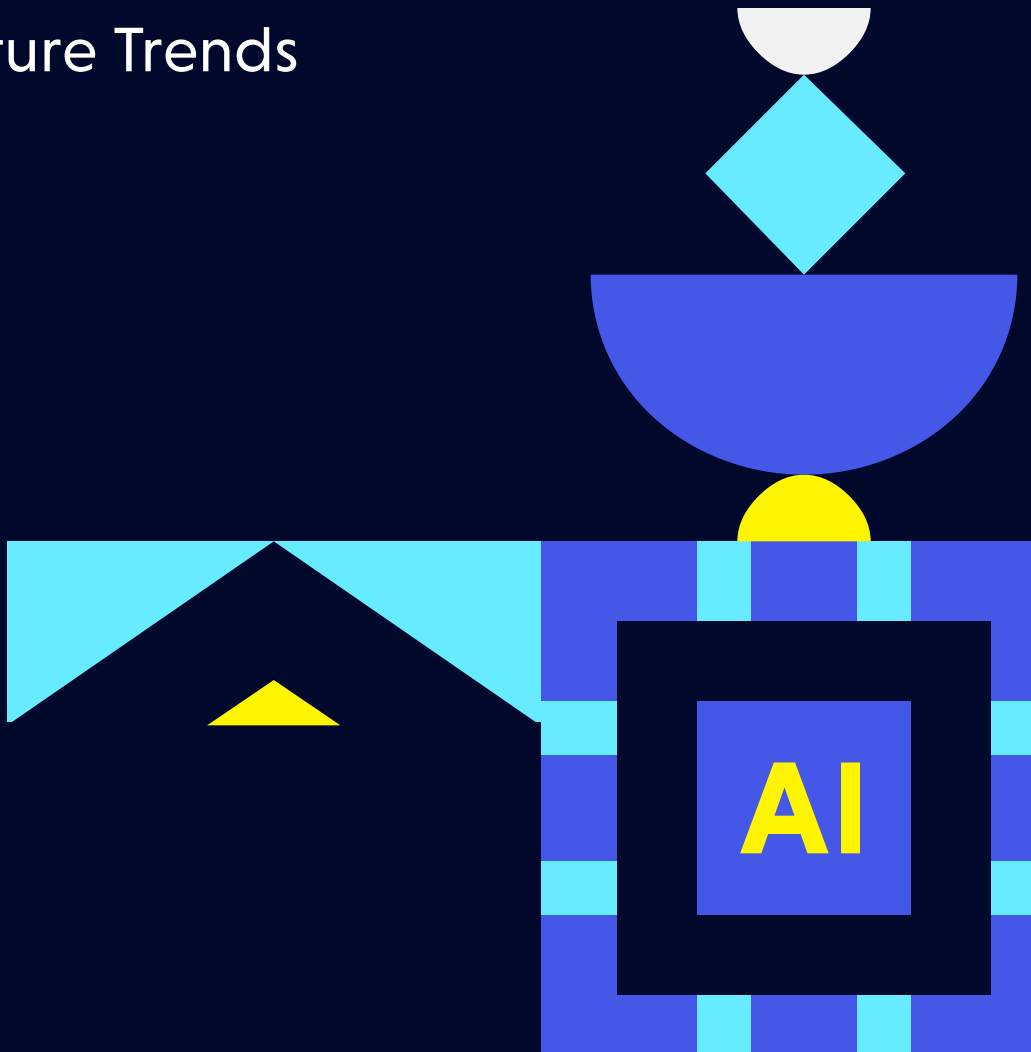
VISO TRUST

REPORT

2024 State of Third-Party Risk Management

AI's Impacts & Future Trends



Executive Summary

Introduction

Background

In today's cloud-first business landscape, the urgency for an adaptive Third-Party Risk Management (TPRM) approach is heightened by a significant shift. Businesses are swiftly moving towards a future where 100% of their digital ecosystem is composed of third-party vendors and partners.

This whitepaper addresses the critical need to modernize TPRM practices in response to this evolution, recognizing that traditional methods, including questionnaire-based assessments, fall short as businesses become entirely reliant on external contributors. By exploring innovative solutions like artifact-based assessments with AI and automation, this whitepaper provides a **timely** and **comprehensive** strategy for businesses navigating the challenges of a digital landscape shaped entirely by third-party relationships. Embracing these advancements in TPRM enables organizations to **fortify cybersecurity, ensure compliance, and foster trust** in their digital operations, positioning themselves for resilience and sustainable growth in a landscape where third-party relationships are **integral to success.**

TPRM Tip

Strengthen your cybersecurity strategy by proactively managing third-party risks. As reliance on external vendors increases, TPRM becomes essential to address vulnerabilities like data breaches and compliance issues. Identify, assess, and mitigate risks to ensure success in today's globalized and technologically driven business landscape.

Current and evolving challenges in TPRM

TPRM is a crucial component of contemporary business strategies, addressing the increasing reliance on external partners. It involves identifying, assessing, and mitigating risks associated with third-party relationships, such as vendors and service providers. With globalization and technological advancements, organizations are exposed to various vulnerabilities, including data breaches and compliance issues.

The traditional method of relying on questionnaires for risk assessments is proving inadequate, as findings show that up to 75% of vendors refuse to participate or fail to do so in a timely manner. With cyber risk ratings, as much as 90% of high severity findings can be false positives making them an invalid determinant of risk. Public data limitations further hinder effective risk evaluations. To adapt to these challenges, organizations are exploring innovative approaches like artifact-based assessments, incorporating AI, and automation. **These advancements enhance accuracy, efficiency, and depth in risk management practices.**

Given the evolving regulatory landscape and growing cybersecurity threats, a proactive and comprehensive TPRM strategy is essential. Organizations that embrace these changes and leverage advanced technologies are better equipped to navigate risks, build resilience, and foster trust among stakeholders in an era where third-party relationships play a pivotal role in business success.

TPRM Tip

Traditional questionnaires, ratings, and exchanges are unreliable and inefficient. Modern solutions using AI and analyzing real data (artifacts) offer a more comprehensive and accurate picture of third-party risk, saving time and resources while ensuring better risk management.

Purpose of the Whitepaper

01 Addressing the current gaps and evolving trends in TPRM

02 Future predictions in TPRM

The purpose of this whitepaper is to highlight the evolving landscape of TPRM by **exposing and examining some of the gaps and shortcomings of the current state of data gathering and assessments, and then** delving into key trends, predicting future developments, and providing invaluable insights for security leaders, IT, and tech executives, as well as security practitioners. As businesses increasingly rely on third-party vendors and partners, traditional risk assessment methods prove insufficient.
The whitepaper explores innovative approaches, such as artifact-based assessments with AI and automation, offering a strategic guide to navigate challenges and capitalize on opportunities. With a focus on both current trends and future predictions, this resource is designed to empower professionals involved in mitigating third-party risk, fostering resilience, and ensuring the security of digital ecosystems.

The Current Landscape of Third-Party Risk Management

Overview of TPRM

Definition of TPRM

In the realm of TPRM, a meticulous analysis evaluates potential risks from engagements with external entities, including vendors, suppliers, and business partners. This strategic approach involves proactive due diligence to identify and mitigate risks that could disrupt organizational operations. TPRM plays a pivotal role by fortifying operational resilience, ensuring consistent service to customers, and acting as a critical defense against sophisticated cybersecurity threats. In today's complex business environment, TPRM positions organizations to navigate challenges deliberately, fostering a secure, resilient, and sustainable operational landscape.

TPRM Tip

Don't be reactive, be proactive! Conduct thorough due diligence on all third-party partners to identify and mitigate risks before they impact your business.

> Identifying and collaborating with key stakeholders is paramount when establishing a robust TPRM program.

Key stakeholders and their concerns in TPRM

Identifying and collaborating with key stakeholders is paramount when establishing a robust Third-Party Risk Management program. Internal stakeholders, including executives (CEO, CFO, CIO, COO, CISO, etc.), general counsel, board members, internal auditors, and personnel from procurement, finance, IT, information security, legal, and compliance departments, play integral roles in shaping TPRM workflows. Their involvement ensures alignment of people, processes, and technologies to create an effective program tailored to the organization's needs.

Externally, critical stakeholders in the development of a TPRM program encompass vendors, regulators, and customers. Inclusion of these external entities is vital for comprehensive risk assessment and management, as their perspectives and requirements significantly influence the program's success. By actively engaging both internal and external stakeholders, organizations can establish TPRM programs that not only meet regulatory compliance but also address the specific risks associated with their industry, operations, and partnerships. This collaborative approach ensures a holistic and effective TPRM strategy that safeguards the organization and fosters trust among stakeholders.

TPRM Tip

Don't go it alone! Engage both internal (executives, departments) and external (vendors, regulators, customers) stakeholders in your TPRM program. Their insights and collaboration ensure a comprehensive, tailored, and effective strategy that meets compliance, addresses specific risks, and fosters trust for all involved.

Challenges in Traditional Approaches

As organizations navigate the complex landscape of TPRM, a critical evaluation of traditional approaches **reveals inherent limitations**. Manual/internal spreadsheet-based questionnaires, often executed on platforms like Google Sheets and Excel, demand substantial effort from a small internal team, proving time-consuming and lacking real-time monitoring capabilities, contextual awareness, or standardized risk determinations. Survey-based Vendor Risk Management (VRM) solutions, including well-known platforms like OneTrust, ProcessUnity, and Prevalent, present challenges such as extensive time and labor requirements, complex implementations, and difficulties in management. In all cases, questionnaire responses present **significant vendor bias**, engendering a **significant false sense of security.**

01 Manual spreadsheet and questionnaires

Manually updating spreadsheets, hosted forms, or other homegrown solutions requires significant effort and resources by a small expert internal team, which is time-consuming and doesn't account for continuous or real-time monitoring that scales with changing regulatory or business requirements.

02 Risk exchanges

Static repositories prove costly, slow, and lack context, resulting in poor vendor adoption.

03 Cyber risk ratings

External/network scanning of vendors introduces challenges such as irrelevant or inaccurate data, and the necessity for supplementary survey-based processes.

04 Procurement or governance, risk, and compliance (GRC) tools

IT GRC and VRM tools offer some visibility into vendor management and onboarding, but fall short in continuous vendor monitoring and risk mitigation. This approach is plagued by poor quality data, low vendor participation rates, and slow, labor intensive processes due to relying solely on complex questionnaire-based workflows.

TPRM Tip

Modernize your TPRM for efficiency and effectiveness!

Findings

The following findings are based on an independent analysis leveraging the VISO TRUST platform and information provided from CISOs, as well as security and TPRM professionals across a broad set of industry verticals, including financial and professional services, healthcare, software, and technology. The VISO TRUST platform contains profiles of more than 2.4 million companies, recognizes more than 25 security frameworks, and leverages hundreds of different types of source artifacts such as SOC 2 reports, penetration test reports, and cybersecurity policies. **These data points further demonstrate challenges we see in current TPRM approaches and solutions:**

Questionnaire-based assessments are NOT working – low vendor adoption rates and poor quality data

Traditional TPRM methodologies, particularly those reliant on questionnaires, are encountering significant impediments in today's evolving cyber and threat landscape. One major issue is the reliance on questionnaire-based assessments, with a growing number of vendors refusing to participate.

A staggering 75% of vendors are now refusing to fill out traditional questionnaire-based assessments or providing them too late in the selection and procurement process, highlighting a substantial breakdown in this conventional approach.

In addition to response rates, the value of questionnaires is significantly undermined by biased responses within. Respondents at vendor organizations are typically highly incentivized to provide positive responses, leading to a false sense of security among customer organizations.

Public data is insufficient for meaningful assessments: **only 6% of vendors can be assessed on public data alone.** Data sources, such as questionnaire-based systems augmented by cyber risk ratings or vendor directories of public data, provide a partial and potentially misleading picture.

Public data limitations

Public data limitations further impede meaningful risk evaluations. The inadequacy of public data for meaningful risk assessments is evident, with a **mere 6% of vendors deemed accessible** through this channel alone.

These challenges underscore the need for a paradigm shift in TPRM methodologies, prompting exploration of innovative approaches like artifact-based assessments to address the shortcomings of traditional practices.

This ineffectiveness of current TPRM approaches underscores the **urgent need for a paradigm shift** in TPRM methodologies. The limitations identified in traditional approaches emphasize the significance of transitioning to more efficient, accurate, and automated methods, such as artifact-based assessments. By leveraging advanced technologies, organizations can overcome the shortcomings of manual and survey-centric practices, ensuring a comprehensive, streamlined, and effective TPRM strategy that aligns with the evolving demands of the digital era.

False positives in high severity findings among cyber risk ratings

Ratings, once considered a determinant of risk, are plagued by a **98% invalidity rate in reports.** Context, complex dependencies, component customization, misattribution (dynamic environments), over aggressive scanning, limited visibility—these challenges underscore the need for a paradigm shift in TPRM methodologies, prompting exploration of innovative approaches like artifact-based assessments to address the shortcomings of traditional practices.

75%

of vendors are now refusing or significantly delaying traditional questionnaire-based assessments

98%

invalidity rate in cyber risk ratings reports

Shifting Paradigm: The Future of AI & Dynamic Artifact-Based Assessments

The evolving landscape of TPRM demands a fundamental shift in methodologies to address the shortcomings of traditional practices and harness the power of advanced technologies like AI. As highlighted by recent challenges in TPRM, including low vendor adoption rates and false positives in severe findings, there's an **urgent need for organizations to embrace innovative approaches** such as artifact-based assessments. In sharp contrast to the industry findings on traditional methods, modern companies leveraging AI and artifacts for TPRM have been able to achieve **near 100% coverage** of their third-party populations while delivering **500% more true positive findings.**

The emergence of AI marks a significant turning point in risk management, offering not just a tool but a strategic collaborator in navigating the complexities of third-party relationships. AI-driven risk management extends beyond conventional functions, enabling organizations to assess and mitigate third-party risks in novel ways while overcoming process and data assessment bottlenecks.

AI and artifact based assessment not only provide accurate data at scale, they save critical time and resources, positioning companies to better serve the business while creating space for rational risk decisions based on quality data. Companies across industry verticals have moved from average assessment times of **60 to 90 days to five to eight day**s with **96% fewer human hours spent** by switching from questionnaire-based assessments to AI and artifacts-based assessments. This means business stakeholders are making more informed decisions about risk earlier in the procurement cycle, and allowing expert resources to be freed from busy work and refocused on consulting with the business, which has led to **75% fewer risk exceptions filed.**

Amidst this AI-driven transformation, principles such as trust, fairness, accessibility, and vigilant governance remain paramount. As organizations navigate this evolving landscape, meticulous consideration of the interplay between human expertise and AI capabilities is essential in driving cutting-edge innovations in risk management.

By leveraging dynamic artifact-based assessments empowered by AI, organizations can not only **mitigate risks more effectively, but also streamline processes**, ensuring a comprehensive and adaptive TPRM strategy aligned with the demands of the digital era. As pioneers in AI-driven risk management, VISO TRUST continues to push the boundaries of possibility, shaping the future of TPRM and beyond.

TPRM Tip

Traditional TPRM methods struggle with low adoption rates and inaccuracies. AI offers a groundbreaking solution, not just a tool, for tackling complex third-party risks and overcoming limitations in data assessment. Through AI-powered artifact-based assessments, organizations can mitigate risks more effectively, streamline processes, and adapt their TPRM for the digital age.

AI and artifact-based assessment delivers **98%** response and completion rates with **500% more true positive findings**

AI-powered assessment reduces average time to assess from **60 to 90 days** to **five to eight days**

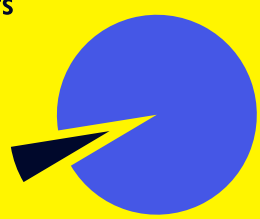
The State of Third Party Risk Management 2024

Questionnaires are not working

Up to **75%** of vendors refuse to fill out questionnaires

Public data is not enough for meaningful risk assessments

Only **6%** of vendors can be assessed on public data alone



Ratings are an invalid determinant of risk

As much as 98% of reports are invalid

90% of high severity findings are false positives

AI-powered assessments empower security teams to save time and resources

Questionnaire-based assessments take **60-90 days**

VS.

AI-powered artifact-based assessments take **5-8 days**

96% fewer human hours spent

$2,400 dollars saved in labor cost

AI-powered artifact-based assessments deliver exeptional results

Near **100%** vendors assessed

98% completion rate

AI in TPRM means greater speed and accuracy, and more risk mitigation

25x more high risk vendors caught

75% fewer exceptions filed

500% more true positive findings

About the author

Paul Valente

Paul Valente is the CEO & Co-Founder of **VISO TRUST**. He is also a former CISO and built successful security teams and programs at several companies including LendingClub, Restoration Hardware, and ASAPP. Paul's security and risk programs have been vetted by hundreds of Fortune 1000 companies and his leadership and expertise has transformed the TPRM programs of forward-thinking companies around the world.

Connect with Paul Valente

linkedin.com/pauldvalente

paul@visotrust.com

About VISO TRUST

VISO TRUST is an emerging cybersecurity company at the forefront of third-party cyber risk management.

VISO TRUST is an emerging cybersecurity company at the forefront of third-party cyber risk management. The VISO TRUST Platform automates at scale and enables teams to access actionable vendor security information in minutes. **VISO TRUST** delivers fast and accurate intelligence needed to make informed cybersecurity risk decisions at scale for hyper-growth tech companies to Fortune 500 enterprises.

For more information, visit www.visotrust.com