ECI Compliance Week

The State of Third-Party Risk & Integrity

Key Findings

Survey report · October 2026

In partnership with

Diligent

About This Report

Third-party risk has outgrown the checklist. Sanctions shift overnight, ownership structures blur, and AI is now both a tool in the due-diligence process and a risk that vendors may introduce. For many organizations, third parties account for a significant share of compliance risk, making the effectiveness of these programs critical.

This flagship survey and report, *The State of Third-Party Risk & Integrity*, is a joint initiative by ECI Compliance Week and Diligent. We asked ethics, compliance, and risk practitioners how they are actually handling third-party risk: what's working, what's slowing programs down, and where teams are investing next.

The report benchmarks how peer programs scope and risk-rank third parties and what triggers enhanced due diligence. It also covers review volumes, turnaround times, common causes of delay, and annual TPRM spend, as well as which risk areas most often lead to mitigation or a decision not to proceed. Finally, it shows where AI is being used in due diligence and how organizations govern their vendors' own use of AI.

In This Report

1. Program Scope and Design 5
2. Reviews and Risk Coverage 8
3. Maturity, Oversight, and AI 16
4. Key Takeaways 23
5. Methodology 24

Key Findings

At a Glance

Material findings

37%

say at least 5% of their reviews in the past year produced a material finding

See p. 8

Program scope

69%

conduct due diligence on all or most categories of third parties

See p. 5

Risk-based approach

90%

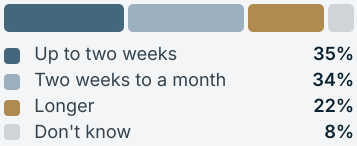
follow a risk-based approach, giving some third parties more extensive review

See p. 5

Time to clear

70%

clear a new third party within a month



See p. 11

Causes of delay

81%

name waiting on the third party for information as a top cause of delay

See p. 12

Fourth-party visibility

25%

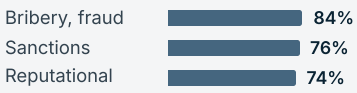
have little or no visibility into their third parties' own subcontractors

See p. 19

Risk areas reviewed

84%

include bribery, corruption, and fraud in third-party reviews



See p. 14

Program maturity

32%

rate their program as standardized, the midpoint of the five-level scale



See p. 16

AI in due diligence

55%

use AI in at least one part of their due-diligence process

See p. 20

Key Findings in Detail

1. **Due diligence programs are broad and risk-based.** Sixty-nine percent of organizations conduct due diligence on all or most relevant categories of third parties, 28% cover selected categories or circumstances, and 90% give some third parties more extensive review than others.

2. **Reviews find issues at a low rate, and findings lead to mitigation far more often than to exit.** Thirty-seven percent of respondents say at least 5% of their reviews in the past year produced a material finding, and only 10% say none did. When a finding arises, the most common responses are enhanced due diligence (71%) and required remediation or contractual protections (53%), and 32% count ending the relationship among their most common responses; across all reviews, 67% say none or fewer than 1% ended in a decision not to proceed.

3. **The third party is the main source of delay.** Eighty-one percent name waiting for information from the third party as a top cause of delay in completing reviews, more than double the share naming the next most common cause, waiting for the internal business sponsor (34%).

4. **Most new third parties are cleared within a month.** Seventy percent of organizations clear a new third party within a month, with 35% clearing within two weeks. Twenty-two percent take longer than 30 days to clear a new third party.

5. **Risk reviews remain focused on traditional ABAC risks.** Bribery, corruption, and fraud are the risks most often reviewed (84%), and the risk topics most often leading to enhanced due diligence, mitigation, or a decision not to proceed (51%). Sanctions (76%) and reputational risk (74%) are reviewed next most often, and sanctions rank second as a driver of action. AML and financial crime, privacy, cyber, financial health, modern slavery and human trafficking, and foreign terrorist organizations are also reviewed by at least half of respondents.

6. **Visibility beyond direct third parties (fourth parties) is limited.** Six percent formally manage material fourth-party risks, while 25% have little or no visibility into fourth parties.

7. **Program maturity sits in the middle of the scale.** Ratings split almost evenly either side of standardized (32%): 33% rate their program as integrated or optimized and 30% as ad hoc or foundational. Only 18% set improvement goals and evaluate their success.

8. **AI is entering due diligence.** Fifty-five percent use AI in at least one due-diligence activity, and 38% track how their third parties use or govern AI.

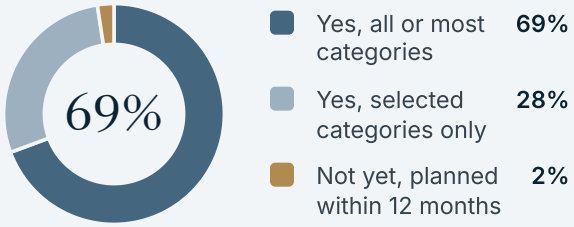
Part 1

Program Scope and Design

Sixty-nine percent of organizations conduct due diligence on all or most categories of third parties, and 90% follow a risk-based approach, giving some third parties more extensive due diligence than others.

Conducts Third-Party Due Diligence

% of respondents



Follows a Risk-Based Approach

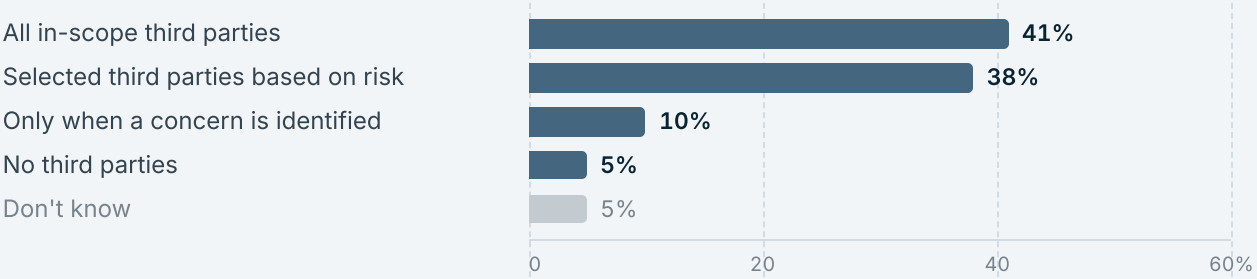
% of respondents



Taken together, all but 2% of the organizations surveyed already conduct third-party due diligence in some form, and those 2% plan to begin within 12 months.

Screening of Beneficial Owners and Key Individuals

% of respondents

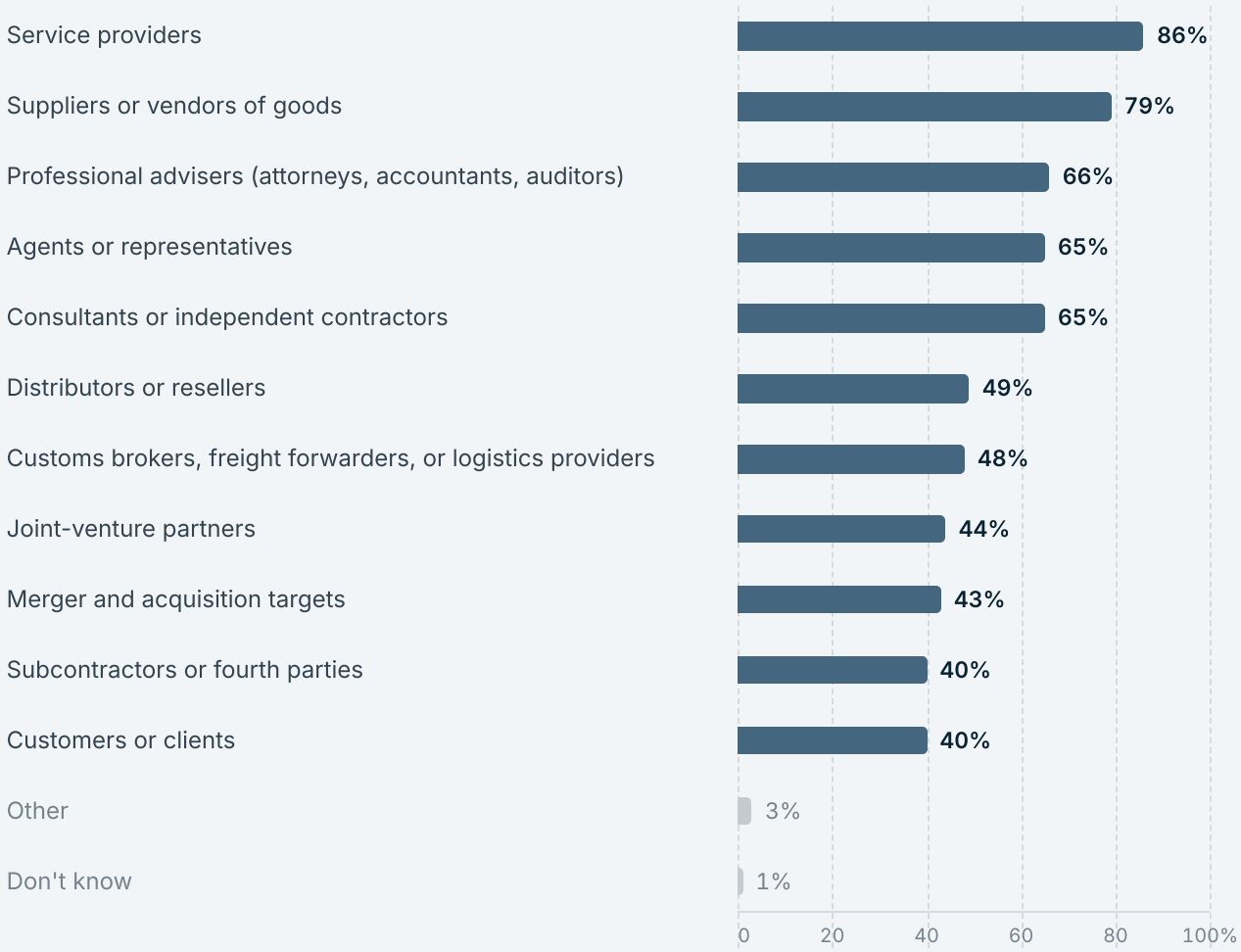


Most programs identify and screen beneficial owners and other higher-risk individuals either broadly or on a risk basis: 79% do so for all in-scope third parties or for those selected on risk. Ten percent screen only when a concern is identified, and 5% screen no third parties.

A broad range of third parties are included in the due-diligence process. Five categories, from service providers (86%) and suppliers of goods (79%) down to consultants, are each covered by at least 65% of programs.

Third-Party Categories Covered by the Due-Diligence Program

% of respondents



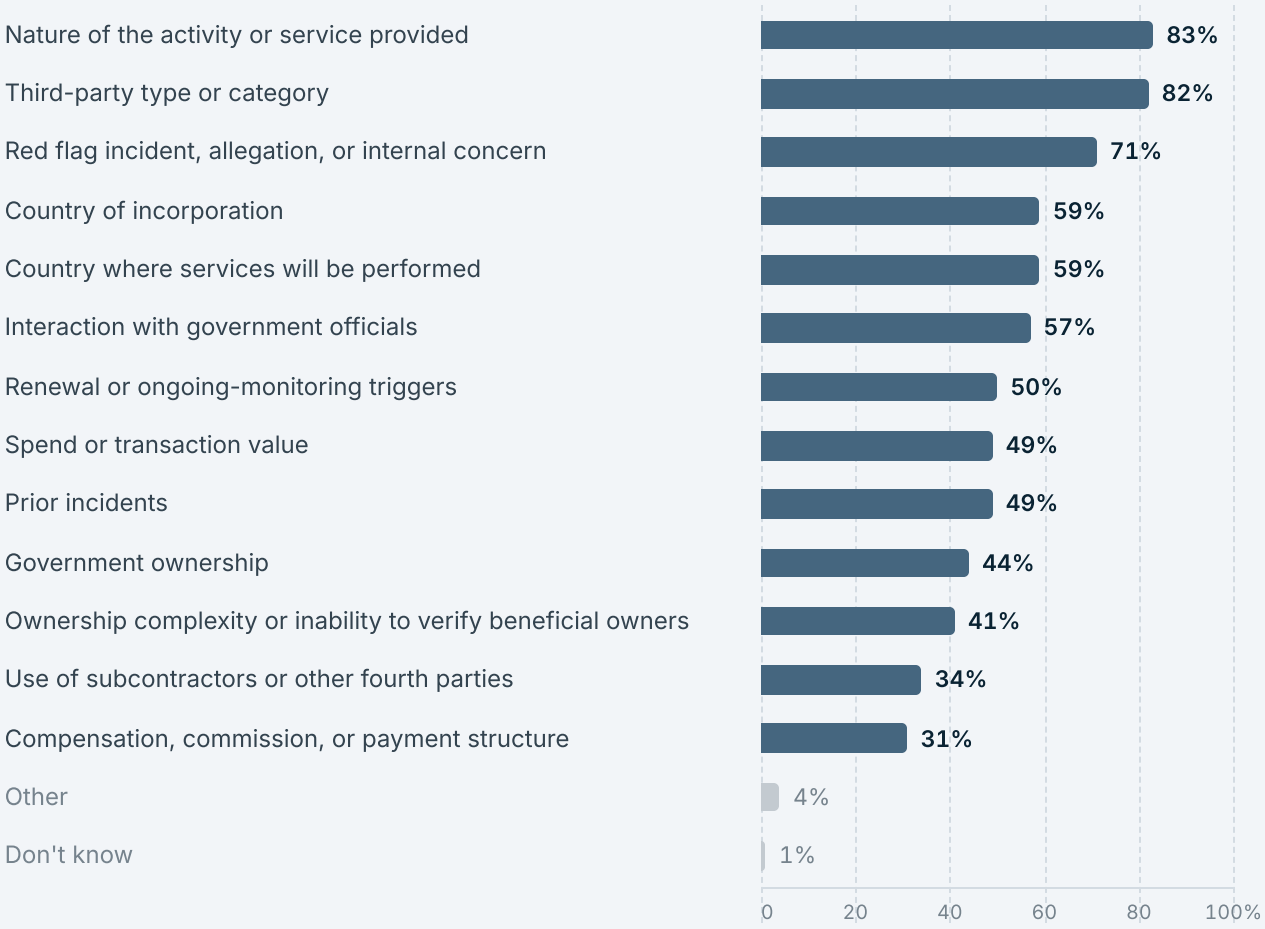
Note: Select all that apply; percentages total more than 100%.

The remaining six categories, from distributors to customers, are each covered by 40% to 49% of programs. Customers or clients and subcontractors or fourth parties (40% each) are the least commonly covered, a gap that reappears later in the report in the findings on fourth-party visibility.

Among organizations with a risk-based approach, the nature of the activity or service (83%) and the type of third party (82%) most often trigger enhanced due diligence, followed by red flags or internal concerns (71%). Ownership complexity (41%) is a less frequent trigger.

Factors That Trigger Enhanced Due Diligence

% of respondents



Note: Select all that apply; asked of those with a risk-based approach; percentages total more than 100%.

Geography also frequently triggers enhanced due diligence. The country of incorporation and the country where services will be performed are each cited as triggers by 59% of organizations, and interaction with government officials is cited by 57%. Commercial characteristics of the engagement rank lower. Spend or transaction value is a factor for 49%, and compensation, commission, or payment structure for 31%. The use of subcontractors or other fourth parties warrants enhanced due diligence for about a third (34%) of organizations.

Part 2

Reviews and Risk Coverage

Review Volume, Findings, and Decisions

Fifty-six percent of respondents completed 100 or more due-diligence reviews in the past 12 months, including 20% who completed 1,000 or more, and more than a third (37%) say at least 5% of their reviews produced a material finding.



Review volumes vary widely: 59% of organizations completed fewer than 500 third-party reviews in the past 12 months. Most organizations encounter material findings, which require additional investigation, mitigation, or approval; only 10% report none.

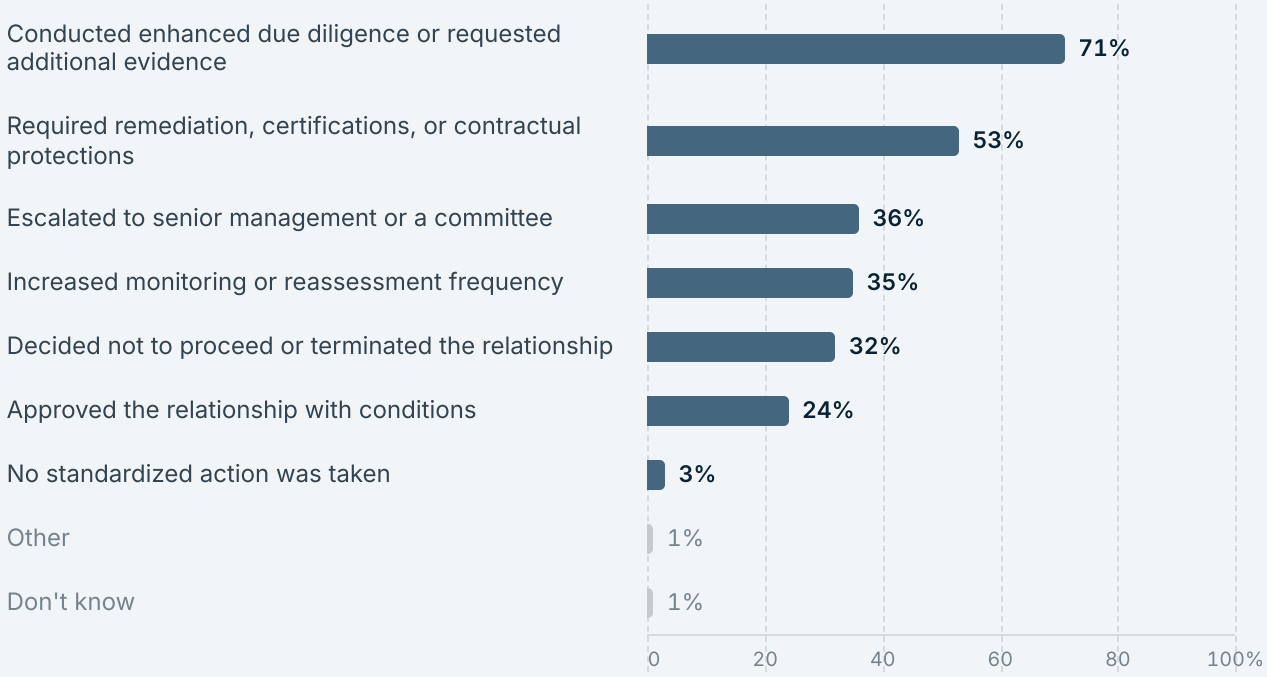
Insight

The relatively low incidence of material findings raises an important question about the effectiveness of third-party due diligence. While 56% of respondents report material findings in fewer than 5% of reviews, it is difficult to determine whether this reflects effective risk selection, lower-risk third-party populations, or limitations in the diligence process itself.

More findings do not necessarily indicate better due diligence. However, as organizations confront increasingly complex third-party risks and expanding compliance obligations, they should consider whether existing approaches are consistently identifying the issues that matter most.

Most Common Actions When a Material Finding Is Identified

% of respondents

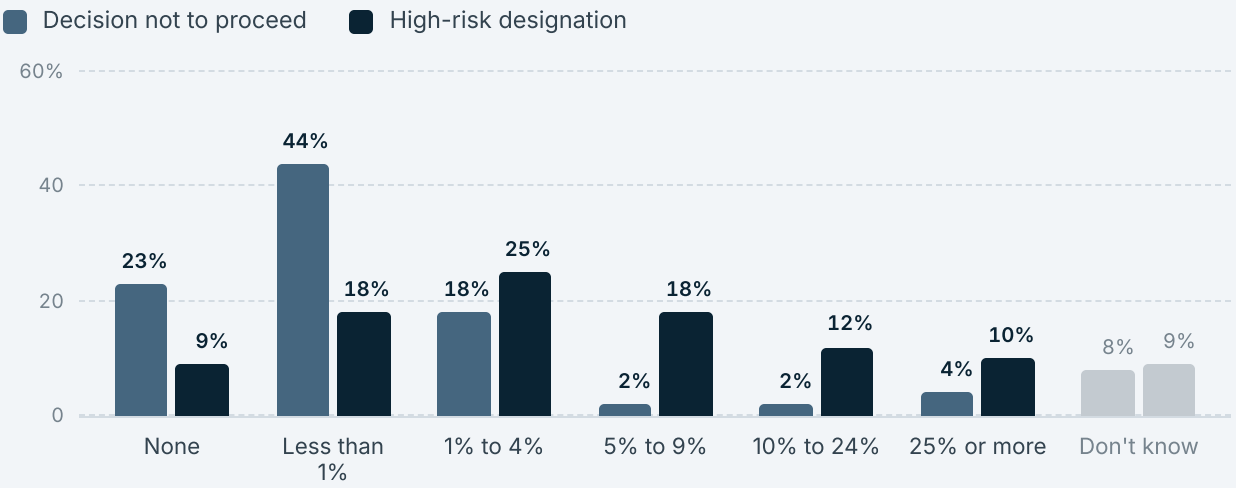


Note: Respondents could select up to three; asked of those reporting material findings; percentages total more than 100%.

When a material finding does arise, enhanced due diligence and required remediation, certifications, or contractual protections are the most common responses, and **32% count deciding not to proceed or ending the relationship** among them.

Share of Reviews Ending in a Decision Not to Proceed or a High-Risk Designation

% of respondents



Asked what share of all their reviews ended in a decision not to proceed, 67% of respondents say none or fewer than 1%, and 6% say 10% or more. That does not conflict with the 32% above, which counts organizations that list ending the relationship among their most common responses to a finding; this chart is a share of all reviews, most of which produce no finding. High-risk designations are far more common: 22% say 10% or more of their reviews resulted in one. A finding usually leads to a high-risk rating and closer handling rather than to the end of the relationship.

Insight

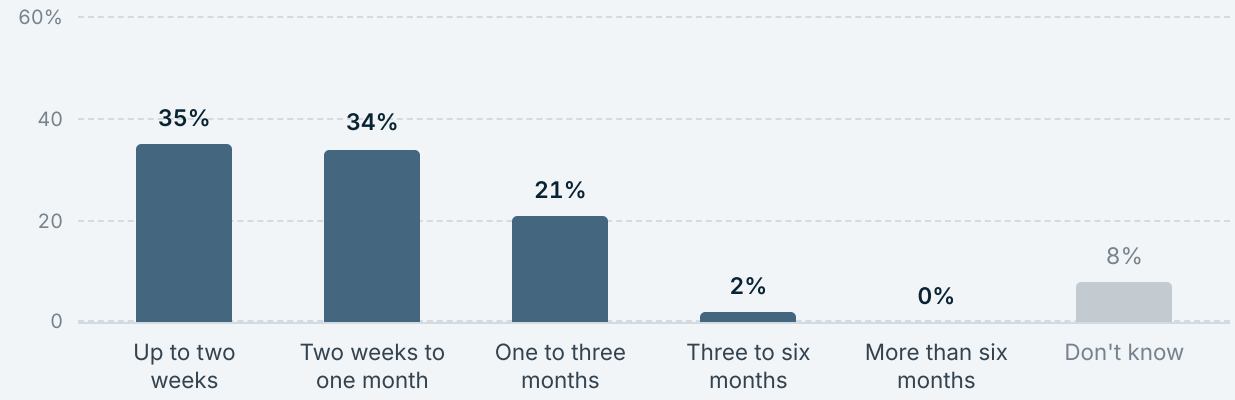
Material findings may not emerge from every review, but their frequency reinforces the value of third-party due diligence. Around a third of respondents uncover material findings in more than 5% of reviews, demonstrating that diligence is identifying significant risks that could otherwise remain hidden. The goal is not simply to generate more findings.

Effective programs identify the issues that matter, understand their significance, and use that insight to inform decisions and mitigation. As third-party risks become more complex and interconnected, organizations should continue testing whether their diligence approach is sufficiently targeted and robust to uncover material exposures before they become bigger problems.

Efficiency and Resources

Average Time to Clear a New Third Party to Conduct Business

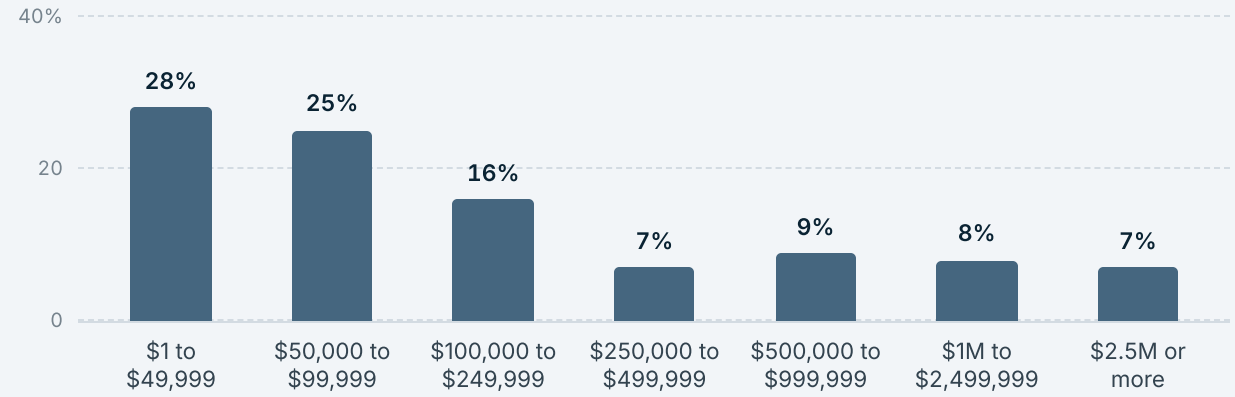
% of respondents



Most organizations clear a new third party to conduct business within a month (70%). **Twenty-two percent take longer than 30 days**, but long clearance times are rare: 2% take three to six months, and no respondent reported taking longer than six months.

Annual TPRM Spending, Excluding Personnel (US$)

% of respondents who gave an estimate



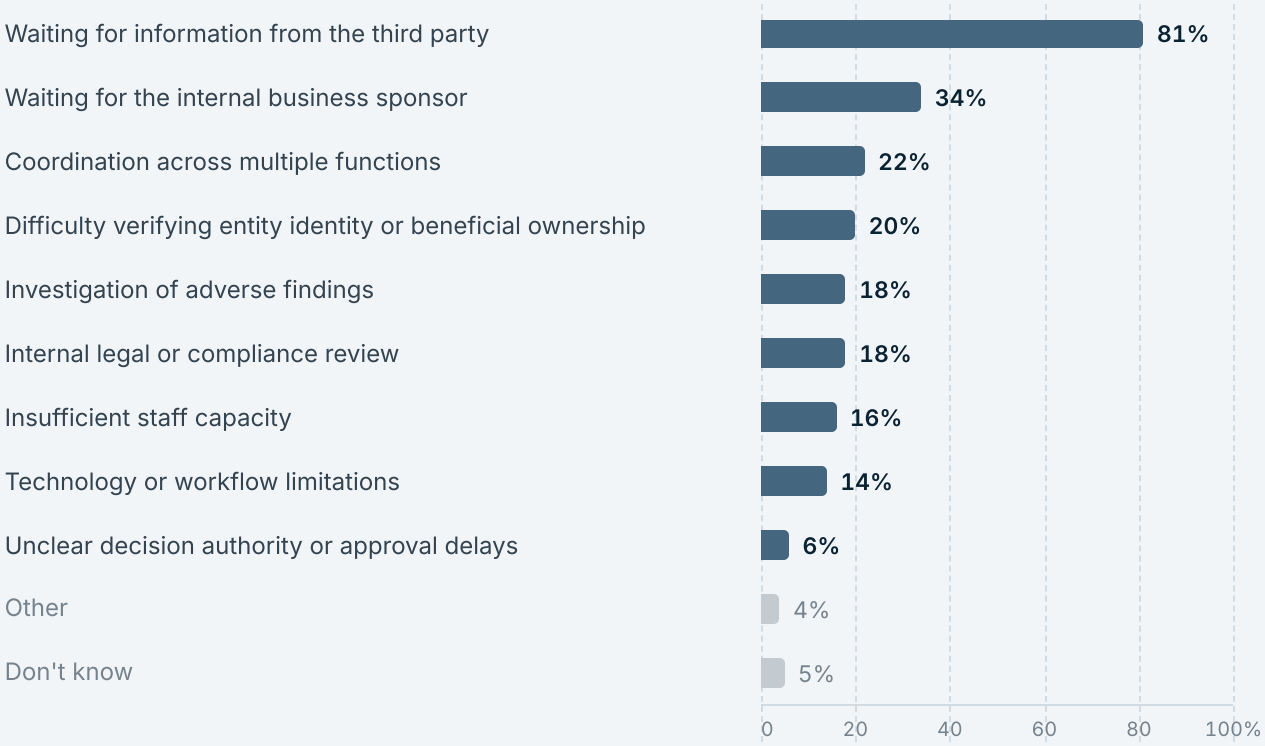
Note: Excludes the 24% who did not know.

Spending clusters at the low end. Among respondents who know their organization's spend, 53% spend less than $100,000 a year and **69% less than $250,000**, while 24% spend $500,000 or more.

Waiting for information from the third party is the most common cause of delay, cited by 81% of respondents.

Most Common Causes of Delay

% of respondents



Note: Respondents could select up to three; percentages total more than 100%.

After waiting on the third party, the next most common cause is waiting for the internal business sponsor (34%). Insufficient staff capacity (16%), technology or workflow limitations (14%), and unclear decision authority or approval delays (6%) are named least often.

Insight

The fact that 81% of respondents identify waiting for third-party information as a leading cause of delay raises questions about the efficiency of traditional due-diligence processes. Many programs rely heavily on requesting information directly from third parties, often through lengthy assessments and supporting documentation. While these requests remain necessary for certain types of information, they can create substantial delays and administrative burden.

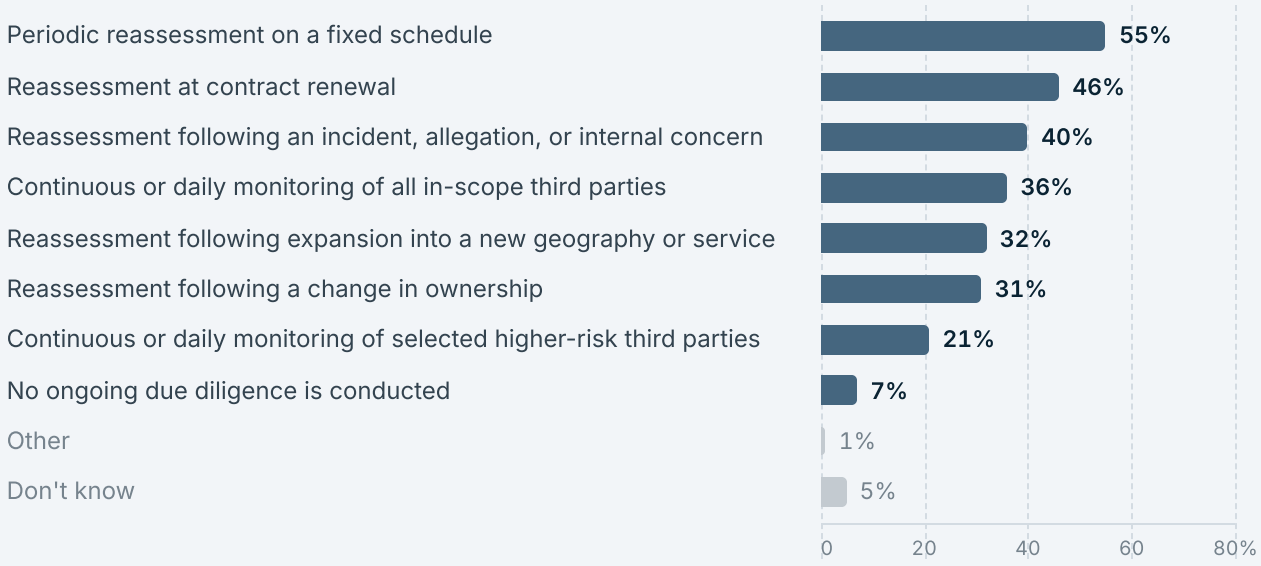
Organizations should consider whether more information could be independently obtained, verified, or continuously monitored, reserving direct information requests for evidence that cannot otherwise be established. The opportunity is not simply to accelerate existing processes, but to rethink how reliable risk intelligence is obtained, validated, and used to support decisions.

Ongoing Due Diligence

Periodic reassessment on a fixed schedule is the most common form of ongoing due diligence (55%), followed by reassessment at contract renewal (46%).

Ongoing Due Diligence After Onboarding

% of respondents



Note: Select all that apply; percentages total more than 100%.

Fifty percent continuously monitor all or selected third parties, and 7% conduct no ongoing due diligence.

Event-driven reassessment is widespread alongside scheduled reviews: contract renewal (46%), an incident or allegation (40%), expansion into a new geography or service (32%), and a change in ownership (31%). Each prompts a fresh look for a sizeable share of programs. Continuous monitoring of all in-scope third parties (36%) is more common than monitoring confined to selected higher-risk third parties (21%).

Insight

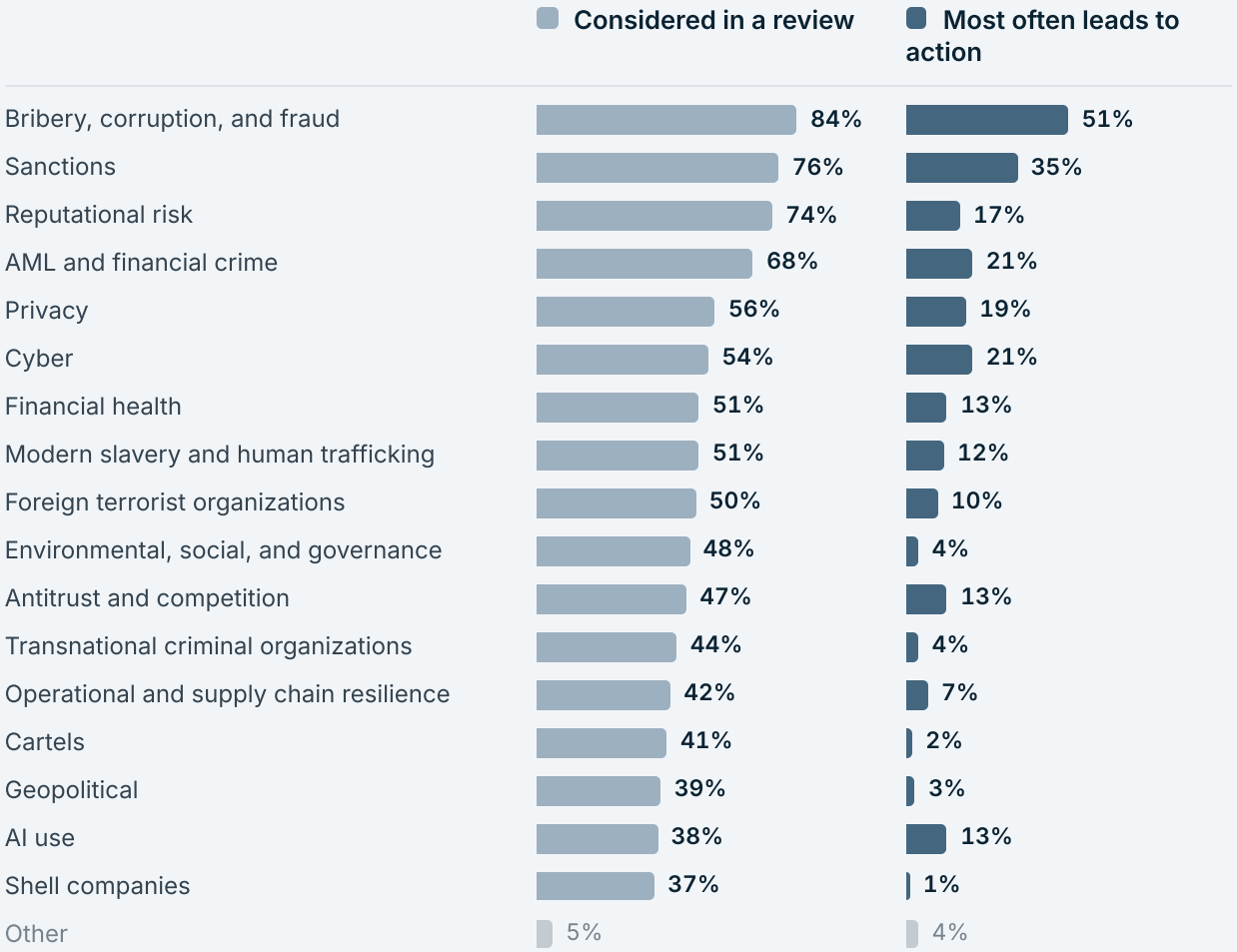
Ongoing due diligence is now the norm, but it is mostly calendar-driven. Fifty-five percent of respondents reassess relationships on a fixed schedule and 46% at contract renewal, while half monitor continuously, whether all in-scope third parties or a higher-risk subset. Combining periodic assessments with event-driven monitoring helps organizations identify significant developments sooner and trigger timely investigation, escalation, and action.

Third-Party Risk Coverage Areas

Bribery, corruption, and fraud are the risk areas most often reviewed and most often cited as leading to action, followed by sanctions, but nine of the 17 risk areas are reviewed by at least half of programs.

Risk Areas Reviewed, and Those That Most Often Lead to Action

% of respondents

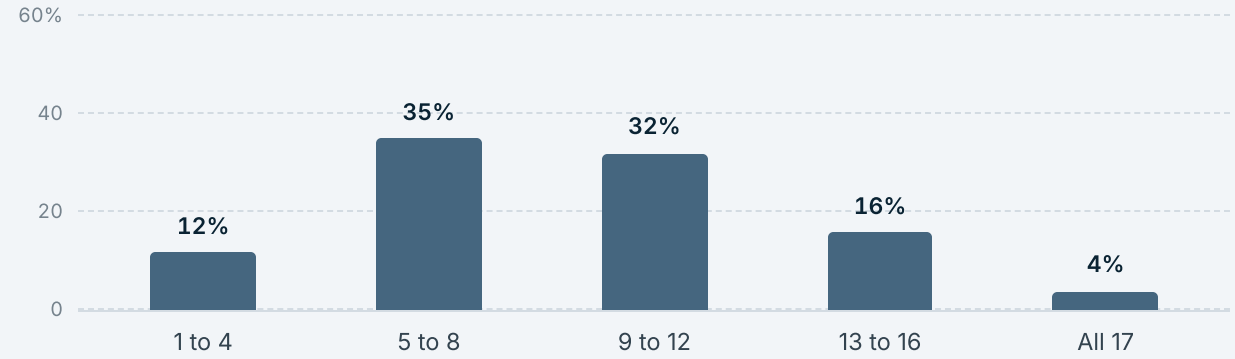


Note: Considered in a review: select all that apply. Leads to action (enhanced due diligence, mitigation, or a decision not to proceed): up to three. Percentages total more than 100%.

Reputational risk is reviewed almost as often as sanctions (74% compared with 76%) but is named as a driver of action by only 17%. **AI use is reviewed by 38% of organizations** and named as a driver of action by 13%.

Number of the 17 Risk Areas Each Organization Reviews

% of respondents



Note: Counts the 17 listed areas, excluding “Other.”.

Coverage is broad within individual programs, not only across the sample as a whole. The median organization reviews nine of the 17 risk areas listed, 53% review nine or more, and only 12% review four or fewer.

Insight

The breadth of risks included in third-party due diligence does not necessarily reflect the weight they receive. Bribery, corruption, fraud, and sanctions remain dominant, while areas such as operational resilience and modern slavery are considerably less likely to trigger action. That may reflect legitimate differences in exposure across industries, geographies, and relationships. But as third-party risks become more interconnected, organizations may need to reconsider not simply which risks they assess, but the depth of scrutiny each receives. Effective coverage means concentrating attention where potential impact is greatest, rather than treating established compliance risks as the default priority.

Part 3

Maturity, Oversight, and AI

Program Maturity and Effectiveness

Self-ratings of program maturity split almost evenly around the middle of the scale: a third rate their program as integrated or optimized, a third as standardized, and three in ten as ad hoc or foundational.

Self-Rated Maturity of the TPRM Program

% of respondents

1	**Ad hoc**	Reviews are primarily reactive, manual, or inconsistently applied.	9%
2	**Foundational**	Written expectations and basic screening are in place, but coverage and execution remain uneven.	21%
3	**Standardized**	Risk-based processes, defined escalation, and repeatable controls are consistently applied.	32%
4	**Integrated**	Workflow, data, monitoring, and decision-making are connected across functions.	25%
5	**Optimized**	Monitoring, analytics, testing, and measurable outcomes are used to improve effectiveness and efficiency.	8%

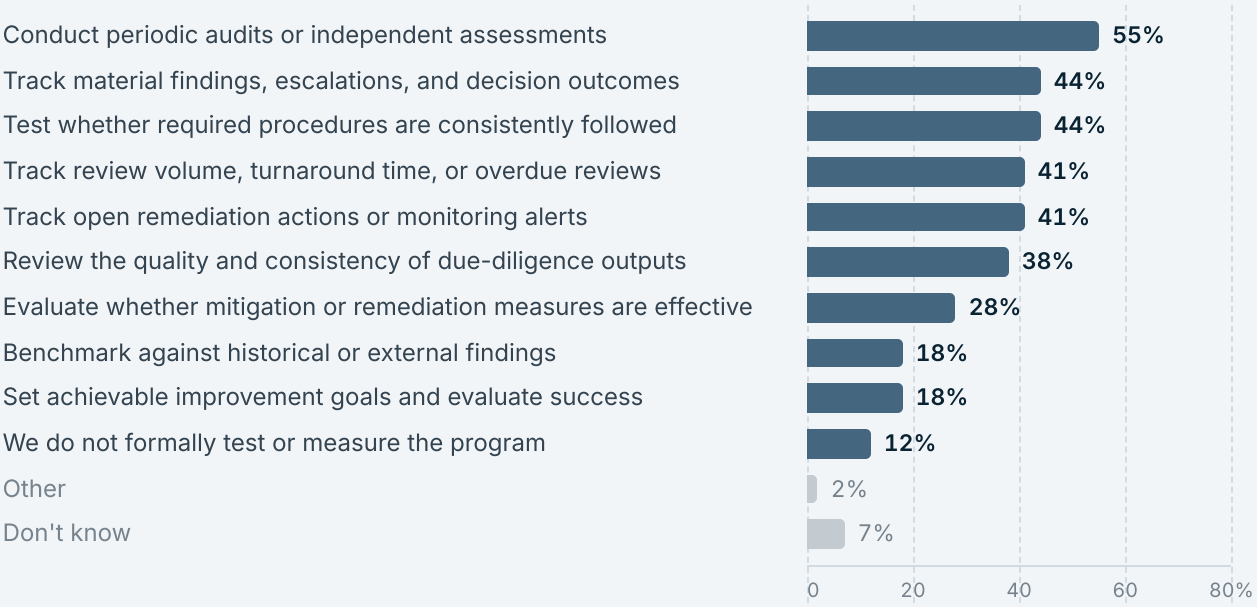
Note: Don’t know: 4%.

Insight

These ratings suggest that many organizations have established structured and repeatable processes for managing third-party relationships. Yet the findings reveal a notable distinction between having an established program and demonstrating that it is effective.

Practices Used to Evaluate or Improve the Program

% of respondents



Note: Select all that apply; percentages total more than 100%.

Periodic audits or independent assessments are the most common way programs are evaluated, and practices aimed at understanding and measuring effectiveness are less common. Eighteen percent benchmark against historical or external findings, and 12% do not formally test or measure their program.

Insight

While 55% conduct periodic audits or independent assessments, only 28% evaluate whether mitigation or remediation measures are effective, and just 18% establish measurable improvement goals and evaluate their success. Organizations are more likely to assess whether their programs are operating as designed than whether those programs are achieving the intended risk management outcomes.

An organization can consistently perform screenings, complete assessments, and follow established procedures without demonstrating that those activities are identifying material risks, influencing decisions, or reducing exposure.

That distinction matters: regulators increasingly expect compliance controls not only to exist but to be tested, assessed for effectiveness, and improved over time. The next stage of program maturity, then, is demonstrating that the program works, and that it is getting better.

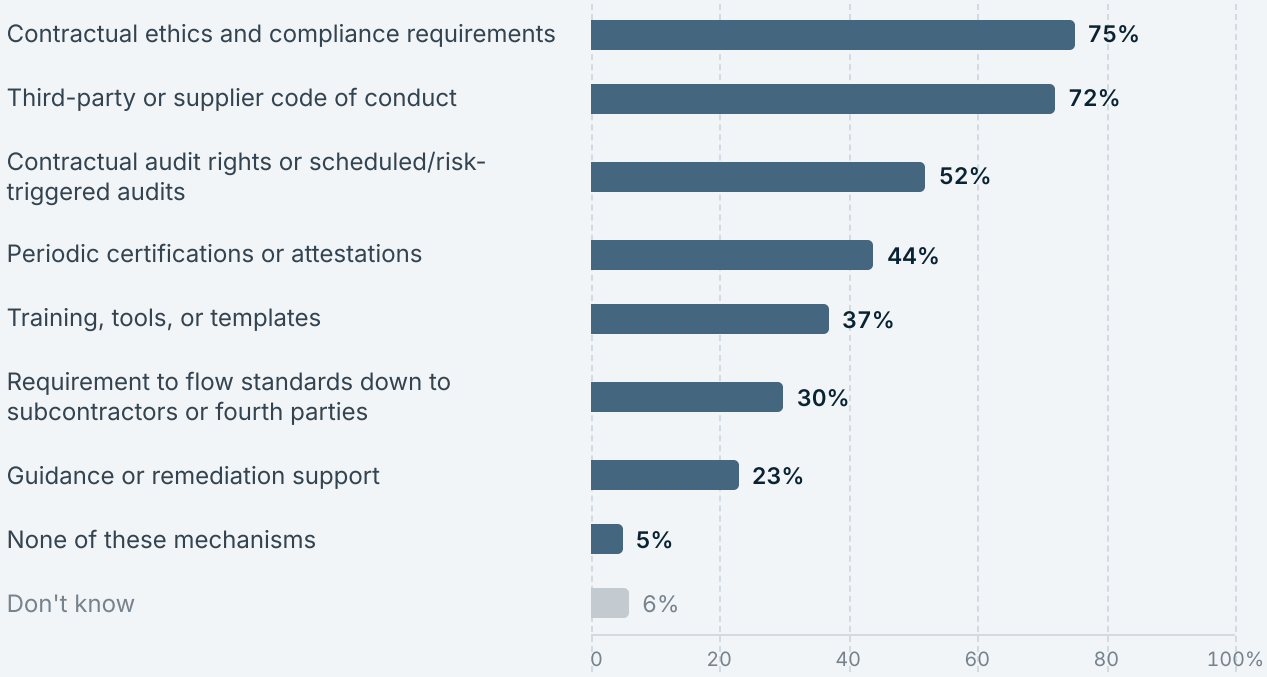
Expectations for Third Parties and Fourth-Party Visibility

Contractual requirements and codes of conduct are the main ways organizations set expectations for third parties.

To convey ethics and compliance requirements or expectations to their third parties, 75% of organizations use contracts as the mechanism, while 72% use a third-party or supplier code of conduct. **Thirty percent require third parties to flow standards down to their own subcontractors.**

Mechanisms Used to Set and Enforce Expectations for Third Parties

% of respondents



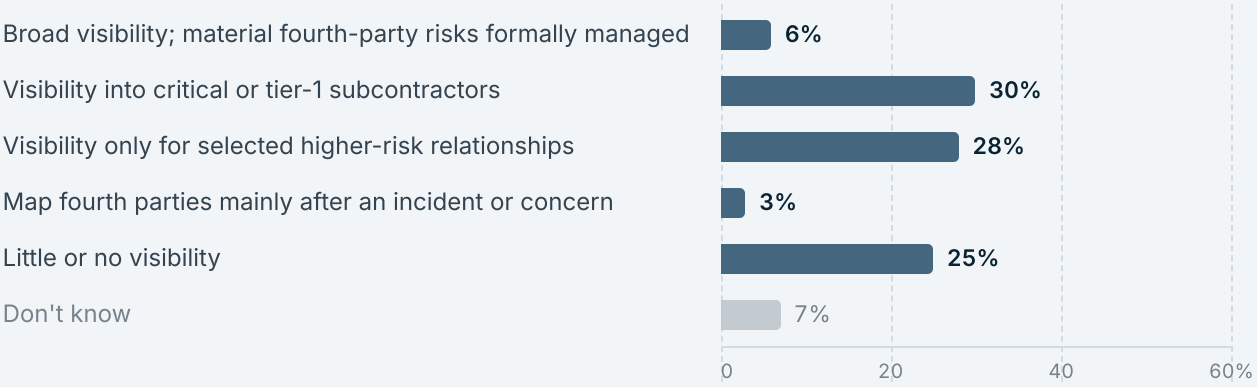
Note: Select all that apply; percentages total more than 100%.

The two leading mechanisms are both written requirements placed on the third party. Mechanisms that call for ongoing effort from the organization itself, such as audit rights, certifications, training, and guidance or remediation support, are less common, and 5% use none of these mechanisms. These mechanisms are also how most findings get handled: organizations tighten terms, require remediation, or monitor more closely rather than end the relationship, which is consistent with how rarely a review ends in a decision not to proceed.

Six percent have broad visibility into fourth parties and formally manage material fourth-party risks, while 25% have little or no visibility.

Visibility Into Fourth Parties and Beyond

% of respondents



Only 36% have either broad visibility into fourth parties or visibility into critical or tier-1 subcontractors; 28% see only selected higher-risk relationships, and 28% either map fourth parties mainly after an incident or have little or no visibility.

Insight

Organizations have made substantial progress in establishing expectations and oversight mechanisms for their direct third-party relationships. Yet visibility often diminishes considerably beyond those relationships.

This limited visibility presents a potentially significant challenge. Critical business services, technology infrastructure, manufacturing operations, and supply chains may depend on entities with which an organization has no direct contractual relationship. Those dependencies can introduce compliance, operational, reputational, and other exposures that may be difficult to identify through traditional third-party assessments alone.

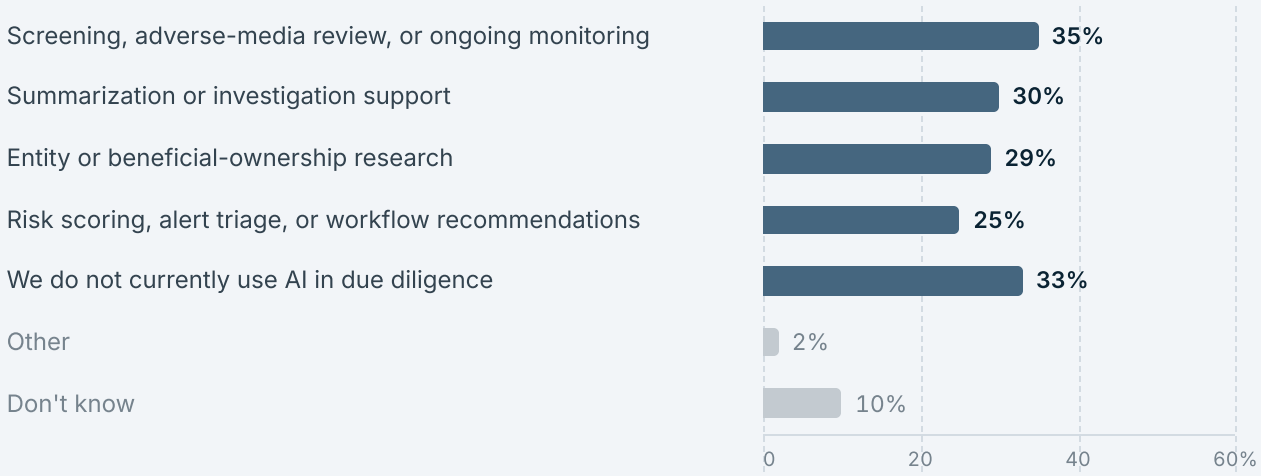
However, comprehensive visibility into every downstream relationship may not be practical or necessary. The challenge is determining which downstream dependencies matter most, and ensuring organizations have sufficient visibility to understand and manage the associated exposure. A more proportionate approach would prioritize visibility into critical subcontractors, service providers, and other dependencies whose failure or misconduct could materially affect the business.

AI in Third-Party Due Diligence

Over half of organizations (55%) use AI in due diligence in some way, while a third do not use it at all.

Current Uses of AI in Due Diligence

% of respondents

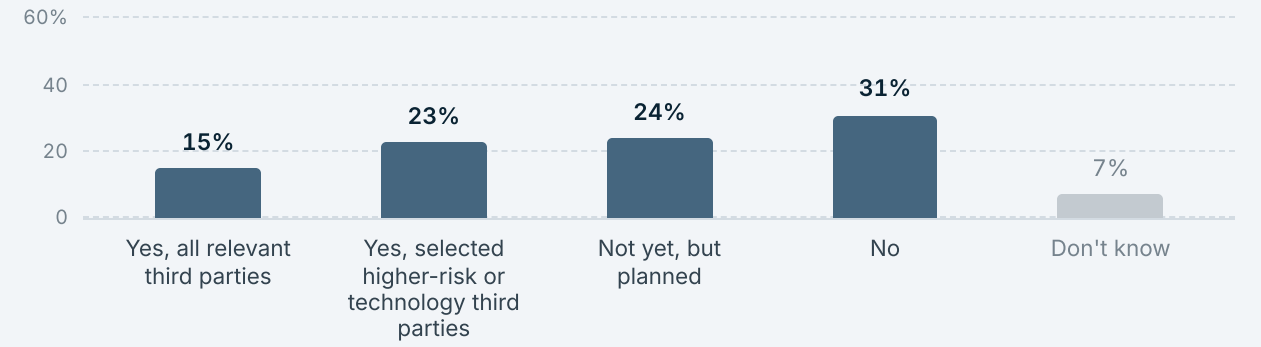


Note: Select all that apply; percentages total more than 100%.

Screening, adverse-media review, and ongoing monitoring is the most common use of AI (35%), followed by summarization or investigation support (30%); 10% do not know whether their organization uses AI. **Thirty-eight percent track how their third parties use or govern AI**, and another 24% plan to start.

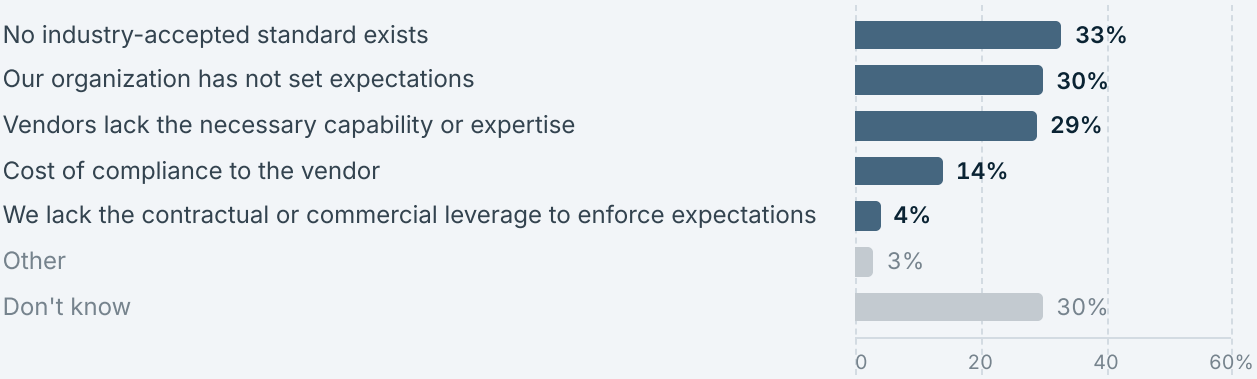
Tracks How Third Parties Use or Govern AI

% of respondents



Obstacles to Third Parties Meeting Expectations for Responsible AI Use

% of respondents

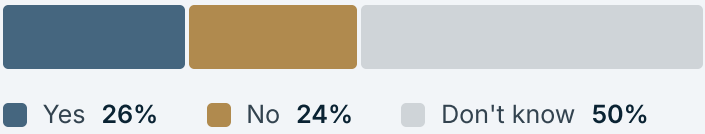


Note: Select all that apply; percentages total more than 100%.

The leading obstacles are that no industry-accepted standard exists (33%), that organizations themselves have not set expectations (30%), and that vendors lack the necessary capability or expertise (29%); 30% do not know. Cost of compliance to the vendor (14%) and a lack of contractual or commercial leverage (4%) are cited far less often.

Would Accept an Independent AI Governance Credential in Place of Its Own Assessment

% of respondents



Respondents are divided on independent AI governance credentials, and half do not know whether they would accept one in place of their own assessment.

Insight

As AI becomes increasingly embedded in third-party products and services, organizations will need to establish clearer expectations for how their third parties use and govern it. Effective oversight will require identifying which AI applications introduce material risk, determining what evidence provides sufficient assurance that appropriate controls are in place, and applying scrutiny proportionate to the sensitivity and potential consequences of each use case. The challenge is not simply to establish AI governance requirements, but to ensure those requirements meaningfully inform third-party risk decisions.

Differences by Organization Size

The largest organizations review more third parties, spend more, and monitor third parties more continuously.

Among organizations with 50,000 or more employees, 50% completed 1,000 or more reviews in the past year, compared with 5% of organizations with fewer than 5,000. Of those who know their spend, 85% of the largest organizations spend $250,000 or more a year on third-party risk management, compared with 16% of the smallest (fewer than 5,000 employees).

The largest organizations (50,000 or more employees) are also more likely to use AI in due diligence (83% compared with 49%) but less likely to track how their third parties use AI (22% compared with 49%). Self-rated maturity and time to clear a new third party vary little by size.

% of respondents in each group	Under 5,000 employees	5,000-49,999 employees	50,000+ employees	All
Due diligence on all or most third-party categories	64%	77%	68%	**69%**
Risk-based approach	86%	91%	95%	**90%**
1,000+ reviews in the past 12 months	5%	23%	50%	**20%**
Clear a new third party within two weeks	37%	37%	30%	**35%**
Annual TPRM spend of $250,000+	16%	28%	85%	**31%**
Continuous monitoring of all or selected third parties	44%	45%	75%	**50%**
Standardized, integrated, or optimized program	65%	63%	74%	**66%**
Use AI for at least one due-diligence activity	49%	50%	83%	**55%**
Track how some or all third parties use AI	49%	32%	22%	**38%**

Bases vary slightly by question. The spend row excludes respondents who did not know their organization's spend. One respondent who did not know the organization's size is included only in "All."

Insight

These findings suggest that greater organizational resources and investment do not necessarily translate into more mature or effective third-party risk management: larger organizations do not consistently demonstrate advantages across other measures of program maturity and oversight.

This distinction reinforces the importance of evaluating program capabilities and outcomes on their own merits, rather than assuming that greater scale, spending, or technological sophistication necessarily indicate stronger risk management. Ultimately, effectiveness depends not simply on the resources devoted to a program, but on how well those resources translate into meaningful risk identification, informed decisions, and measurable outcomes.

Key Takeaways

Third-party due diligence is now a mature, broadly adopted discipline. Nearly every organization surveyed conducts it, nine in ten apply it on a risk basis, and the risk agenda is broad. Bribery, corruption, and fraud, then sanctions, are what reviews look for most and what most often leads to action, but reputational risk, AML and financial crime, privacy, cyber, financial health, modern slavery and human trafficking, and foreign terrorist organizations are each reviewed by at least half of programs, and nearly four in ten already review third parties' use of AI.

The work is routine in its outcomes, but not empty. Most programs find a material issue in fewer than one review in twenty, yet nearly four in ten find them more often, and when they do, the response is almost always enhanced review, remediation, or closer monitoring rather than the end of the relationship. Seven in ten new third parties are cleared to conduct business within a month, and where programs lose time, it is while waiting on others, above all the third party itself, rather than on the review.

The gaps sit at the edges of the program. Visibility into fourth parties is thin, only a minority of organizations set improvement goals and measure against them, and AI has entered due diligence faster than the governance around it: over half of organizations now use AI somewhere in the process, fewer than four in ten track how their third parties use it, and half have not decided whether they would rely on an independent AI governance credential. Those are the areas where the next year of investment is likely to go.

Taken together, these findings point to an important transition in third-party risk management. As programs become more established and increasingly standardized, the next challenge is to demonstrate that the processes organizations have built are delivering meaningful results.

That means moving beyond the volume of reviews conducted, the breadth of third-party coverage, or the sophistication of supporting technology. Organizations must be able to demonstrate that they are identifying relevant risks, obtaining reliable information, making timely and defensible decisions, and continually improving their ability to manage third-party exposure.

The next generation of third-party risk management is not necessarily about doing more due diligence. It is about doing better due diligence, and being able to prove it.

Part 4

Methodology

About the Survey

124
responses analyzed: 105 complete and 19 partial

Sept 9 – Oct 12
2026 fielding period, online

ECI & Diligent
conducted by ECI Compliance Week in partnership with Diligent

The State of Third-Party Risk & Integrity Survey was conducted by ECI Compliance Week in partnership with Diligent. The survey was fielded online from September 9 to October 12, 2026. Invitations were sent by email to ECI Compliance Week's members and contacts, and to Diligent's customers. The survey was also promoted on LinkedIn and on Diligent's platform.

Respondents were asked whether their organizations conduct third-party due diligence. Those who said they do not, have no plans to, did not know, or said their organizations do not use third parties were exited from the survey. The analysis includes 124 responses: 105 complete and 19 partial responses that answered at least the first program questions. Responses with no substantive answers, repeat submissions by the same person, responses completed in less than a third of the typical time, and a small number of responses from outside the target population were removed.

Percentages are based on the respondents who answered each question. Bases vary by question, from 96 to 124, because respondents who were not shown a question because of earlier answers are not included in its base. "Other" and "Don't know" bars are drawn in grey. "Don't know" is shown as a response everywhere except the spend chart, whose base excludes respondents who did not know. Results for select-all questions add to more than 100%, and other results may not add to exactly 100% because of rounding.

Results are unweighted. Because respondents chose to participate, the sample is not a probability sample, and a margin of sampling error is not reported. Comparisons between small groups, such as the organization-size groups, should be read as indicative.

About the Respondents

In all, 124 professionals responsible for or involved in third-party risk management took part, with 65% of respondents working in the ethics and compliance function.

Respondent's Function

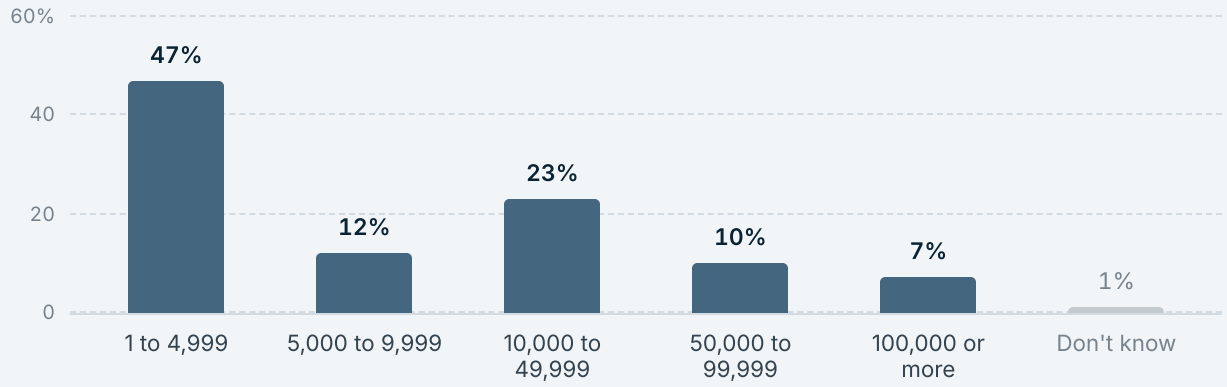
% of respondents



Taken together, 81% of respondents work in an oversight or assurance function: ethics and compliance, internal audit, or enterprise risk management.

Organization Staff Size

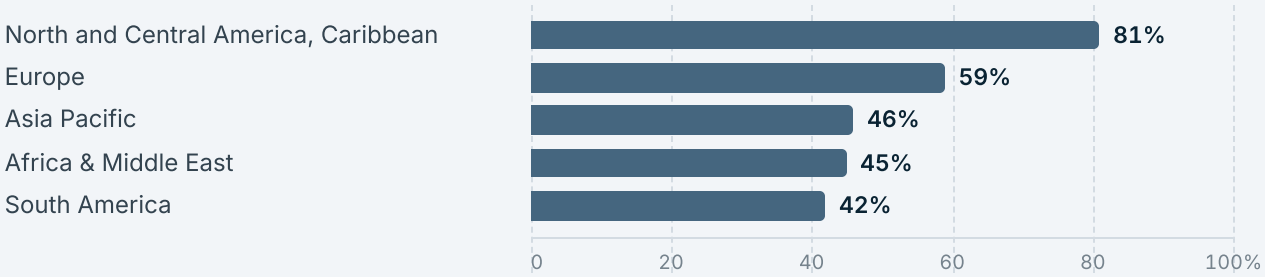
% of respondents



Organizations of every size are represented. **Forty-seven percent have fewer than 5,000 employees** and 18% have 50,000 or more. Mid-sized and large organizations are well represented: 40% have 10,000 or more employees.

Regions Where the Organization Operates

% of respondents

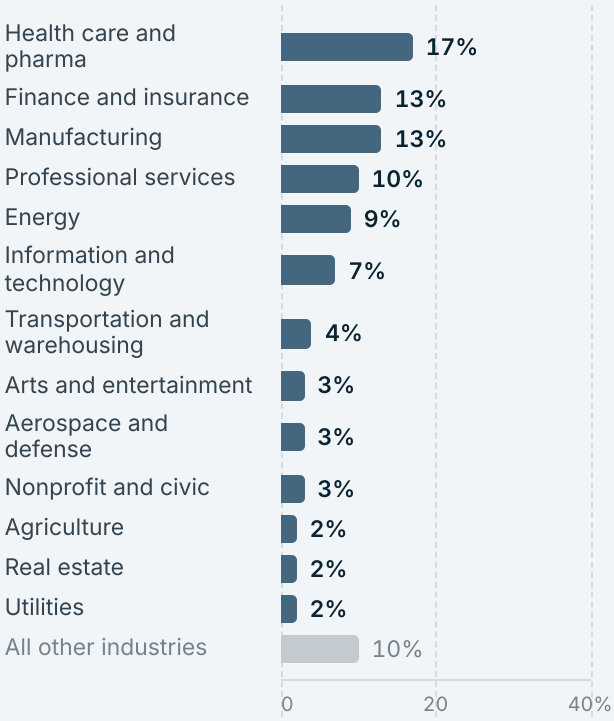


Note: Select all that apply; percentages total more than 100%.

Multinational footprints are common: **53% of organizations operate in more than one region**, and 33% operate in all five regions listed in the survey. Outside North and Central America and the Caribbean (81%), each of the four remaining regions draws between 42% and 59% of respondents, with Europe the most common.

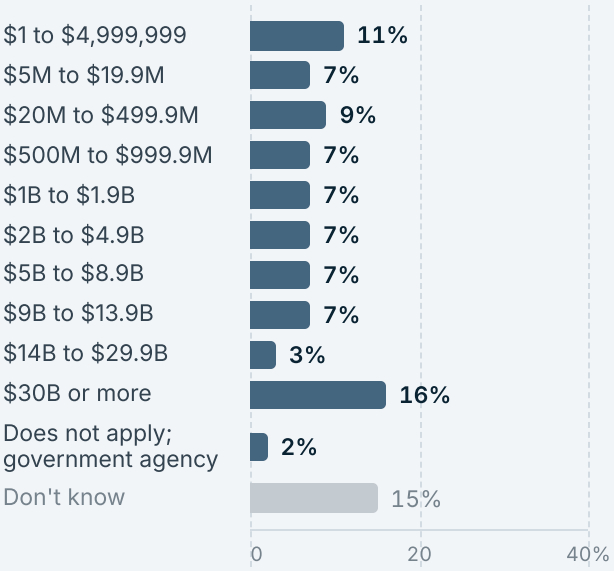
Organization Industry

% of respondents



Organization Annual Revenue (US$)

% of respondents



Health care and pharmaceutical companies are the largest industry group (17%), followed by finance and insurance and manufacturing (13% each).

Sixteen percent of organizations report annual revenue of $30 billion or more, and 15% of respondents do not know their organization's revenue.

ECI Compliance Week

About ECI Compliance Week

ECI Compliance Week is the membership organization for ethics, compliance, and risk professionals. It brings together the Ethics & Compliance Initiative, which has set the standard for ethics and compliance programs since 1922, and Compliance Week, its newsroom. Through research such as this report, benchmarking, and education, we serve about 700 corporate members and more than 50,000 professionals in 179 countries.

For teams managing third-party risk

Benchmark your program. Compare your ethics and compliance program and your AI governance against ECI's validated High-Quality Program (HQP) framework and against peers in your industry.

Extend the standard to your suppliers. Corporate members can require AI Governance Essentials and Ethics & Compliance Essentials of their third parties at no extra cost. You send the invitation, suppliers submit evidence, ECI reviews it, and your portal shows each supplier's status and rating.

Credential the whole team. Certifications in ethics and compliance leadership (LPEC), AI governance (LPAIG), and anti-financial crime (through Financial Crime Academy) are included for every user, along with 50+ courses and no per-person fees.

For suppliers and smaller organizations

Answer your customers once. AI Governance Essentials and Ethics & Compliance Essentials are independent, evidence-based assessments. Each one results in a single ECI-reviewed report and badge you can share with every customer who asks. Both are included in membership.

Show your people are qualified. Certified staff in ethics and compliance, AI governance, and financial crime give customers another reason to trust you in due diligence.

Membership built for smaller teams. Organizations under $50 million in revenue receive reduced rates on every corporate tier.

Events. Member rates for Compliance Week National and the TPRM and Supply Chain Summit.

Learn more at eci-insights.com.

Diligent

About Diligent

Diligent is the AI leader in governance, risk and compliance (GRC) SaaS solutions, helping more than 1 million users and 700,000 board members to clarify risk and elevate governance. The Diligent One Platform gives practitioners, the C-Suite and the board a consolidated view of their entire GRC practice so they can more effectively manage risk, build greater resilience and make better decisions, faster.

© 2026 ECI Compliance Week. All rights reserved.