

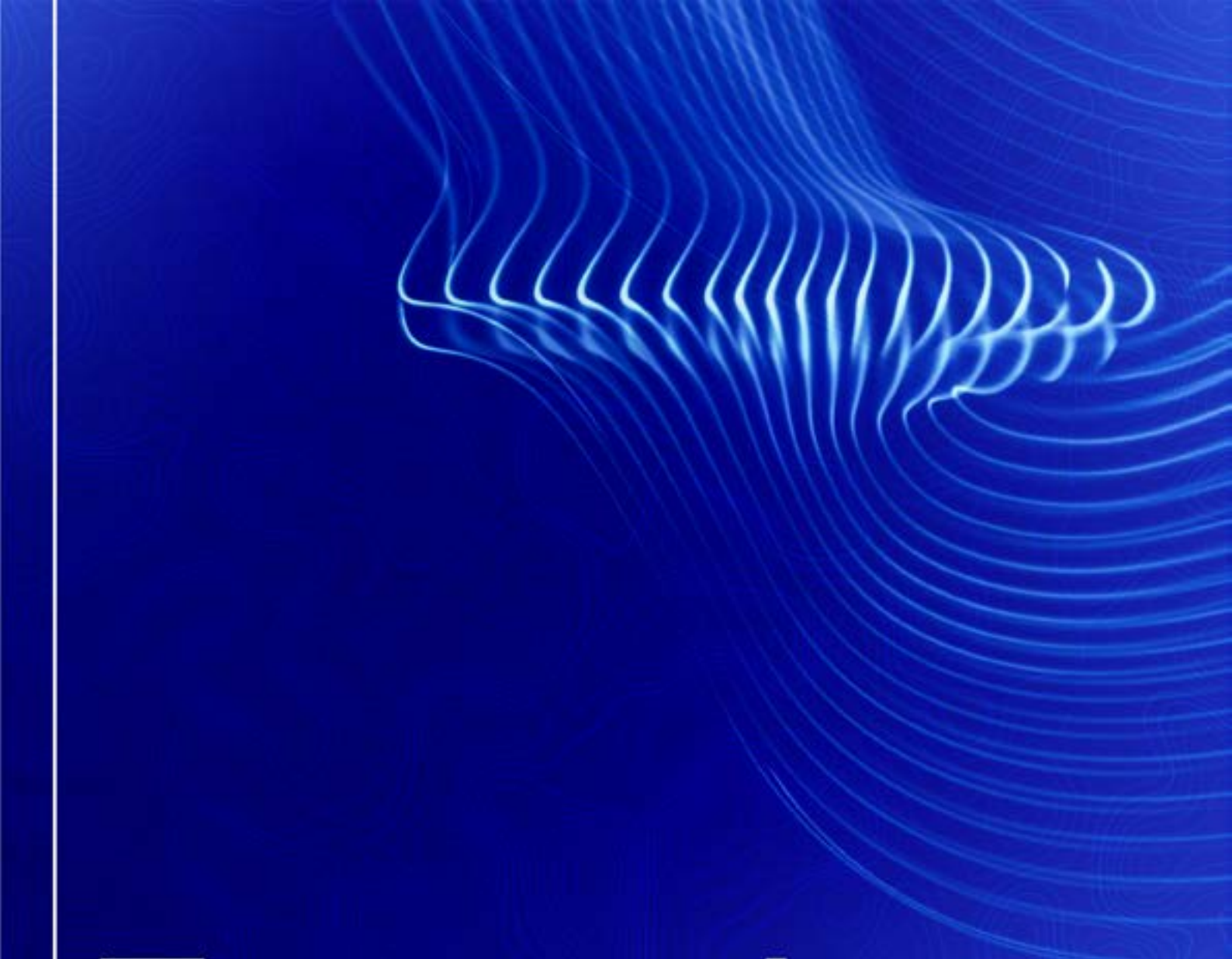
Survey on Third-Party Cyber Risk Management in Brazil

3rd edition | 2026



Table of Contents

Executive Summary	3
Understanding TPCRM	5
Insights	9
Data and Analysis	15
TPCRM Programs in Companies	16
Who Has TPCRM Programs	16
Which department handles third-party cyber risks?	17
Key Challenges	18
Elements for Success	18
Third-Party Assessment in TPCRM Programs	20
Methods and Tools	20
Which third parties are managed	22
Cloud Visibility and Risks	23
Security Policies and Incidents	25
Governance, Contracts, and Collaboration	26
Our Research	28
Purpose of the Survey	29
Transparency and Sampling	29
Company Profiles	30
Profile of Respondents	31



Executive Summary

For the third consecutive year, we at Tenchi Security have conducted the Survey on Third-Party Cyber Risk Management to better understand how Brazilian companies address this issue.

We emphasize that this publication is not intended exclusively for IT technicians and cybersecurity professionals. Third-party cyber risk management should be of interest to various teams within a company because it impacts both contracting processes and the lifecycle of business partnerships, while information security—especially today—is closely tied to day-to-day business operations.

In fact, among the professionals who have dealt with a security incident in the past two years and who responded to our survey, **68%** say the incident had an operational impact, resulting in service instability or disruptions.

Forming partnerships with resilient companies and robust suppliers is not just a concern for the cybersecurity team. For this reason, this report aims to use accessible language, and this year we have included a dedicated chapter to explain the topic of *Third-Party Cyber Risk Management* (TPCRM) and the current landscape, including examples of relevant incidents.

Over the past three years, our research has indicated that the elements considered necessary for successful third-party cyber risk management are not aligned with the methods used to assess third parties. According to the professionals who responded to the survey, the key to effective management lies in timely information, responsiveness, and visibility into the cloud infrastructure.

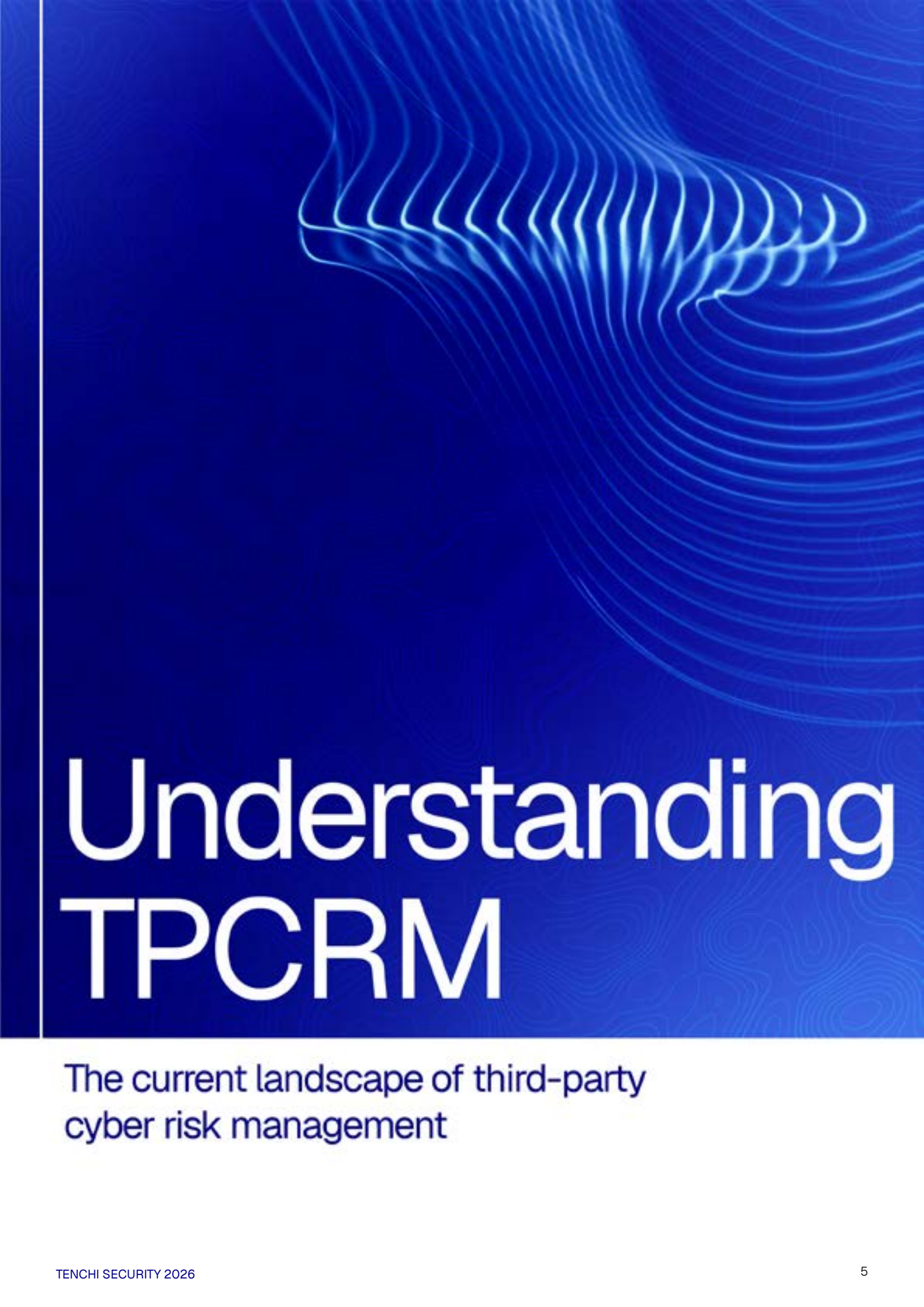
However, the most commonly used methods for evaluating third parties provide one-time assessments, without continuous visibility into any infrastructure, and sometimes do not yield any concrete data on the cloud infrastructure. Instead of automation, we rely on questionnaires and the collection of certificates that are not always directly relevant to the business or the task to be performed.

With some reflection, we can understand the framework that gave rise to this scenario: the link between TPCRM and governance, risk, and compliance (GRC) processes.

But we cannot be overly critical of our history. The world used to be much simpler and less connected than it is today. Companies had fewer suppliers, products had fewer components, and services were simpler.

The key lies in recognizing this change, understanding that the transformations we've undergone and the risks we face today are partly the result of a reality that didn't exist before. From this perspective—and with valuable insights into what other companies are already doing—we can decide on our next steps. Providing these insights is our goal with this research.





Understanding TPCRM

The current landscape of third-party
cyber risk management

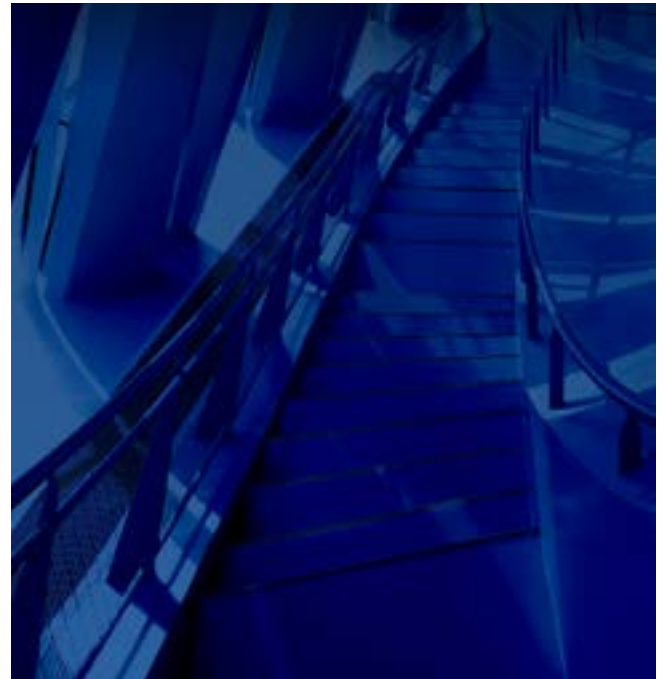
Third-Party Cyber Risk Management (TPCRM) is a set of processes, tools, and technologies designed to monitor IT infrastructure and security controls, evaluate policies, and support decisions involving third parties associated with an organization.

TPCRM is an offshoot of Third-Party Risk Management. This terminology, which is widely used by regulators, expands the concept of supplier risk management, making it clear that this approach must also extend to other third parties, including business partners.

As information technology infrastructures become essential to business processes, the risk arising from incidents involving these assets tends to increase. Furthermore, many companies seek outsourced solutions to meet their technology needs.

Even when technology is hosted on the company's own infrastructure ("on-premises"), it is often connected to and exposed to external and internal threats, creating a scenario in which the use of a product inherently entails operational risks. The use of outsourced platforms or infrastructure is an aggravating factor when the company does not implement any risk management to align its operations and its relationship with these third parties.

Thus, just as information security has become a discipline in its own right, the prevalence of cyber risk justifies the adoption of measures specifically designed to address cyber risk originating from third parties. Many companies are still experimenting with different methods and processes to carry out this work, as this survey shows.



Third-Party Cybersecurity Risks

Third-party cyber risks can have operational, financial, and legal impacts and, in this sense, resemble common cyber risks. However, third-party risks also have specific elements, such as concentration risk (when a large portion of the market or an economic sector depends on a few specialized suppliers), which give rise to new forms of cyber risk.

Malicious actors may be interested in attacking popular suppliers because of the opportunity to target hundreds or thousands of companies simultaneously. Similarly, a major company may be indirectly affected by cyberattacks and breaches at smaller suppliers.

Key Methods for Third-Party Security Assessment

Self-Assessment Questionnaires (SAQ)

A questionnaire that may contain hundreds of questions designed to elicit information from a third party regarding its cybersecurity policies and controls. It relies on information provided by the third party itself.

Outside-in monitoring (Security Rating Service)

Periodically examines third parties' external assets to identify potential issues. It does not rely on information provided by the third party, but it does not offer the same automated visibility into internal controls and systems as the technology used for external assessment.

Inside-out monitoring

Periodically examines third-parties' internal assets to identify issues and operational misconfigurations. It provides automated visibility into security controls, at-risk assets, and compliance with defined policies, but requires the third party to authorize a scan of its cloud environment.

Audits

Audits provide visibility similar to the self-assessment questionnaire, but the evidence is documented with greater reliability. Audits rely on manual effort and are therefore one-time analyses.

Collection of Certifications, Assessment Reports, and Audit Reports

The company requires the vendor or partner to provide certifications of compliance with ISO standards or other standards, such as SOC 2. The assessments underlying these certifications are point-in-time evaluations and are not supervised by the company.

Penetration testing

A penetration test (or *pentest*) simulates a cyber-attack in a controlled manner to detect vulnerabilities, exposed infrastructure, and even weaknesses in employee training. It requires manual effort by offensive security specialists.

Notable Incidents in 2025

Attacks on the Pix System in Brazil

Financial institutions in Brazil have suffered a series of attacks that were disclosed by the Central Bank. Unlike fraud, which affects account holders and consumers, these attacks directly targeted the reserve accounts maintained by the institutions to guarantee transactions in the Instant Payment System (SPI), which is linked to Pix.

Several of these attacks originated at third-party companies that supplement the banks' infrastructure. Although the Central Bank requires these companies to be certified to operate within the financial system's network, existing rules were insufficient to prevent these attacks, prompting regulators to revise existing requirements and impose stricter risk management rules on these third parties.

Shai-Hulud and tj-actions

Shai-Hulud is malicious code capable of spreading to code repositories, contaminating new packages and dependencies when it infects software engineers. This malware emerged in September 2025, but its concept has already been adapted for other attacks. The name "Shai-Hulud" is inspired by *the sandworms* from Frank Herbert's novel **Dune**, alluding to the concept of a "worm" that defines malicious code capable of spreading.

Even when an attack lacks specific code for propagation, code can spread through unmitigated integrated dependencies. An example of this occurred in March 2025, when cybercriminals compromised *tj-actions*, a GitHub repository containing predefined actions for workflows. The compromised code was executed across more than 200 repositories.

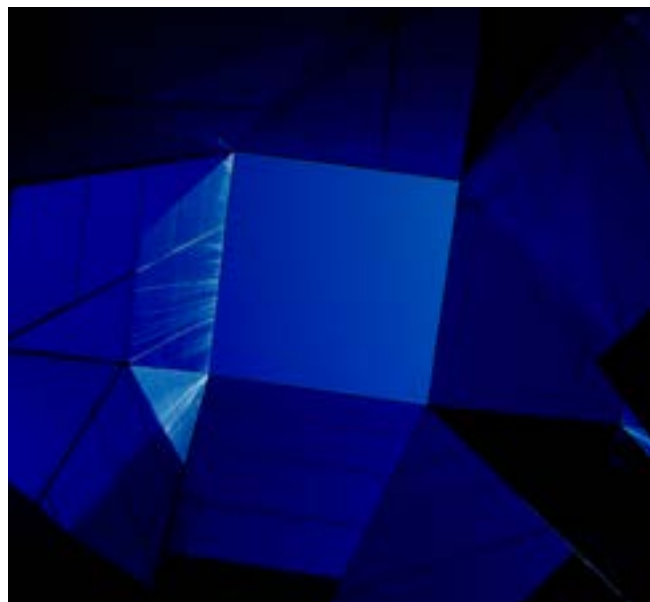
Salesforce Integrations

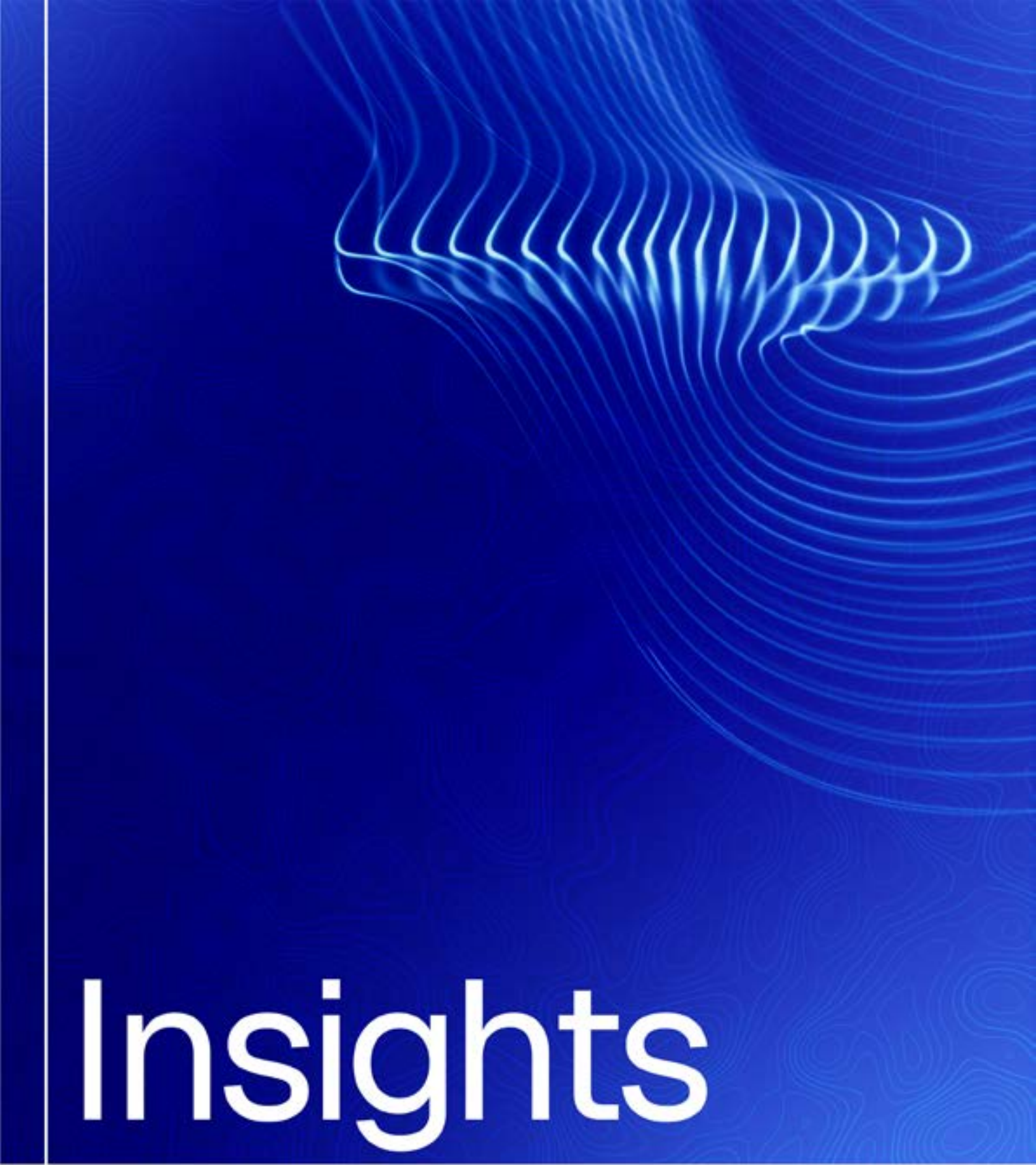
Criminals targeted the companies Salesloft and Gainsight, which offer applications that integrate with Salesforce instances. Using access obtained through these providers, the criminals were able to steal corporate data without compromising Salesforce and without attacking the companies that operate the instances.

Collins Aerospace

A cyberattack took down an air cargo management system provided by Collins Aerospace. The incident caused flight delays in Europe, leading to a ripple effect that impacted several European airports.

This case illustrates how systemic risks can exist even when there is no direct concentration of operations. An aircraft experiencing a delay at one airport impacts operations at other airports along its route, even if those airports use different software that has not experienced any instability.





Insights

Main findings of the research

1

Professionals seek agility, but TPCRM still focuses on one-off assessments

84%

Believe that detecting threats in real time is important for the success of the TPCRM program

Many professionals consider continuous monitoring capable of identifying threats in near-real-time to be one of the three most important elements for the success of a third-party cyber risk management program.

In addition to being the most frequently cited element, near-real-time threat monitoring was also the most commonly selected as the top choice among survey participants: 31% consider it the most important element.

However, the most widely used method for managing third-party risks remains the Self-Assessment Questionnaire (SAQ). In addition to relying on the third party's good faith, this method provides only a one-time assessment and does not offer continuous or real-time information. This means there is a potential disconnect between what professionals consider important and the assessment methods used in practice.

2

Continuous monitoring facilitates more frequent assessments

45%

Third-party security is assessed at most twice a year

37%

Conduct assessments weekly or more frequently

While some companies conduct only semianual or annual assessments to evaluate third parties' cybersecurity posture, about one-third of organizations are able to conduct these assessments on a weekly basis or even more frequently, moving closer to the goal of real-time threat detection.

The explanation for this difference appears to lie in the method used to assess third-party cybersecurity.

Among companies that use continuous monitoring, 53% are able to conduct weekly or more frequent assessments. Among companies that use inside-out continuous monitoring—which scans the third-party's infrastructure “from the inside”—this figure rises to 58%. When companies do not use any type of monitoring, only 19% conduct weekly assessments.

3

Visibility, engagement, and automation are the biggest challenges



37%

Believe that a lack of visibility is the biggest challenge for third-party cyber risk management

Among survey participants, 37% believe that a lack of visibility into third parties' cybersecurity posture is the biggest challenge for risk management.

Meanwhile, 25% pointed out that the greatest difficulty is engaging third parties to respond to risk assessments.

In practice, the two issues cited by professionals share some commonalities. When third parties fail to engage in risk management initiatives, visibility is often reduced.

The third most common challenge, cited by 21% of survey participants, is automating the management process so that it can be scaled to meet risk management demands.

4

SaaS and the cloud are the infrastructures that cause the most concern

84%

Cloud infrastructure is one of the top three concerns

In 2025, several high-impact incidents underscored the relevance of concerns regarding Software-as-a-Service platforms. One example is the incident involving applications integrated with the Salesforce system.

Then, in 2026, Vercel, a company specializing in cloud applications, was compromised through an attack on Context.ai, an artificial intelligence solutions provider that had been authorized to access files in a Vercel employee's Google account via OAuth.

In the software supply chain, a series of incidents compromised popular GitHub repositories, triggering a ripple effect in the integration and deployment workflows linked to these tools. The problem even affected security tools, such as the Trivy code scanning tool.



5

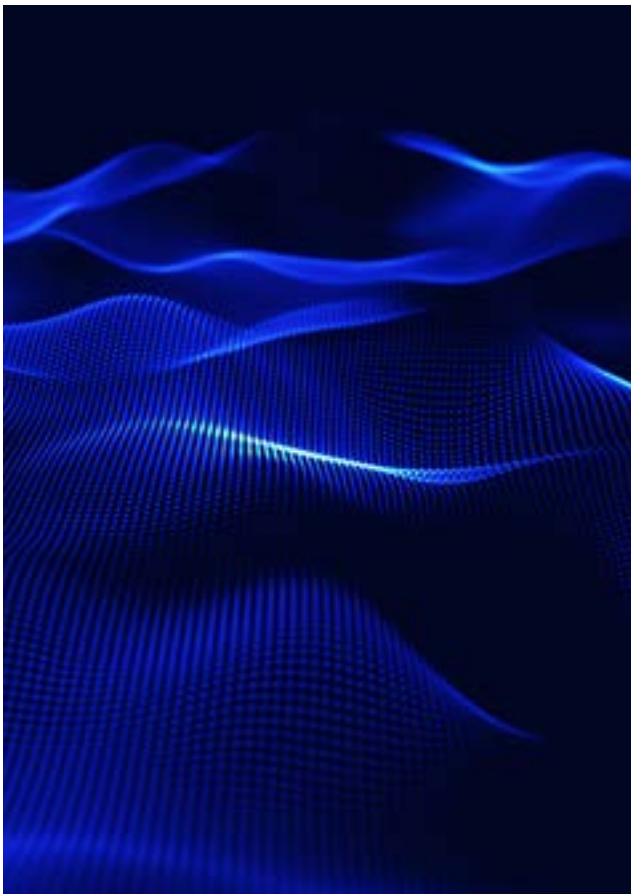
Companies Still Lack Visibility into the Cloud

52%

Say they lack visibility into third-party cloud services

Although monitoring cloud IT infrastructure is considered one of the most important elements for successful third-party cyber risk management, more than half of respondents (52%) said they lack this visibility.

When this capability is available, it tends to be used frequently. 35% of professionals who reported having this capability use it on a daily or weekly basis. However, 31% said they conduct annual checks, and 4% do so only once for each third party.



6

The Volume of Third Parties Expands the Attack Surface



49%

Of respondents indicate that the company has more than 1,000 third-party vendors.

49% of the professionals surveyed said their companies have more than 1,000 third-party vendors.

Every organization needs to protect its IT assets and its own attack surface. However, vendors and third parties also have their own attack surfaces and assets, which often have some point of contact with those of the contracting company.

When the number of third-party vendors is high, it is almost certain that many of them are, in practice, expanding the attack surface that exposes the company to risks.

7

Coverage of TPCRM programs is increasing



38%

Of respondents report that the company manages all third parties using at least one tool

Our survey data indicates that companies are expanding their third-party cyber risk management programs to gain visibility into all third parties, including those not considered critical to the business.

In 2023, only 30% of respondents said their companies managed all third parties. This percentage rose to 35% in 2024 and 38% in 2025.

Some assessment methods, however, are reserved primarily for critical third parties. For example, only 20% of professionals who cited the use of penetration testing (pentesting) said they conduct it on all third parties.

8

Lack of Budget and Prioritization Hinder TPCRM Programs

86%

Have a formal program for third-party risk management

Most survey participants reported that their organizations already have a third-party cyber risk management program.

Among companies with more than 5,000 employees, 92% have a third-party cyber risk management (TPCRM) program.

However, when no such program exists—which is the case for 14% of respondents—the main obstacles cited are a lack of organizational prioritization (47%) and a lack of budget (35%). The remaining 18% who do not yet have a TPCRM program reported that it is currently in some stage of development.



9

Internal teams handle risk management

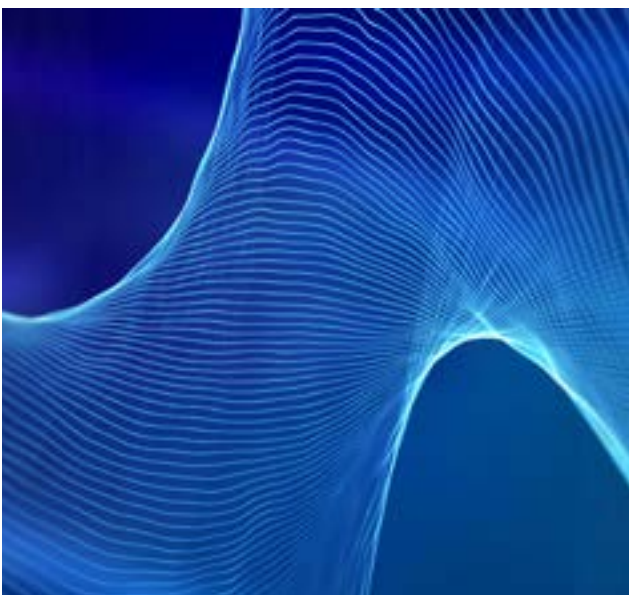
77%

Of respondents manage third-party cyber risk using in-house teams

The professionals surveyed indicated that their companies generally handle third-party cyber risk management with in-house teams, which operate the tools acquired for this purpose.

Looking at all respondents in our survey, more than half (53%) reported that their company has at least three people dedicated to third-party risk management.

- Among professionals working at companies with **up to 1,000** employees, 39% said they do not have a team dedicated to third-party risk management.
- In contrast, among companies with **more than 1,000** employees, 82% said they have a dedicated team, and the percentage of companies with at least three professionals dedicated to this task rises to 61%.



10

Professionals Want More Information on TPCRM

89%

Of professionals say they lack educational materials or guidance on TPCRM

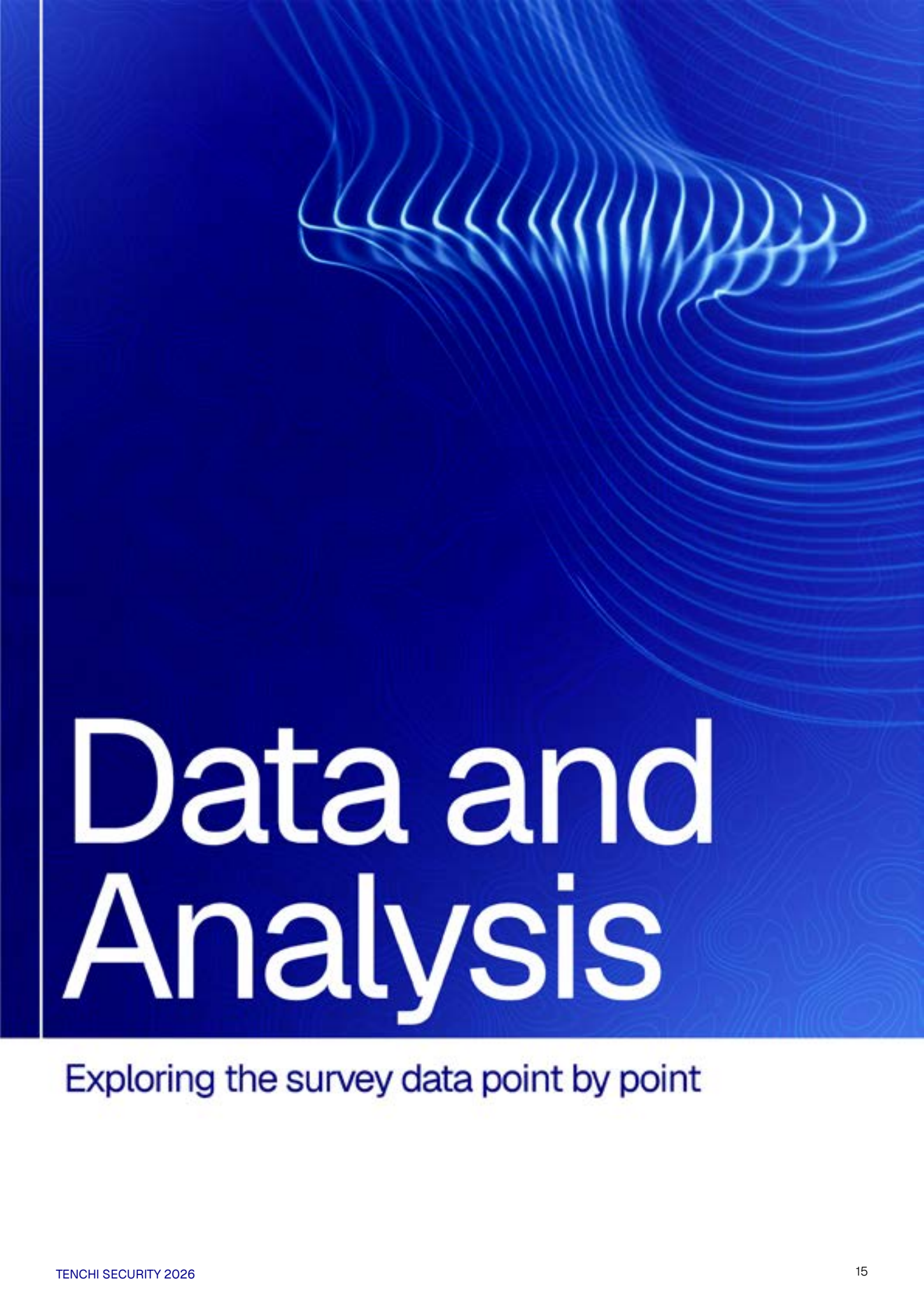
34%

Want to learn more about frameworks and industry best practices

Many professionals want access to materials or training related to third-party cyber risk management.

The most sought-after content covers frameworks and industry best practices (34%), followed by real-world case studies and lessons learned (24%). This indicates that professionals want to understand how TPCRM challenges are addressed in the real world.

Unfortunately, the evolving threat landscape necessitates a review of established processes and the development of new methods and guidelines. The severity and frequency of incidents involving third parties show that some “best practices” are no longer sufficient to address the problem. Innovating with real business threats in mind can yield better results than conventional solutions.

The background of the slide is a solid blue color. In the upper right quadrant, there is a series of white, wavy, concentric lines that resemble a stylized fingerprint or a series of ripples. These lines are more prominent in the upper right and fade out towards the bottom left.

Data and Analysis

Exploring the survey data point by point

TPCRM Programs in Companies

Who Has TPCRM Programs

- **86%** of survey participants said that the companies where they work have a program for managing third-party cyber risk.
- Among companies with more than 5,000 employees, **92%** have a TPCRM program.
- 100% of participants in the insurance sector said their company has a TPCRM program.
- In the retail sector, the figure was 75%.

As in previous years of the survey, we found that smaller companies have more difficulty establishing a program for managing third-party cyber risks. In general, these companies are focused on other areas of business.

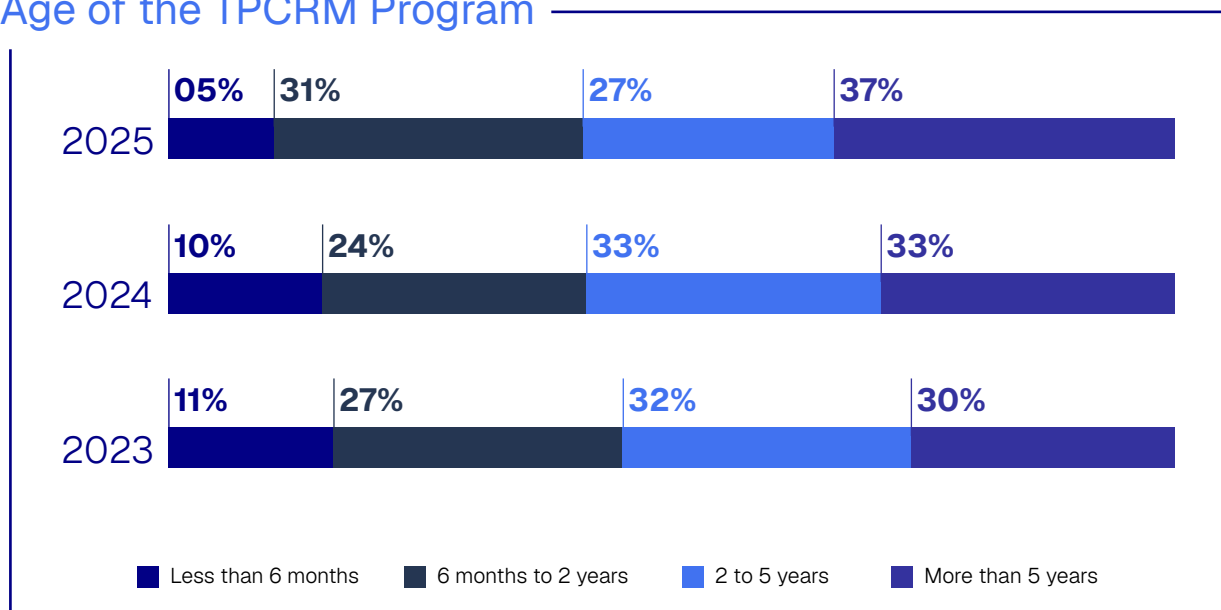
In large companies, it is prudent to take this fact into account when managing third-party cyber risk. After all, smaller companies that struggle to establish their own programs are often suppliers to larger companies, and this unmanaged risk can impact relationships with major clients.

It is worth noting that smaller companies face barriers that do not exist for larger companies.

Some technology products bundle advanced security and management features with functionalities designed for large corporations, which impacts the security of companies that still need security but do not need the other features. This phenomenon is sometimes called the “security poverty line.”

When we analyze the data by sector, we also observe some interesting patterns. The data suggest that insurance companies and financial institutions are the ones most likely to have a third-party risk management program: 100% in the case of insurance companies, and 93% in financial institutions.

Age of the TPCRM Program



Since the concept of TPCRM is relatively new, many of these initiatives were established only recently. In 2023, when we first conducted this survey, 30% of companies had had a TPCRM program for more than 5 years, but 11% of them were just getting started, with programs established less than six months ago. In 2025, 37% of participants said their program had been in place for more than 5 years, and only 5% said it had been in place for less than six months.

In industries where the very existence of a TP-CRM program is less common, these programs are also more likely to have been in place for a shorter period of time. In our 2025 survey, no participants in the retail sector indicated that the program had been in place for more than 5 years at their companies. Among insurance companies and financial institutions, 44% of programs have been in place for more than 5 years.

Which department handles third-party cyber risks?

68%

Information
Security

26%

Risk
Management

4%

Privacy

2%

Other

77%

Have an in-house team to handle third-party cyber risk management

Third-party cyber risk management can involve various departments, including the procurement and acquisitions department. In certain jurisdictions, regulations impose requirements for contracting third parties, particularly in specific sectors such as critical infrastructure (water, energy), health-care, and financial services.

For this reason, the management of these risks is not always the responsibility of the information security team. Although this is the most common scenario, we also see that about one in four professionals report that this work is carried out by the risk management team.

In the case of Brazil, as we mentioned last year, one of the main laws that specifically addresses relationships with third parties is the General Data Protection Law (LGPD), which defines in some detail the responsibilities of the data controller and third-party processors. Therefore, it is understandable that some companies have entrusted this work to the team responsible for data privacy.

It is possible that regulatory changes will introduce more comprehensive rules, creating challenges for teams focused solely on the LGPD. Whatever the strategy, it is important that its continuity can be guaranteed even after such changes.

Key Challenges

Since most survey participants work at companies that already have a TPCRM program in place, the biggest challenge they mentioned was the lack of visibility into third parties' security posture. In other words, it is difficult to manage risk when you do not know exactly how third parties handle their security.

In a sense, the three most frequently cited challenges are linked to the methods used for assessment. Many methods do not ensure visibility into third parties' security posture over time and require the third party to be constantly engaged to collaborate promptly and provide the requested clarifications.

More accurate and automated methods make it easier to overcome these challenges.

The fourth obstacle can also be mitigated with a method capable of generating comprehensive reports on all assessed third parties. Approaches based on document reviews tend to be more labor-intensive, requiring a professional to analyze whether the evidence provided is sufficient to address the requested clarifications.



What is your biggest challenge in third-party risk management?

(single choice)

37%

Lack of visibility into third parties' security posture

25%

Engaging third parties to respond to risk assessments

21%

Difficulty automating and scaling the management process

13%

Lack of time and/or staff to manage the volume of third parties

5%

Justifying the investment (budget/ROI) to senior management

Elements for Success

Here, each participant could choose three elements they consider most important for the TPCRM program to succeed. As in the previous edition, the main element cited is the ability to continuously monitor cyber risks to identify threats in near real time.

This is the same operating model as cybersecurity tools, which continuously assess the reliability of the systems they protect. Governance and compliance practices that rely on questionnaires and certifications do not offer this level of visibility to mitigate risks in real time.

It is not uncommon for third-party incident investigations to take months. We saw an example of this in February 2026, when Conduent, which provides services to state and local governments in the United States, revealed that millions of people were affected by an incident detected in January 2025—more than a year earlier.

What Matters for the Success of the TPCRM Program	Mentions	Top priority
Continuously monitor cyber risks to identify threats in near real time	84%	31%
Have a cyber risk score to support decision-making	64%	25%
Conduct a comprehensive cyber risk analysis, even if it requires more effort	62%	16%
Make quick decisions based on an initial high-level analysis	36%	15%
Have an executive report that maps the cybersecurity risks of all third parties	30%	2%
Rely on third-party-issued reports (audits, certifications, etc.).	24%	11%

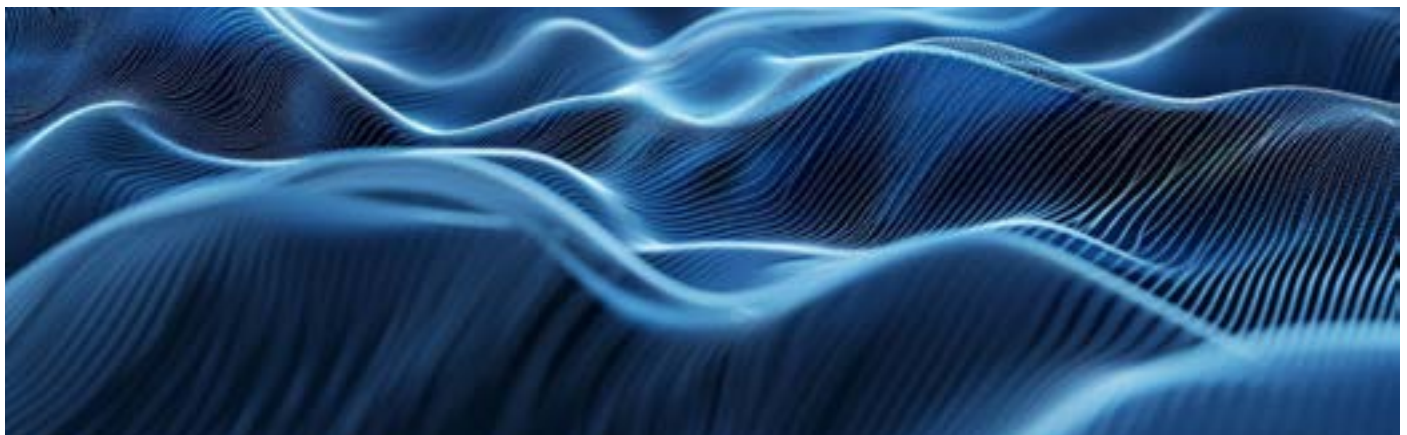
Each participant chose three options and could rank them to identify the most important one (1st choice)

On the other hand, we see that few professionals prioritize certifications and third-party audits. In early 2026, a whistleblower made allegations of fraud involving SOC 2 reports, claiming that a company in the industry was fabricating evidence to facilitate and expedite the certification process.

Unfortunately, certification audits rarely manage to thoroughly analyze all the required criteria and rely on the good faith of the company being

evaluated. Since many companies seek certification to open doors in the market, there is an incentive to obtain the certification even if it does not accurately reflect the company's day-to-day operations.

Although it is often viewed as of little relevance, the collection of certifications is one of the most widely used methods for evaluating third parties, as we will see below.



Third-Party Assessment in TPCRM Programs

When structuring a third-party cyber risk management program, one of the most important decisions concerns the assessment mechanisms and tools that will be used.

These methods have a direct impact on the quality of the evidence, the nature of the data that will inform decision-making, and the speed with which this assessment can be conducted.

More profoundly, the choice of methods shapes the approach of the risk management program. Some methods are more collaborative, offering benefits to both parties in the event of a rejection or an incident. Other methods are more adversarial, in which the contracting party merely determines whether the third party is qualified to provide services.

Methods and Tools

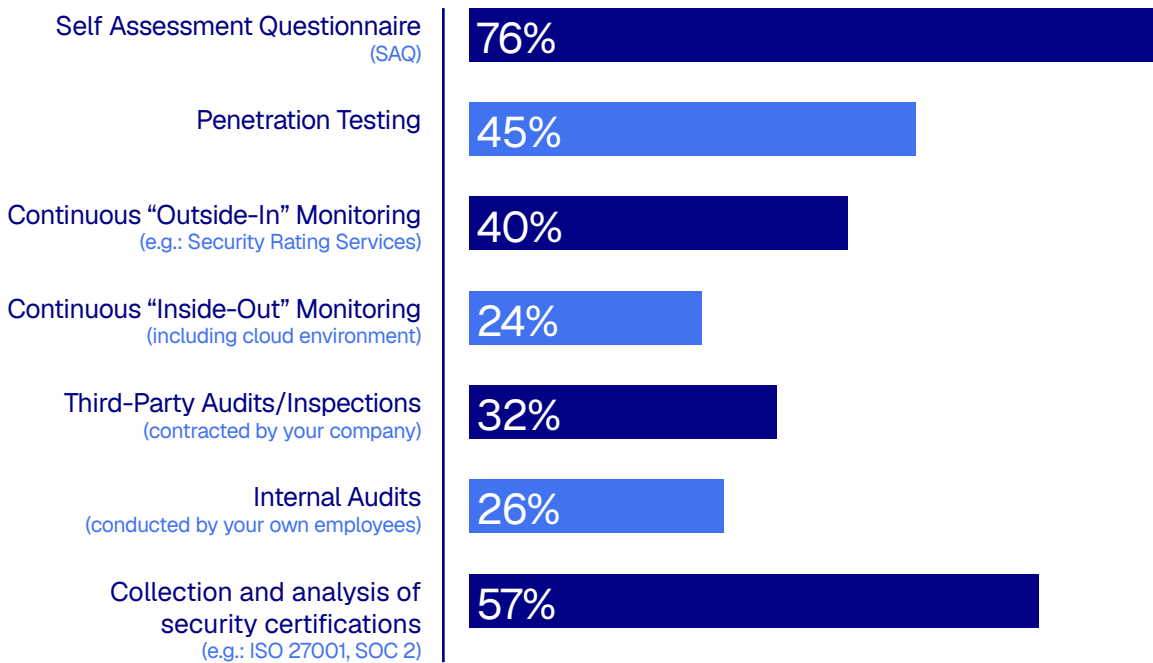
In the 2024 survey, respondents could list all the methods used to evaluate third parties. In the 2025 edition, we limited this question to just three methods, asking participants to select the most important ones.

For this reason, the figures are not directly comparable, and all of them declined compared to the previous year.

It is important to note that the percentages include only those companies that have TPCRM programs.

Key Methods and Tools | 2025

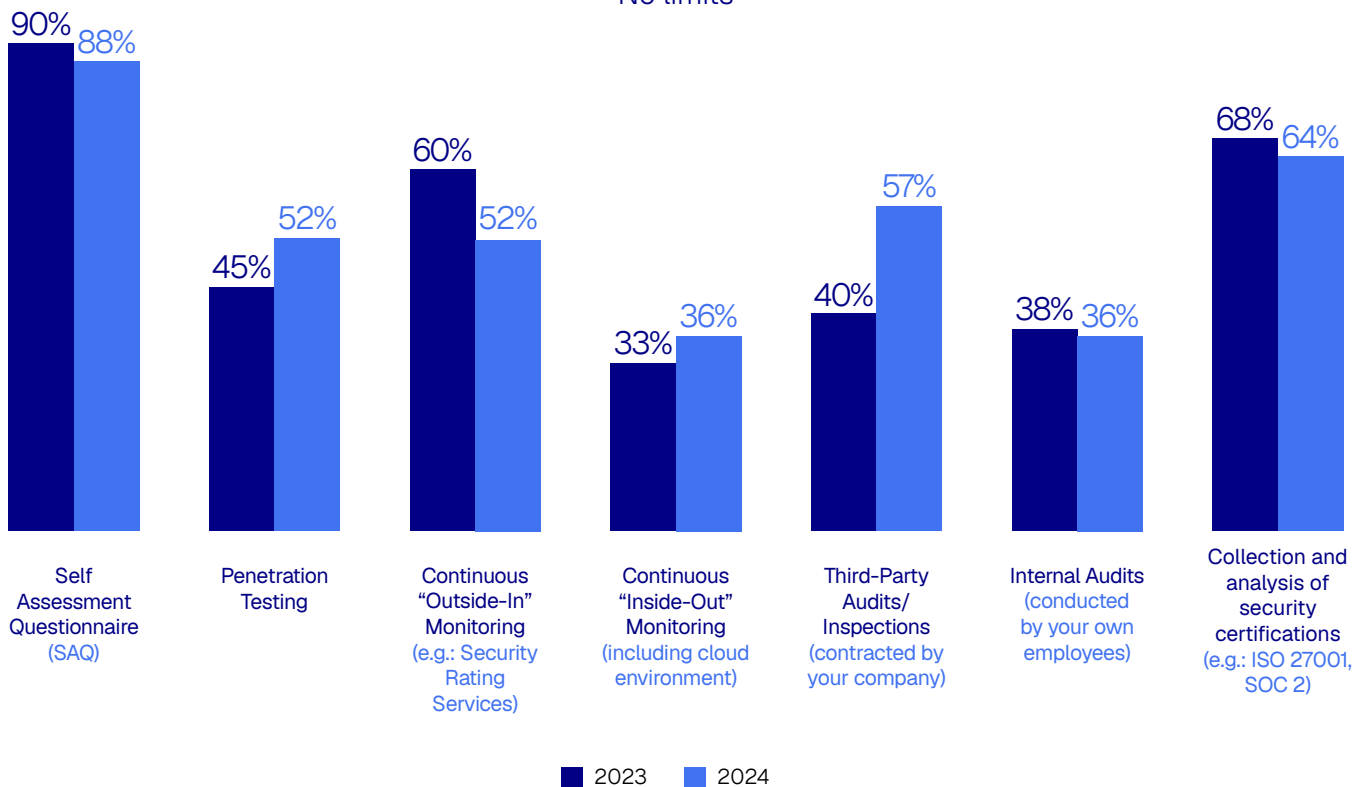
Maximum of 3



Although the question was phrased differently, the overall picture provided by the data is the same: companies prefer to use self-assessment questionnaires and collect security certifications or market reports.

Methods and Tools | 2023/2024

No limits



The choice of tools is not aligned with the priorities identified by professionals, since questionnaires and certifications do not provide the ability to detect threats quickly.

One interpretation of these findings is that companies still approach third-party security primarily as a compliance and governance role, rather than as a cybersecurity effort. Certificates and questionnaires are useful for assessing a third party's overall security posture, but not for detecting, mitigating, and responding to cyber threats.

One of the survey questions, which addresses the frequency of assessments, helps us visualize this. On average, **31% of companies conduct third-party security assessments only once a year**. In other words, visibility into everything that happens throughout the year is quite limited.

However, when we break down the companies into those that use continuous monitoring and those that do not, we see that the ability to increase the frequency of assessments appears to be closely linked to the use of these assessment methods. When a company does not use any type of continuous monitoring, the frequency of assessments drops even further, and 47% of companies perform this work at most once a year.

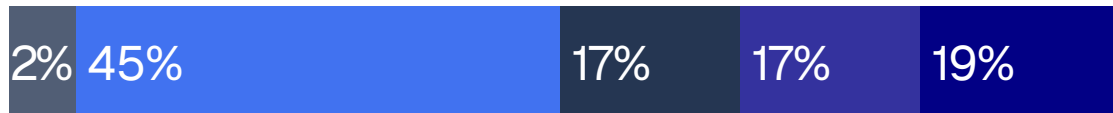
When continuous monitoring is used, the trend reverses: more than half of the companies are able to conduct weekly or more frequent assessments, and only 19% reduce the frequency to once a year.

Comparison of the Frequency of Third-Party Assessments in Companies with and without Continuous Monitoring

With continuous monitoring



No continuous monitoring



Only once
Annually
Every six months
Monthly
Weekly (or more often)

“Snapshot” or “Continuous” Approach

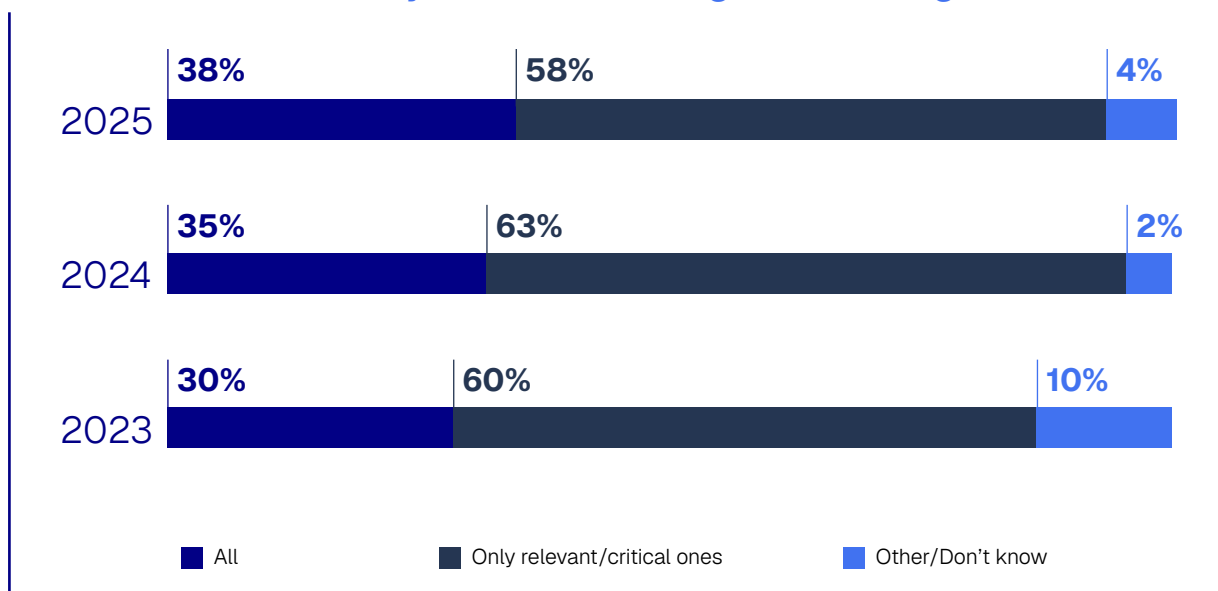
In many cybersecurity scenarios, tools rely on constant monitoring of systems. Firewalls, XDR, and IDS are just a few examples of solutions that require constant operation.

In risk assessments, many mechanisms function as a snapshot of a specific moment. In practice, it's a photo frozen in time that won't be updated until a later point.

Continuous monitoring brings the standard established by cybersecurity tools to third-party risk management. It's like a “movie” that records the company's security posture over time, providing greater visibility into the third party's day-to-day operations and offering a real-world understanding of how security issues are detected and how long it takes to resolve them.

Which third parties are managed

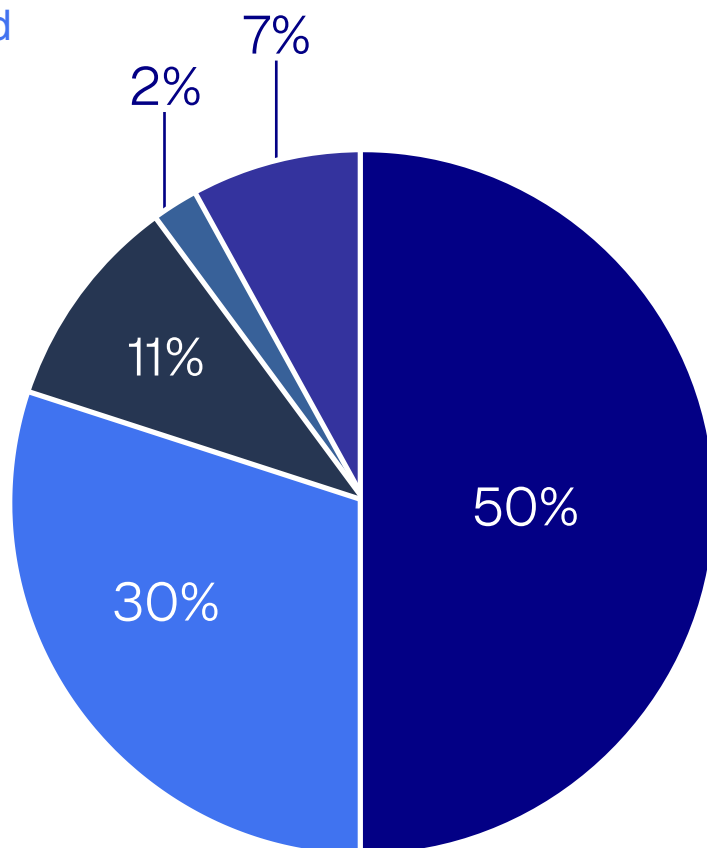
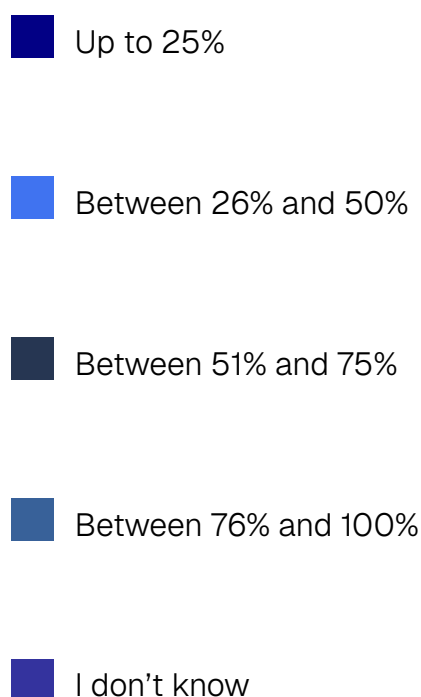
Third Parties in the Cyber Risk Management Program



Since the program's inception, there has been a trend toward an increase in the number of companies managing all their third parties. This trend is positive, as it expands the program's coverage and prevents errors in third-party mapping (where a critical third party is not classified as such and is not assessed in any way).

In fact, half of the professionals who responded to the survey said that at least one-quarter of third parties are critical to the business. For 13%, more than half of the third parties are critical. Since this question was modified in 2025 to ask for a percentage of critical third parties rather than an absolute number, there is no comparison with 2023 and 2024.

Percentage of third parties considered relevant or critical to the business



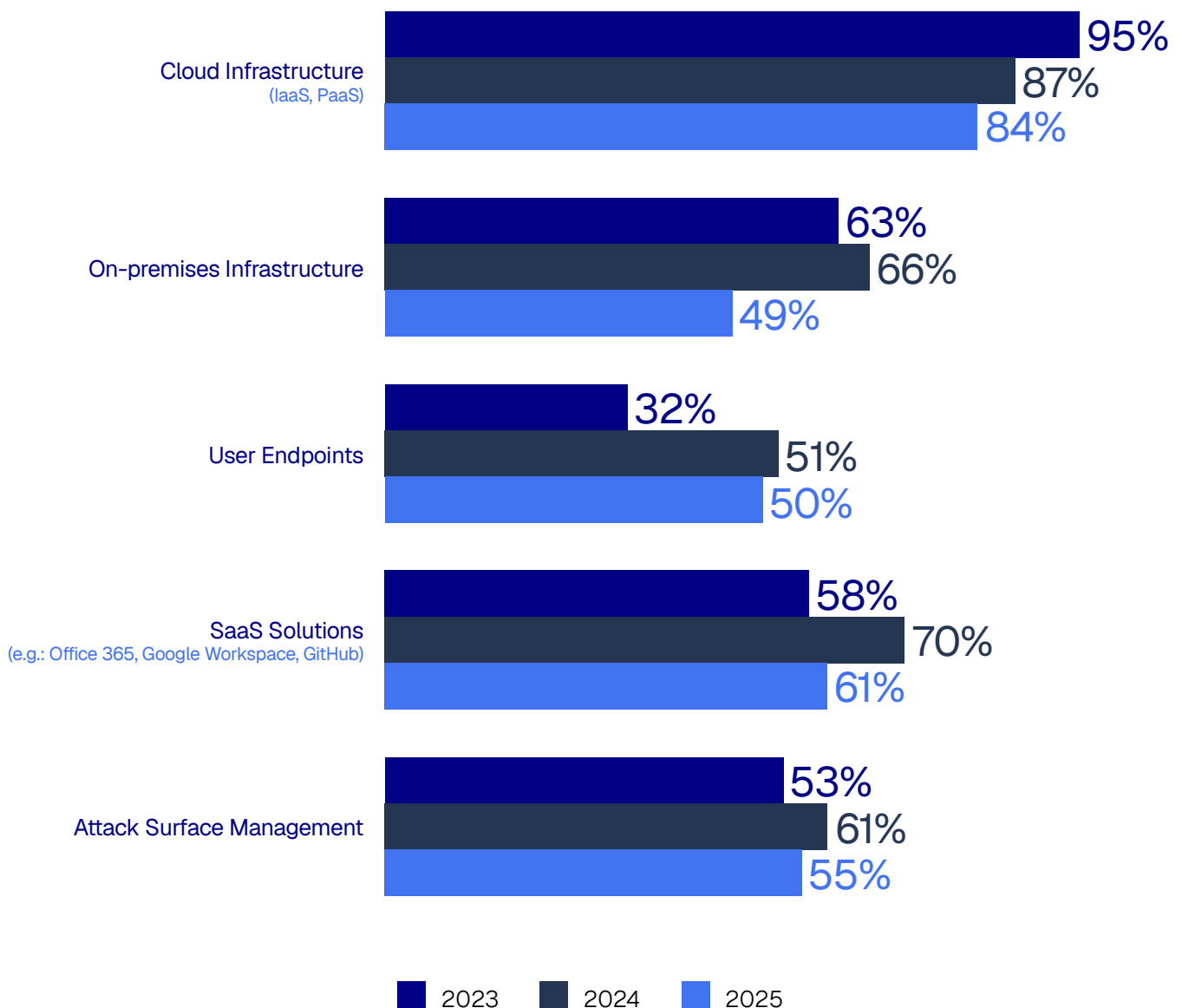
Cloud Visibility and Risks

As in previous years of the survey, we asked participants to assess the most important infrastructures for monitoring risks associated with third parties.

Cloud infrastructure continues to be viewed as the most important, followed by software-as-a-service (SaaS) solutions and attack surface management. The growing concern about user endpoints, which was observed in 2024, was confirmed once again in 2025.



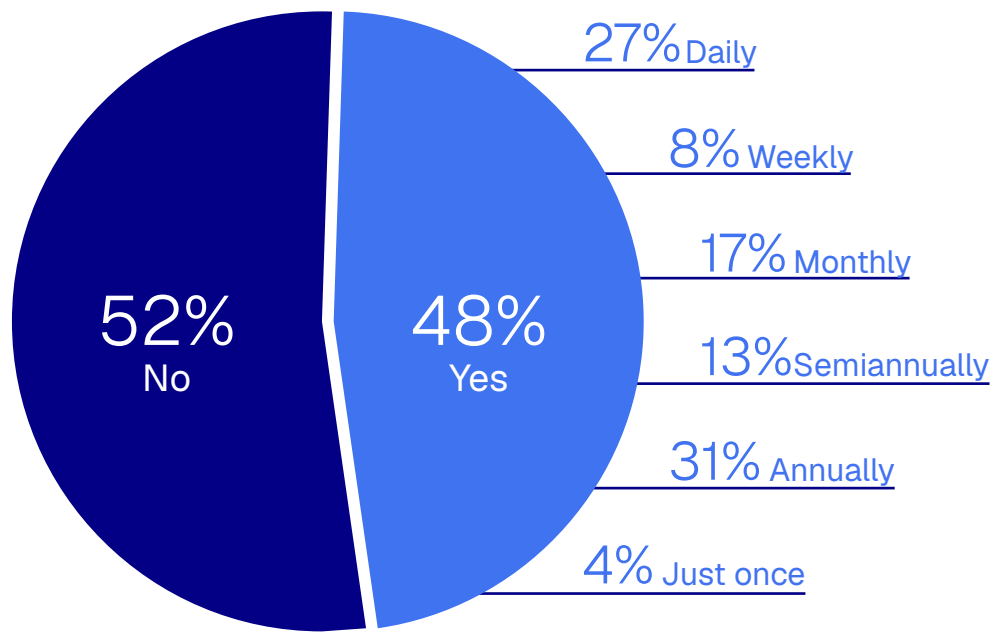
What are the three most important third-party infrastructures to monitor for risks?



In recent years, several incidents involving user endpoints have been documented. The case of Vercel, known as the developer of the Next.js framework, also serves as an example of this. Attackers gained access to Vercel through a SaaS integration with Context.ai, a provider of artificial intelligence solutions. Context.ai, in turn, was compromised when an employee installed software to cheat in the game Roblox on their computer.

When it comes to the cloud, although it is a priority for most, fewer than half of companies have visibility into third-party cloud environments. However, when companies can monitor third-party cloud environments, they do so fairly frequently: 52% of companies with this capability conduct monthly or more frequent analyses, while 27% perform daily monitoring.

Do you have visibility into your third-party cloud environment?
If so, how often do you monitor then?



Security Policies and Incidents

46% Reported at least one security incident in the past 24 months

In this group

76%

Identified that at least one incident originated with a third party.

60%

Cited **financial impact** related to incidents, the second most common impact after operational impact (68%).

Among the survey respondents, just under half of the professionals revealed that their companies had experienced a security incident in the past 24 months. Of these, 68% said the incidents had an operational impact, such as system instability and service interruptions.

The second most common impact was financial (60%), followed by reputational and regulatory (36% each). Participants could select multiple impacts when answering this question.

It is important to remember that there are cases in which security incidents are not reported to the responsible teams or are not even consid-

ered incidents by the departments they affect. The more mature a company is, the greater the likelihood that incidents will be identified and handled correctly.

This means that some companies are constantly experiencing security incidents but are unable to account for the losses they cause or notify customers and partners. Certain third-party risk management methods, such as inside-out monitoring can help third parties facing this challenge detect such incidents and security policy violations.

Governance, Contracts, and Collaboration

3 out of 4 professionals...

...say their companies **include clauses defining liability for security incidents** in their contracts with third parties

...reveal that **there is a shared incident policy** that instructs third parties on communication and response

However, these companies do not belong to the same group.

8% of companies define third-party liability in the contract without sharing an incident policy with their third parties.

As we noted in the section on tools, there are cases where companies' relationships with their third parties are somewhat antagonistic or even hostile, based on the assumption that third parties will take full responsibility for their own security and for any losses resulting from failures or attacks.

This perspective becomes clear when we consider that 8 out of 10 professionals report that their companies hold third parties liable for incidents in their contracts, yet some do not share an incident response policy with them nor provide guidance or training to align the security stances of both organizations.

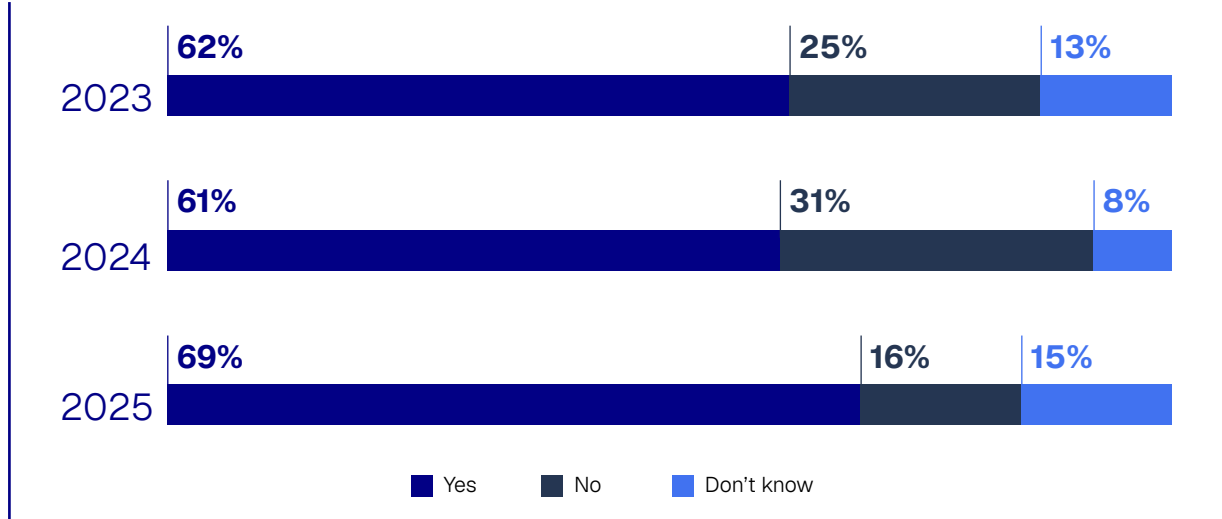
This approach can be risky for some companies. Third parties do not always have incentives to disclose incidents, and in some cases, they would be unable to cover the resulting losses—especially when a contractor is

much larger than the supplier. The media has already documented cases in various countries where the contractor had to bear fines and other liabilities, either because the supplier was unable to pay (in the event of bankruptcy, for example) or because regulators determined that the risk of the operation remained the contractor's responsibility.

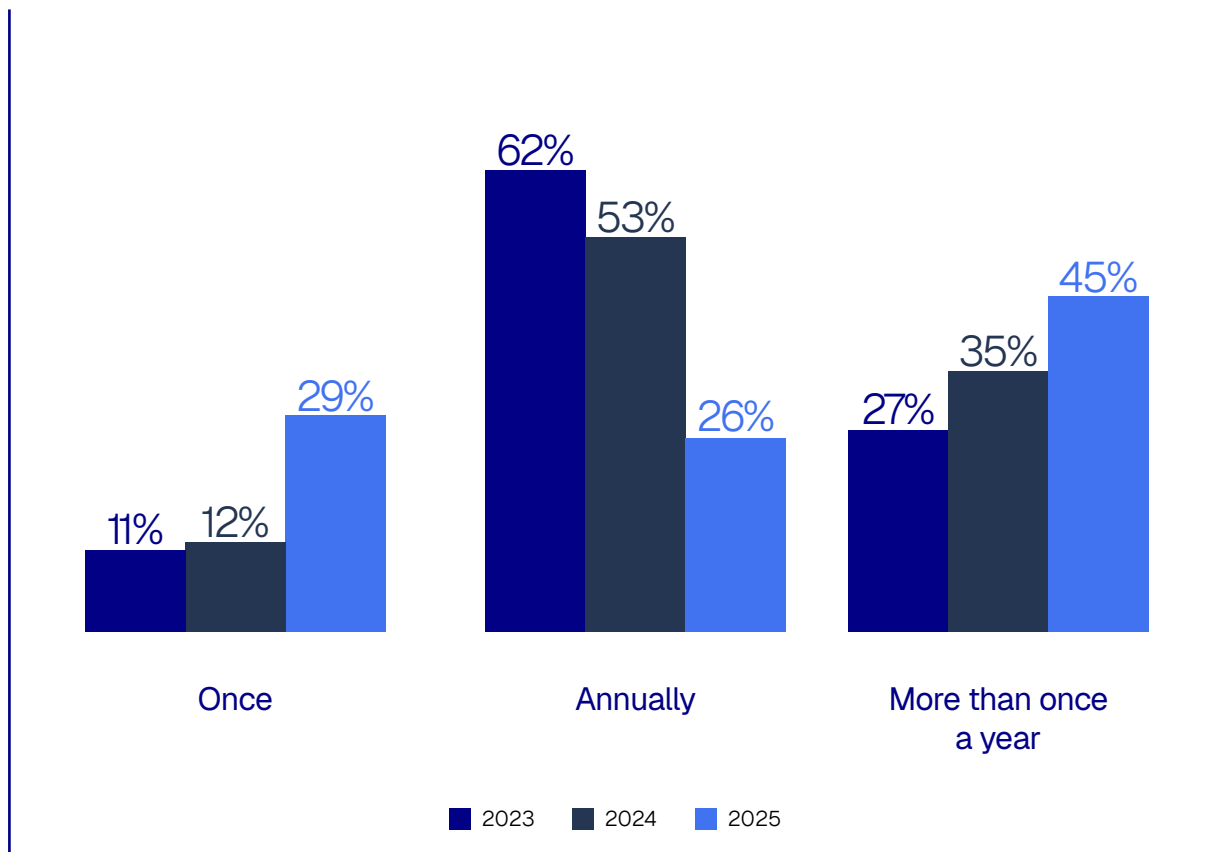
Fortunately, the trend observed in the survey so far indicates that these figures are improving: more companies are collaborating with their third-party vendors by providing safety instructions. Furthermore, these guidelines are being communicated more frequently.

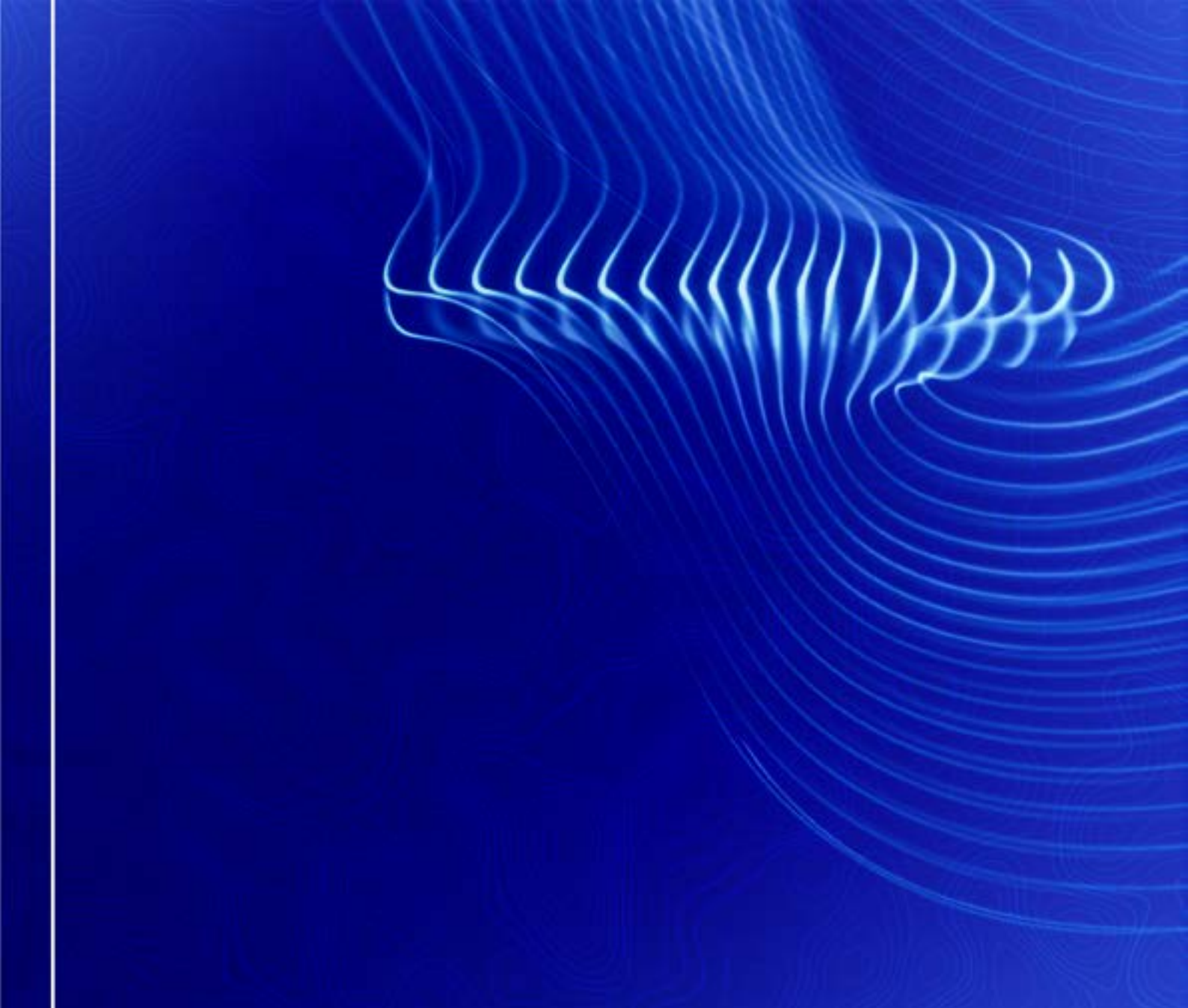


Does your company offer cybersecurity guidance to third parties?



Frequency of training offered to third parties





Our Survey

The 3rd Third-Party Cyber Risk Management Survey was conducted on November 5, 2025, by Tenchi Security. Participants responded individually to the questions using tablets set up for this purpose during the Tenchi Conference, our event focused on third-party cyber risk management.

Participants received no compensation for taking part in the survey. To encourage voluntary participation, interested individuals were informed that completed questionnaires would result in donations to the Support Group for Adolescents and Children with Cancer (<https://graacc.org.br> (GRAACC), a nonprofit organization specializing in pediatric oncology. Tenchi Security has been supporting GRAACC for over three years.

As in previous editions, the survey was designed to better understand how companies manage the risks associated with their suppliers, service providers, business partners, and other third par-

ties that are in some way linked to their information technology infrastructure and digital assets. However, some aspects of the survey were modified. We reduced the number of questions to about 30 and changed the way data was collected. Instead of having interviewers approach our conference participants, we facilitated voluntary participation through kiosks.

For some questions, the response options were refined to better reflect the reality of businesses. In cases where changes were made, we did not draw comparisons with previous editions. Consequently, all charts containing data from 2023 and 2024 are based on questions that retained the same structure.

Research Objective

To explore how large organizations are addressing the issue of third-party cyber risk management in Brazil and to identify the main challenges and opportunities.

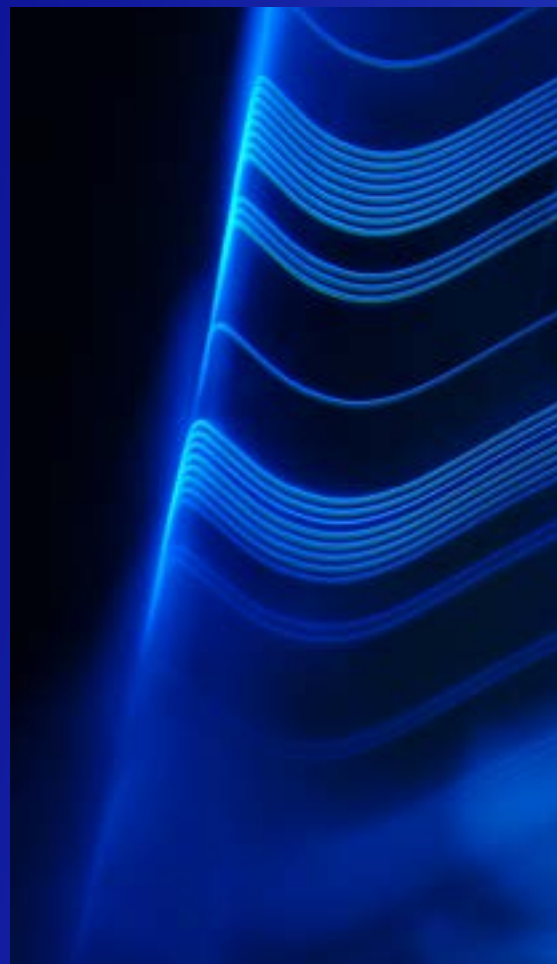
Transparency and Sampling

Sample _____

136 respondents (total)

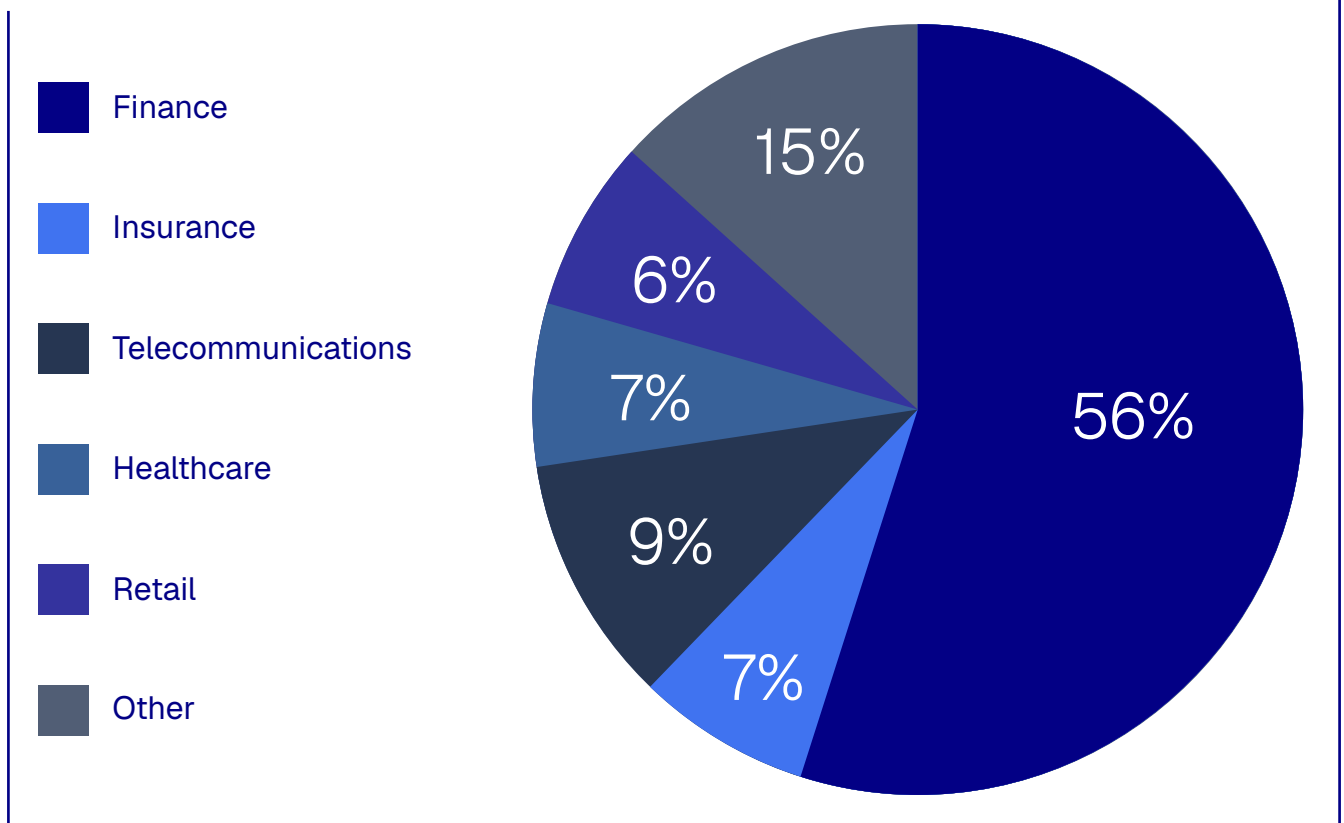
120 included (Brazil)

16 responses were collected outside Brazil, but we did not include them in this report. The charts regarding respondent profiles refer to the 120 respondents used in all charts in the report.

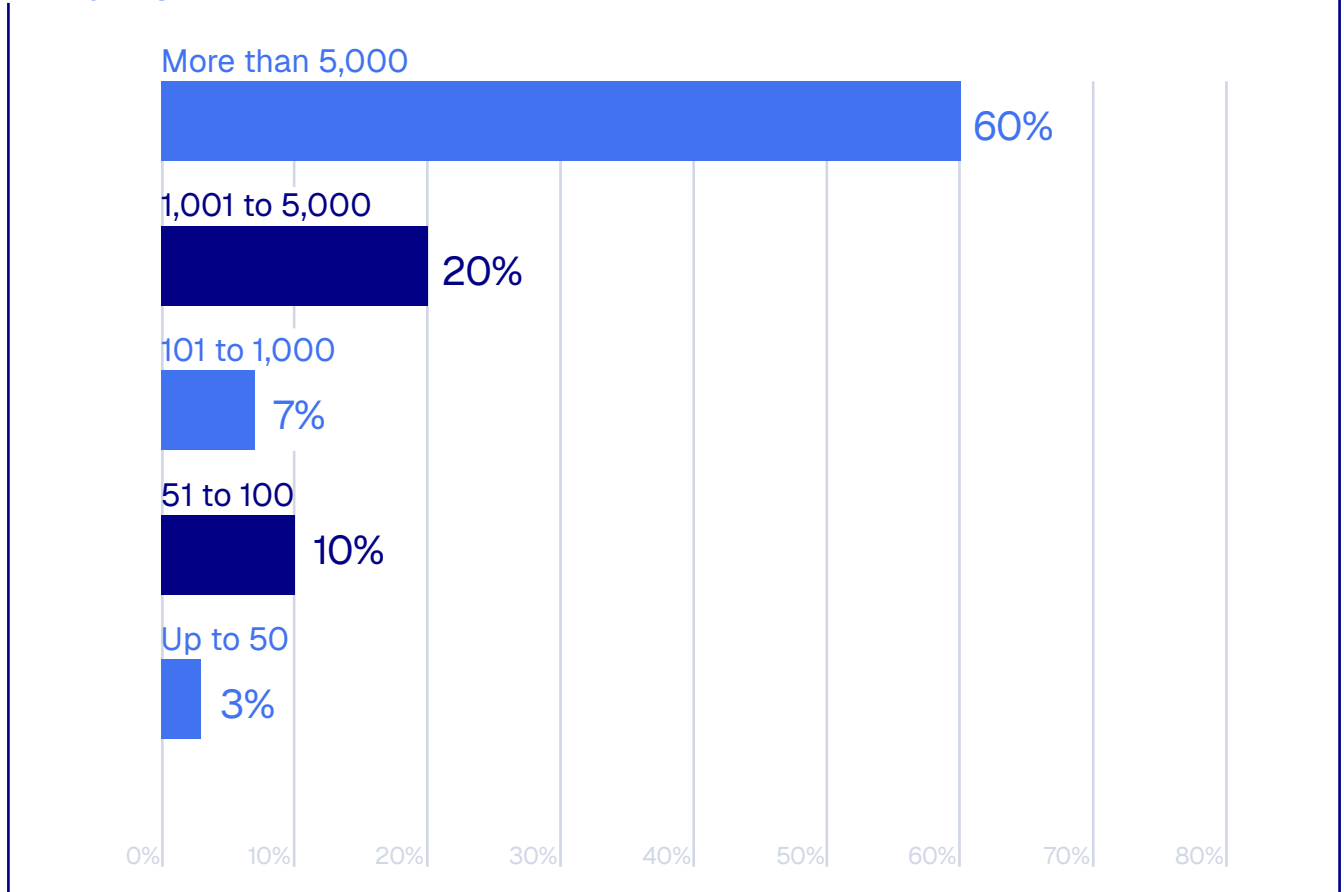


Company Profile

Industry

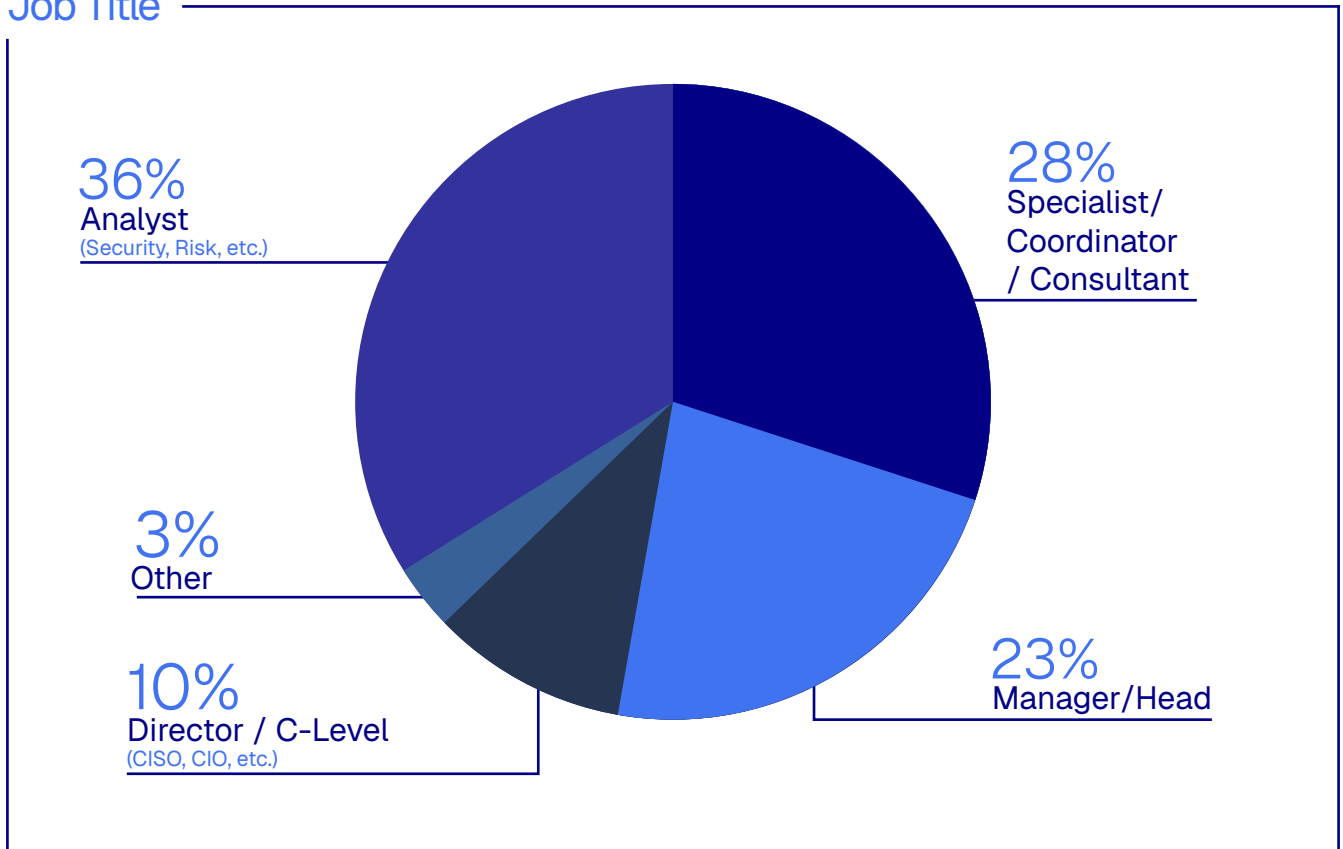


Company size (number of employees)



Respondent Profile

Job Title



Professional Field

