications (TMT)</td>
<td>24</td>
</tr>
<tr>
<td>Other</td>
<td>24</td>
</tr>
<tr>
<td>Advanced manufacturing and mobility</td>
<td>22</td>
</tr>
<tr>
<td>Consumer</td>
<td>15</td>
</tr>
<tr>
<td>Power and utilities</td>
<td>14</td>
</tr>
<tr>
<td>Wealth and asset management</td>
<td>13</td>
</tr>
<tr>
<td>Health</td>
<td>12</td>
</tr>
<tr>
<td>Life sciences</td>
<td>12</td>
</tr>
</tbody>
</table>

- Number of respondents
Almost two-thirds of the companies surveyed were in the US, more than one-quarter in Europe, and the remainder in Asia-Pacific. The companies were nearly evenly split among those that had third-party risk management programs in place for more than five years, three to five years and fewer than three years.

## Respondent profile (Q2, Q3, Q4)

<table>
<thead>
<tr>
<th>Region</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>155 (63%)</td>
</tr>
<tr>
<td>Europe</td>
<td>75 (30%)</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>16 (7%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By company size (headcount)</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 5,000</td>
<td>88 (36%)</td>
</tr>
<tr>
<td>5,001 to 15,000</td>
<td>52 (21%)</td>
</tr>
<tr>
<td>15,001 to 25,000</td>
<td>27 (11%)</td>
</tr>
<tr>
<td>25,001 to 50,000</td>
<td>25 (10%)</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>28 (11%)</td>
</tr>
<tr>
<td>More than 100,000</td>
<td>26 (11%)</td>
</tr>
</tbody>
</table>

## TPRM program resources

Q8. How many resources support your third-party risk management program/function in the following categories?

- Dedicated TPRM Resources
- Resources within the business to support the TPRM program/function

- 0: 17%
- 1-5: 36%
- 6-10: 18%
- 11-15: 17%
- 16-20: 16%
- 21-25: 6%
- 26-50: 4%
- 51+: 11%
Third-party risk management program/function organization, governance and oversight
TPRM program structure
Q5. How is your third-party risk management program/function structured?

- Centralized — enterprise-wide TPRM office responsible for setting organization-wide standards
- Decentralized — TPRM offices embedded within each business area
- Unknown/uncertain
- Hybrid — TPRM offices located both within the business areas and centrally at the enterprise level

TPRM committee oversight
Q6. Which of the following committees oversees your third-party risk management program/function activities?

- Risk committee: 55%
- Other oversight committee: 25%
- Third-party risk management steering committee: 22%
- Unknown/uncertain: 13%

Centralized and hybrid models continue to be the most common structure for TPRM programs, signifying the importance of a consistent, yet flexible, TPRM function across the organization.
Looking out over the next two to three years, there is a clear desire among the organizations surveyed to leverage external solutions more actively. More than 40% of the organizations surveyed expect to more frequently use managed service providers or co-sourcing to execute their third-party risk management function; that figure jumps to more than 50% for market utilities or sector-based consortiums.
There is still no consensus across the organizations surveyed as to who owns the TPRM function; 26% of respondents indicated that procurement has primary ownership, while 15% indicated that operational/enterprise risk owns it. An additional 15% indicated they have a dedicated TPRM group that owns it.
TPRM functional area responsibility

Q10. Which functional area has primary responsibility for the execution of the following components of your organization’s third-party risk management program/function?

<table>
<thead>
<tr>
<th>Component</th>
<th>Procurement</th>
<th>Third-party risk management</th>
<th>Legal/general counsel</th>
<th>Information security</th>
<th>Operational/enterprise risk</th>
<th>Compliance</th>
<th>Line of business</th>
<th>Technology/operations</th>
<th>Internal audit</th>
<th>Other</th>
<th>Not conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party inventory management</td>
<td>40%</td>
<td>20%</td>
<td>2%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>11%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>5%</td>
</tr>
<tr>
<td>Design and facilitation of the inherent risk assessment process/framework</td>
<td>12%</td>
<td>24%</td>
<td>5%</td>
<td>16%</td>
<td>17%</td>
<td>11%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Review and updating of contract terms as part of ongoing monitoring</td>
<td>27%</td>
<td>5%</td>
<td>35%</td>
<td>7%</td>
<td>1%</td>
<td>5%</td>
<td>15%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
</tr>
<tr>
<td>Identification of expired contracts</td>
<td>48%</td>
<td>4%</td>
<td>17%</td>
<td>2%</td>
<td>1%</td>
<td>2%</td>
<td>21%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
</tr>
<tr>
<td>Termination of contracts</td>
<td>38%</td>
<td>4%</td>
<td>24%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>25%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Issue management/risk treatment</td>
<td>8%</td>
<td>15%</td>
<td>6%</td>
<td>12%</td>
<td>14%</td>
<td>11%</td>
<td>24%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Note: Outlined percentages represent responses greater than 20%
TPRM policy types

Q11. Which of the following best describes the policies your organization has in place to support your third-party risk management program/function?

More than half of the organizations surveyed indicated they have comprehensive policies that are enforced and integrated; however, 39% indicated that policies are either documented but not enforced or exist but are not fully documented, indicating that there is a long way to go on the maturity curve for many organizations.
Third-party population breakdown/risk tiering
Contrary to previous years, when there was general consensus on the percentage of third parties subject to the TPRM program or a risk assessment, there is now more variability in the subsets of the overall inventory. This is likely due to continual challenges on totality of inventories and the changing environment of relevant risks.

Third-party volume

Q12. Approximately how many third parties does your organization work with on an annual basis?

Of the total number of third parties, approximately how many third parties are in scope for your third-party risk management program/function?

Of the total number of third parties in your program/function, how many have been risk-assessed?
Third-party risk scale
Q13. What percentage of third parties is in scope for your third-party risk management program/function in each of your organization’s risk tiers/ranks? Total must equal 100%.

- Critical third parties: 18%
- Highest-risk tier (not including critical third parties): 26%
- Second-highest risk: 17%
- Third-highest risk: 20%
- Remaining risk: 19%

In comparison with previous years, the nature of critical third parties is highly dependent on sector differences in maturity.
Information maintained

Q14. What types of information do you maintain with respect to your third parties?

<table>
<thead>
<tr>
<th>Information Maintained</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party master</td>
<td>89%</td>
</tr>
<tr>
<td>Third-party point of contact and/or relationship manager</td>
<td>87%</td>
</tr>
<tr>
<td>Service details</td>
<td>84%</td>
</tr>
<tr>
<td>Contract information</td>
<td>82%</td>
</tr>
<tr>
<td>Assessment details</td>
<td>72%</td>
</tr>
<tr>
<td>Risk rating</td>
<td>72%</td>
</tr>
<tr>
<td>Types of data/systems accessed</td>
<td>67%</td>
</tr>
<tr>
<td>Methods by which data/systems are accessed</td>
<td>53%</td>
</tr>
<tr>
<td>Applicability of relevant regulations</td>
<td>43%</td>
</tr>
<tr>
<td>Fourth parties supporting critical third-party services</td>
<td>39%</td>
</tr>
<tr>
<td>Fourth parties supporting any third-party services</td>
<td>24%</td>
</tr>
<tr>
<td>Unknown/uncertain</td>
<td>7%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

Critical third-party criteria

Q15. What are the three most important criteria your organization uses to define a critical third party?

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitivity of data involved in providing the service</td>
<td>18%</td>
</tr>
<tr>
<td>Business continuity and resiliency</td>
<td>16%</td>
</tr>
<tr>
<td>Strategic importance</td>
<td>14%</td>
</tr>
<tr>
<td>Financial impact</td>
<td>13%</td>
</tr>
<tr>
<td>Type of data and systems accessed</td>
<td>12%</td>
</tr>
<tr>
<td>Organizational footprint (delivery of services across the organization)</td>
<td>10%</td>
</tr>
<tr>
<td>Reputational impact</td>
<td>7%</td>
</tr>
<tr>
<td>Amount of spend</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>We do not maintain a list of critical third parties</td>
<td>2%</td>
</tr>
<tr>
<td>Physical access</td>
<td>1%</td>
</tr>
<tr>
<td>Unknown/uncertain</td>
<td>1%</td>
</tr>
</tbody>
</table>
Assessments
For nearly two in three organizations surveyed, the inherent risk profile of third parties is reassessed either based upon their inherent rating (e.g., only reassessing higher-risk third parties) or on a regular basis (e.g., annually) showing that continual refreshes do not always depend on a contract event.

Assessing inherent risk of third party
Q16. What is your organization’s approach to refreshing/reassessing the inherent risk profile of your third parties?
Pre-contract risk assessments

Q17. Does your organization currently conduct pre-contract due diligence risk assessments?

- Yes: 87%
- No: 7%
- Unknown/uncertain: 6%

Q18. [If Yes to Q17] What level of depth is your organization's pre-contract due diligence risk/control assessment?

- Same level of depth as post-contract monitoring risk assessments: 57%
- Due diligence risk/control assessments are only conducted pre-contract: 26%
- Lighter touch than post-contract risk/control assessments: 15%
- Unknown/uncertain: 3%

Q19. [If Yes to Q17] Does your organization have an expedited process for pre-contract risk assessments for urgent requests?

- Yes: 50%
- No: 39%
- Unknown/uncertain: 12%
Based on survey responses, the typical pre- and post-contract risk assessment questionnaires typically have fewer than 200 questions. Cybersecurity and privacy risk account for almost half of all questions asked, aligning with respondents’ answers to prior question on most important criteria of data sensitivity (Q15).

### Risk assessment questionnaire

Q20. How many questions within your organization’s risk/control assessment questionnaires are used to assess third parties in each of the following risk areas?

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Inherent risk assessment questionnaire</th>
<th>Pre-contract risk assessment questionnaire</th>
<th>Post-contract risk assessment questionnaire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory and compliance</td>
<td>6.1</td>
<td>17.3</td>
<td>23.1</td>
</tr>
<tr>
<td>Strategic risk</td>
<td>1.7</td>
<td>1.9</td>
<td>5.1</td>
</tr>
<tr>
<td>Cybersecurity and privacy risk</td>
<td>26.8</td>
<td>57.9</td>
<td>72.5</td>
</tr>
<tr>
<td>Financial risk</td>
<td>2.6</td>
<td>4.0</td>
<td>15.9</td>
</tr>
<tr>
<td>Business continuity and resiliency</td>
<td>5.5</td>
<td>12.5</td>
<td>12.9</td>
</tr>
<tr>
<td>Geopolitical risk</td>
<td>1.0</td>
<td>1.1</td>
<td>1.8</td>
</tr>
<tr>
<td>Digital risk</td>
<td>1.6</td>
<td>4.2</td>
<td>16.4</td>
</tr>
<tr>
<td>Operational risk</td>
<td>3.2</td>
<td>6.5</td>
<td>27.1</td>
</tr>
<tr>
<td>Brand and reputational risk</td>
<td>1.9</td>
<td>2.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Sustainability risk</td>
<td>0.7</td>
<td>1.3</td>
<td>13.2</td>
</tr>
<tr>
<td>Total</td>
<td><strong>51.1</strong></td>
<td><strong>108.7</strong></td>
<td><strong>191.0</strong></td>
</tr>
</tbody>
</table>

Note: Average number of questions outlined are greater than 25.
Over the past two to three years, there has been a significant uptick in the proportion of firms using NIST, although ISO and COBIT have also seen increased usage by organizations. By using industry-proven and trusted frameworks such as NIST, the organizations surveyed feel comfortable with using such frameworks as a baseline.

**Risk assessment questionnaire framework**

**Q21. Which framework is used as a baseline for your risk assessment questionnaire?**

- National Institute of Standards and Technology (NIST): 18%
- Proprietary/institutional: 18%
- International Organization for Standardization (ISO): 17%
- Shared Assessments Program (Standard Information Gathering Questionnaire (SIG/SIG Lite)): 11%
- Unknown/uncertain: 11%
- Control Objectives for Information and Related Technologies (COBIT): 10%
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): 7%
- Other: 6%
- Health Information Trust Alliance (HiTRUST): 2%
About half of the organizations surveyed found System and Organization Controls (SOC) 2 or SOC 2+ an additional framework to be useful, consistent with previous results. Other frameworks (ISO, PCI, etc.) are seen to be moderately less useful; however, organizations still have not found any frameworks that have been entirely successful in reducing or eliminating the need to perform a risk/control assessment.

### Usefulness of tools/documentation in reducing/removing risk

**Q22.** On a 5-point scale, with 1 being not at all useful and 5 being extremely useful, how useful is each of the following in reducing or removing the need to perform a risk/control assessment on a third party?

<table>
<thead>
<tr>
<th>Tool/Documentation</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party data providers (e.g., SecurityScorecard, RapidRatings, BitSight)</td>
<td>24%</td>
<td>9%</td>
<td>19%</td>
<td>23%</td>
<td>18%</td>
</tr>
<tr>
<td>Payment Card Industry (PCI) certification</td>
<td>21%</td>
<td>9%</td>
<td>17%</td>
<td>24%</td>
<td>16%</td>
</tr>
<tr>
<td>ISO certification</td>
<td>11%</td>
<td>7%</td>
<td>21%</td>
<td>28%</td>
<td>23%</td>
</tr>
<tr>
<td>SOC 2+ (i.e., additional framework – NIST cyber framework, HITRUST)</td>
<td>18%</td>
<td>3%</td>
<td>10%</td>
<td>22%</td>
<td>24%</td>
</tr>
<tr>
<td>SOC 2 (security, availability, confidentiality, processing, integrity, privacy)</td>
<td>15%</td>
<td>2%</td>
<td>11%</td>
<td>23%</td>
<td>28%</td>
</tr>
<tr>
<td>SOC 1 or International Standard for Assurance Engagements 3402</td>
<td>16%</td>
<td>8%</td>
<td>24%</td>
<td>24%</td>
<td>18%</td>
</tr>
<tr>
<td>Third-party pre-completed SIG</td>
<td>28%</td>
<td>7%</td>
<td>17%</td>
<td>18%</td>
<td>19%</td>
</tr>
</tbody>
</table>

- **Not used**
- **1 — Not at all useful**
- **2 — Somewhat useful**
- **3 — Moderately useful**
- **4 — Very useful**
- **5 — Extremely useful**
Frequency of performing third-party risk assessments
Q23. How often does your organization reassess (risk/control assessment) your third parties based on risk posed to the organization?

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Every six months</th>
<th>One year</th>
<th>Two years</th>
<th>Three years or more</th>
<th>Not assessed</th>
<th>Unknown/uncertain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical risk</td>
<td>10%</td>
<td>76%</td>
<td>5%</td>
<td>6%</td>
<td>3%</td>
<td>0%</td>
</tr>
<tr>
<td>Highest risk</td>
<td>3%</td>
<td>52%</td>
<td>18%</td>
<td>7%</td>
<td>5%</td>
<td>14%</td>
</tr>
<tr>
<td>Second-highest risk</td>
<td>1%</td>
<td>22%</td>
<td>28%</td>
<td>19%</td>
<td>10%</td>
<td>20%</td>
</tr>
<tr>
<td>Third-highest risk</td>
<td>1%</td>
<td>15%</td>
<td>13%</td>
<td>30%</td>
<td>20%</td>
<td>22%</td>
</tr>
<tr>
<td>Remaining risk</td>
<td>1%</td>
<td>11%</td>
<td>6%</td>
<td>24%</td>
<td>35%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Note: Outlined percentages are responses greater than 25%
Issue management/risk treatment
Issue tracking
Q24. How are issues and exceptions stored and tracked?

Actions for issues
Q25. For third-party issues that you identify in each of the following risk tiers, what actions do you take?

For identified third-party issues in the critical-risk tier, termination and contractual changes are not uncommon outcomes, revealing that organizations use termination more often in the critical-risk tier than in the other tiers to resolve third-party issues despite the third party’s significance to the organization. Action severity has a direct correlation to inherent risk.
Termination of third parties due to issues

Q26. Over the past 12 months, how many third parties have been terminated because of issues identified?

Correlating to the data on actions taken after issue identification (Q25), the most common action is remediation or contractual changes, and the majority of the organizations surveyed indicated that no third parties have been terminated due to issue identification. The remaining nearly one-third of the organizations terminated only one to five third parties, which is a small percentage since more than 50% of the organizations surveyed have more than 100 third parties in a TPRM program (Q12).
Fourth-party management
Fourth-party data collection
Q27. Which fourth parties/subcontractors does your organization collect information on?

- Fourth parties supporting critical third-party services: 46%
- Fourth parties supporting any third-party services: 28%
- Unknown/uncertain: 17%
- Other: 9%

Fourth-party data collection methods
Q28. How is fourth-party information identified and collected (e.g., name, location, services provided)?

- Gathered during the risk/control assessment: 36%
- Captured within the inherent risk assessment: 26%
- Documented during the contracting phase: 25%
- Unknown/uncertain: 8%
- Other: 5%

The majority of survey respondents (56%) collect information only on fourth parties that support critical third-party services. Only one in three of the organizations collect information on all fourth parties. Typically, fourth-party information is gathered during the risk/control assessment process. It is likely that privacy and global inventory expectations will increase the collection of fourth-party data in years to come.
A meaningfully larger proportion of the organizations surveyed rely on contractual terms with their third parties for the purposes of overseeing/monitoring fourth parties. Increasingly, firms are also relying on contractual terms between the third and fourth party. Relatively few of the surveyed organizations (less than 20%) perform their own independent reviews of fourth parties.

### Fourth-party monitoring

**Q29. How does your organization assess/monitor fourth parties?**

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rely on contractual terms established with the third party</td>
<td>31%</td>
</tr>
<tr>
<td>Rely on the third party’s risk/control assessment of the fourth party</td>
<td>25%</td>
</tr>
<tr>
<td>Rely on contractual terms between the third party and the fourth-party organization</td>
<td>17%</td>
</tr>
<tr>
<td>Perform independent review of the fourth party</td>
<td>8%</td>
</tr>
<tr>
<td>Rely on the risk-monitoring activities performed by the relationship manager</td>
<td>7%</td>
</tr>
<tr>
<td>Fourth parties are identified but are not currently assessed or monitored</td>
<td>6%</td>
</tr>
<tr>
<td>Unknown/uncertain</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
Technology
The organizations surveyed indicated that no tool or manual effort is used for approximately one-third of all functions to manage risk. Archer, SAP Ariba and other methods are used more frequently for the functions. Respondents indicated that other tools are used as well, revealing that organizations are possibly using tools from smaller or bespoke providers.

Technology tools to manage risk

Q30. What technology/tools does your organization use for each of the following functions to manage risk?

<table>
<thead>
<tr>
<th>Function</th>
<th>No tool used (manual)</th>
<th>Archer®</th>
<th>Bwise®</th>
<th>Metric-Stream</th>
<th>SAP Ariba®</th>
<th>Hiperos®</th>
<th>Process Unity®</th>
<th>Prevalent®</th>
<th>Aravo</th>
<th>Service-Now</th>
<th>OneTrust</th>
<th>Lockpath</th>
<th>Proprietary</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcing</td>
<td>34%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>29%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>8%</td>
<td>19%</td>
</tr>
<tr>
<td>Inherent risk assessment</td>
<td>31%</td>
<td>19%</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>5%</td>
<td>6%</td>
<td>0%</td>
<td>2%</td>
<td>4%</td>
<td>1%</td>
<td>1%</td>
<td>14%</td>
<td>14%</td>
</tr>
<tr>
<td>Contract management</td>
<td>33%</td>
<td>5%</td>
<td>0%</td>
<td>1%</td>
<td>22%</td>
<td>2%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>12%</td>
<td>22%</td>
</tr>
<tr>
<td>Primary third-party inventory</td>
<td>32%</td>
<td>15%</td>
<td>0%</td>
<td>0%</td>
<td>12%</td>
<td>3%</td>
<td>3%</td>
<td>0%</td>
<td>1%</td>
<td>4%</td>
<td>1%</td>
<td>0%</td>
<td>11%</td>
<td>17%</td>
</tr>
<tr>
<td>Risk/control assessment facilitation</td>
<td>29%</td>
<td>17%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>5%</td>
<td>7%</td>
<td>0%</td>
<td>2%</td>
<td>5%</td>
<td>2%</td>
<td>1%</td>
<td>11%</td>
<td>18%</td>
</tr>
<tr>
<td>Issue management</td>
<td>28%</td>
<td>20%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
<td>5%</td>
<td>0%</td>
<td>2%</td>
<td>8%</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Note: Outlined percentages represent the top three technology/tools to manage risk per function.
Among the surveyed organizations that use tools/technology as part of their TPRM programs, few note that a technology platform is fully integrated within the organization. Of the organizations that do have a technology platform, they are actively incorporating external data into their systems via application program interfaces (APIs). There is an opportunity for technology integration and platform adoption to enhance today’s predominantly manual processes across TPRM as seen in the previous question (Q30).

Technology integration
Q31. How well integrated are the various tools your organization uses as part of your third-party risk management program/function?

![Integration Levels](chart)

- **42%** Not at all integrated; primarily manual reconciliations to enable the ability to report out of multiple systems
- **7%** Partially integrated; a mix of manual reconciliations and automated reporting
- **7%** Fully integrated; primarily automated reporting capabilities
- **42%** Don’t know/uncertain

Technology integration
Q32. If you have a third-party risk management technology platform, which active application program interfaces are configured to feed your third-party risk management technology platform to support ongoing monitoring activities?

- **43%** Not applicable (we do not have a third-party risk management technology platform)
- **17%** External threat intelligence (BitSight, SecurityScorecard, etc.)
- **17%** External supplier data (Dun & Bradstreet)
- **9%** External negative news
- **8%** Office of Foreign Assets Control/sanctions/AML
- **5%** External geopolitical data
Reporting
**Reporting for TPRM**

Q33. Which groups receive reporting for each of the following components of your third-party risk management program/function listed below?

<table>
<thead>
<tr>
<th>TPRM component</th>
<th>Board of directors</th>
<th>Senior management</th>
<th>Business management</th>
<th>Third-party relationship manager</th>
<th>No reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational metrics of the program</td>
<td>24%</td>
<td>48%</td>
<td>44%</td>
<td>36%</td>
<td>15%</td>
</tr>
<tr>
<td>KPIs/KRIs</td>
<td>22%</td>
<td>48%</td>
<td>43%</td>
<td>32%</td>
<td>15%</td>
</tr>
<tr>
<td>Third-party landscape</td>
<td>21%</td>
<td>43%</td>
<td>35%</td>
<td>28%</td>
<td>18%</td>
</tr>
<tr>
<td>Critical third parties</td>
<td>29%</td>
<td>54%</td>
<td>48%</td>
<td>33%</td>
<td>12%</td>
</tr>
<tr>
<td>Third parties with breaches or incidents</td>
<td>33%</td>
<td>60%</td>
<td>56%</td>
<td>40%</td>
<td>8%</td>
</tr>
<tr>
<td>Third parties with significant issues</td>
<td>24%</td>
<td>58%</td>
<td>58%</td>
<td>42%</td>
<td>9%</td>
</tr>
<tr>
<td>Third parties terminated prior to contract end date</td>
<td>11%</td>
<td>32%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Note: Outlined percentages are greater than 50%
Cybersecurity and threat intelligence
A significant number of the organizations surveyed have faced breaches or outages caused by third parties. Almost one in five organizations reported having at least three breaches, while nearly in one in three reported at least three outages.

Data breaches caused by third parties
Q34. Over the past two years, how many data breaches or losses have been caused by third parties?

Outages caused by third parties
Q35. Over the past two years, how many outages have been caused by third parties?
Despite the significant number of the organizations surveyed that have suffered a breach, nearly half of them do not utilize threat intelligence tools. This may be driven by the fact that only half found threat intelligence tools to be very useful at driving risk-based ongoing oversight activity, showing a low degree of valuable integration with threat intelligence tools.

Threat intelligence

Q36. Does your organization utilize threat intelligence products or services to continuously monitor the cybersecurity environment of your third-party providers?

- Yes, internally developed products or services: 41%
- Yes, externally developed products or services: 23%
- No: 36%

Q37. [For those who answered Yes] On a scale of 1 to 5, with 1 being not at all useful and 5 being extremely useful, how useful are threat intelligence tools at driving risk-based ongoing oversight activity?

- 5 — Extremely useful: 15%
- 4 — Very useful: 28%
- 3 — Moderately useful: 25%
- 2 — Somewhat useful: 13%
- 1 — Not at all useful: 2%
- Unknown/uncertain: 16%
Inbound requests
Inbound requests for TPRM

Q38. Approximately how many inbound requests for completion of third-party risk assessment questionnaires does your organization receive annually?

- Fewer than 50: 31%
- 51 to 100: 10%
- 101 to 150: 5%
- 151 to 200: 5%
- 201 to 250: 0%
- More than 251: 13%
- Not applicable—we do not receive inbound request for completion of third-party risk assessments: 9%
- Unknown/uncertain/not tracked: 26%

On-site vs. remote reviews

Q39. What percentage of inbound requests are on-site third-party reviews vs. remote reviews? Please provide percentages for each; total must equal 100%.

- Remote: 79%
- On-site: 21%

A third of the organizations surveyed facilitate more than 50 inbound assessments per year, and an additional quarter of participants don’t even know if they are being assessed, showing a disconnect between inbound request management and internal risk management functions.
When it comes to inbound requests, more than half of the organizations surveyed noted that resource constraints presented a significant challenge. This is in alignment with organizations, indicating that they plan to use more internal resources for TPRM execution in next two to three years (Q7).

Difficulty related to inbound TPRM

Q40. On a 5-point scale, with 1 representing no difficulty and 5 representing significant difficulty, what degree of difficulty does your organization face in addressing each of the following related to inbound third-party risk management?

- Responsibilities and the required knowledge and skills: 2.74
- Capacity of resources: 3.43
- Policies, procedures and guidelines: 2.50
- Understanding of services provided to customers: 2.53
- Clarity of customer requests: 2.65
- Development of standard responses to customer: 2.82
- Tracking of customer requests and feedback: 2.64
Privacy regulations
Privacy regulations in TPRM

Q41. On a scale of 1–5, how difficult will it be to address the expectations of the guidance specific to the privacy laws (e.g., GDPR, CCPA) as they relate to your third-party population?

Provide timely disclosures to consumers regarding personal information that is being collected and the purposes for which that data is being used

Provide consumers the right to opt out of the sale of their personal information through easily accessible and transparent means

Comply with consumer requests to delete personal information about the consumer that has been collected, inclusive of data shared with third-party service providers

If requested, provide consumers with categories of personal information collected, the sources from which information was collected, the purpose of collecting the information, and third parties with whom the information is shared

Average

2.74

2.67

3.12

3.11

Privacy regulations in TPRM

Organizations are not yet fully prepared to address all aspects of recent privacy regulations (CCPA, GDPR, etc.). In particular, the organizations surveyed feel it will prove challenging to provide customers the right to opt out of the sale of their personal information and provide timely disclosures regarding the information that they are collecting and how it will be used.
Regulatory and internal audit exams
As with previous years, oversight and governance was the dominant area of focus among the organizations surveyed, with cybersecurity following in both areas and enterprise-critical third parties following for regulatory body and onboarding activities following for internal audit.

Areas of focus during regulatory body review and internal audit

Q42. During your organization’s most recent regulatory body review and most recent internal audit of your third-party risk management program/function, what were the two to three most important areas of focus? Please select no more than three.

<table>
<thead>
<tr>
<th>Important areas of focus</th>
<th>Regulatory body review</th>
<th>Internal audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight and governance</td>
<td>72</td>
<td>94</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>45</td>
<td>56</td>
</tr>
<tr>
<td>Enterprise-critical third parties</td>
<td>33</td>
<td>27</td>
</tr>
<tr>
<td>Third-party assessments —information security and business continuity</td>
<td>29</td>
<td>36</td>
</tr>
<tr>
<td>Inherent risk assessment</td>
<td>25</td>
<td>39</td>
</tr>
<tr>
<td>Fourth-party oversight and governance</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>Privacy/confidentiality</td>
<td>16</td>
<td>23</td>
</tr>
<tr>
<td>Issue management and/or risk acceptance</td>
<td>15</td>
<td>29</td>
</tr>
<tr>
<td>Onboarding activities</td>
<td>14</td>
<td>45</td>
</tr>
<tr>
<td>Third-party assessments —compliance</td>
<td>13</td>
<td>25</td>
</tr>
<tr>
<td>Operating models</td>
<td>12</td>
<td>19</td>
</tr>
<tr>
<td>Maintenance of third-party inventory</td>
<td>10</td>
<td>23</td>
</tr>
<tr>
<td>Foreign-based third parties</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Nontraditional third parties (i.e., brokers, agents, financial intermediaries)</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Third-party assessments —performance</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>Consumer protection/compliance</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Residual risk model</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Not applicable</td>
<td>52</td>
<td>39</td>
</tr>
</tbody>
</table>
Nontraditional third parties
Nontraditional third parties
Q43. For each of the following types of nontraditional third parties, are the third parties covered by your third-party risk management program/function?

<table>
<thead>
<tr>
<th>Nontraditional third parties*</th>
<th>Strategic partnerships</th>
<th>Law firms providing outside legal counsel (litigation)</th>
<th>Insurance carriers</th>
<th>Joint ventures</th>
<th>Pension plans</th>
<th>Landlord premises</th>
<th>Broker dealers</th>
<th>Charitable organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered by TPRM</td>
<td>29%</td>
<td>29%</td>
<td>29%</td>
<td>38%</td>
<td>40%</td>
<td>51%</td>
<td>35%</td>
<td>46%</td>
</tr>
<tr>
<td>Covered by specialized program</td>
<td>15%</td>
<td>22%</td>
<td>20%</td>
<td>19%</td>
<td>14%</td>
<td>20%</td>
<td>22%</td>
<td>23%</td>
</tr>
<tr>
<td>Not covered</td>
<td>56%</td>
<td>49%</td>
<td>51%</td>
<td>42%</td>
<td>46%</td>
<td>29%</td>
<td>43%</td>
<td>31%</td>
</tr>
</tbody>
</table>

* Results shown for the most common nontraditional third parties based on survey results.

Of the organizations surveyed, the most likely nontraditional third parties to be covered by TPRM are strategic partnerships, insurance carriers and law firms providing outside legal counsel. The most likely not to be covered by TPRM are landlord premises, charitable organizations and pension plans.
Concentration risks
(financial services only)
About half of the organizations surveyed find it relatively easy to report on concentration of spend and third-party concentration, but far fewer find it easy to report on fourth-party or reverse concentration.

Financial services concentration risk
Q45. [Financial services firms only] On a scale of 1–5, what is your organization’s ability to report on each type of concentration risk, with 1 being not at all and 5 being extremely well?

- Third-party concentration (i.e., widespread use of a third party across the enterprise): 3.37
- Concentration of spend: 3.49
- Concentration of a specific service (i.e., organization is dependent on a third party for a significant portion of an internal process/function): 3.26
- Geographic concentration: 3.18
- Fourth-party concentration (i.e., a significant portion of the service is performed by a fourth party): 2.00
- Reverse concentration (i.e., an organization comprises a significant amount of business to the service provider): 2.20
Affiliate management (financial services only)
Twenty-eight percent of the organizations surveyed have intercompany affiliates that are in scope for their TPRM programs. Of those, 61% maintain those intercompany affiliates as part of their golden-source inventory.

Q46. Are intercompany affiliates providing goods/services to your organization’s US operating unit in scope for third-party risk management?

- Yes: 28%
- No: 44%
- Unknown/uncertain: 29%

Q47. [If Yes] Are intercompany affiliates included in the golden-source third-party inventory or maintained separately?

- Maintained in golden-source inventory: 61%
- Maintained separately/outside of golden-source inventory (e.g., with legal, separate groups): 26%
- Unknown/uncertain: 13%
For those organizations surveyed that have intercompany affiliates that are in-scope for their TPRM programs, 55% say that the process is the same for assessing them. For those organizations that have a different process, most are leveraging internal audit reviews or other control testing, suggesting that there are ways to rightsize affiliate management without additional assessment efforts.

Intercompany affiliates assessment process
Q48. Is your process for assessing internal affiliates the same as your third-party risk management process?

Q49. [If No] How is the process different for intercompany affiliates?

- 54% leverage internal audit reviews or other control testing performed
- 25% no assessment or monitoring activities
- 13% no defined process for assessing affiliates
- 8% other
Affiliate monitoring requirements seem to vary greatly, without consensus on even the basic activities like service-level monitoring.

Intercompany monitoring requirements
Q50. Which of the following ongoing monitoring requirements apply to intercompany affiliates providing goods/services to your organization?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service-level agreement monitoring</td>
<td>19%</td>
</tr>
<tr>
<td>Ongoing control assessments at scheduled intervals (e.g., annual, biannual)</td>
<td>16%</td>
</tr>
<tr>
<td>Review of internal audit reports</td>
<td>15%</td>
</tr>
<tr>
<td>Scorecards</td>
<td>11%</td>
</tr>
<tr>
<td>Review of business operations reporting, including loss events</td>
<td>10%</td>
</tr>
<tr>
<td>Review of regulatory reports</td>
<td>9%</td>
</tr>
<tr>
<td>Review of business executive reporting</td>
<td>8%</td>
</tr>
<tr>
<td>Quarterly business reviews</td>
<td>6%</td>
</tr>
<tr>
<td>Unknown/uncertain</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
Innovation
### Emerging technologies for TPRM

**Q51. A.** Does your organization currently use any of the following emerging technologies to support your third-party risk management program/function?

**B.** If not, does your organization plan to begin using any of the following in the next two to three years?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Currently use</th>
<th>Plan to use</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain</td>
<td>3%</td>
<td>16%</td>
<td>81%</td>
</tr>
<tr>
<td>Advanced analytics</td>
<td>8%</td>
<td>29%</td>
<td>63%</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>13%</td>
<td>19%</td>
<td>69%</td>
</tr>
<tr>
<td>Robotics</td>
<td>19%</td>
<td>20%</td>
<td>63%</td>
</tr>
</tbody>
</table>

Just one in five organizations surveyed are using advanced analytics, and even fewer are using artificial intelligence (AI), robotics or blockchain. However, many more organizations recognize the benefits that such technology can provide. More than one in three expect to start using advanced analytics in the next two to three years, and almost one in three plan to use AI.
Areas of investment
To better leverage the technology they have, and stay ahead of the curve when it comes to emerging technologies, most organizations surveyed plan to increase their spending on technology, supporting their TPRM programs and advanced analytics. Advanced analytics is the most common emerging technology currently used (Q51), and 50% of organizations plan to spend more in the future. Eighty-five percent of the organizations will maintain spend or increase spend for third-party risk management processes.

Time investment in activities

Q52. Compared with the current year, does your organization plan to spend more, less or the same amount for the following activities?

- Advanced analytics and reporting
- Third-party risk management program/function technology
- Third-party risk management process
- Policies and standards
- Risk models
- Third-party inventory
- Governance and oversight

Unknown/uncertain  | Spend less | Spend more | Spend will not change
---|---|---|---
Advanced analytics and reporting | 19% | 0% | 50% | 31%
Third-party risk management program/function technology | 17% | 3% | 51% | 30%
Third-party risk management process | 14% | 2% | 50% | 35%
Policies and standards | 14% | 3% | 28% | 55%
Risk models | 20% | 2% | 33% | 46%
Third-party inventory | 17% | 3% | 35% | 45%
Governance and oversight | 16% | 2% | 41% | 42%
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2020 EYGM Limited
All Rights Reserved.

002185-20Gbl
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

Global

Amy Brachio
EY Global Advisory Risk and Performance Improvement Leader
amy.brachio@ey.com
Tel: +1 612 371 8537

Nitin Bhatt
EY Global Advisory Risk Transformation Leader
Email: nitin.bhatt@in.ey.com
Tel: +91 80 6727 5127

Americas

Matthew Moog
EY Global Financial Services TPRM Leader
matthew.moog@ey.com
+1 201 551 5030

Vignesh Veerasamy
EY Global and Americas TPRM Leader
vignesh.veerasamy@ey.com
+1 415 425 3993

Michael Giarrusso
Americas TPRM Financial Services Leader
michael.giarrusso@ey.com
+1 617 585 0395

Asia-Pacific

Chris Lim
APAC Financial Services TPRM Leader
chris.lim@sg.ey.com
+65 6309 6320

Steven Xiong
APAC Risk Transformation Leader
steven.xiong@ch.ey.com
+862122282688

Oceania

Hanny Hassan
Oceania Financial Services TPRM Leader
nanny.hassan@au.ey.com
+61 2 9248 4141

Heidi Riddell
APAC and Oceania Risk Leader
heidi.riddell@au.ey.com
+61 2 9248 4569

Europe, Middle East, India and Africa (EMEIA)

Kanika Seth
EMEIA Financial Services TPRM Leader
kseth@uk.ey.com
+44 20 7951 7469

Netta Nyholm
EMEIA TPRM Leader
netta.nyholm@de.ey.com
+49 221 2779 16427