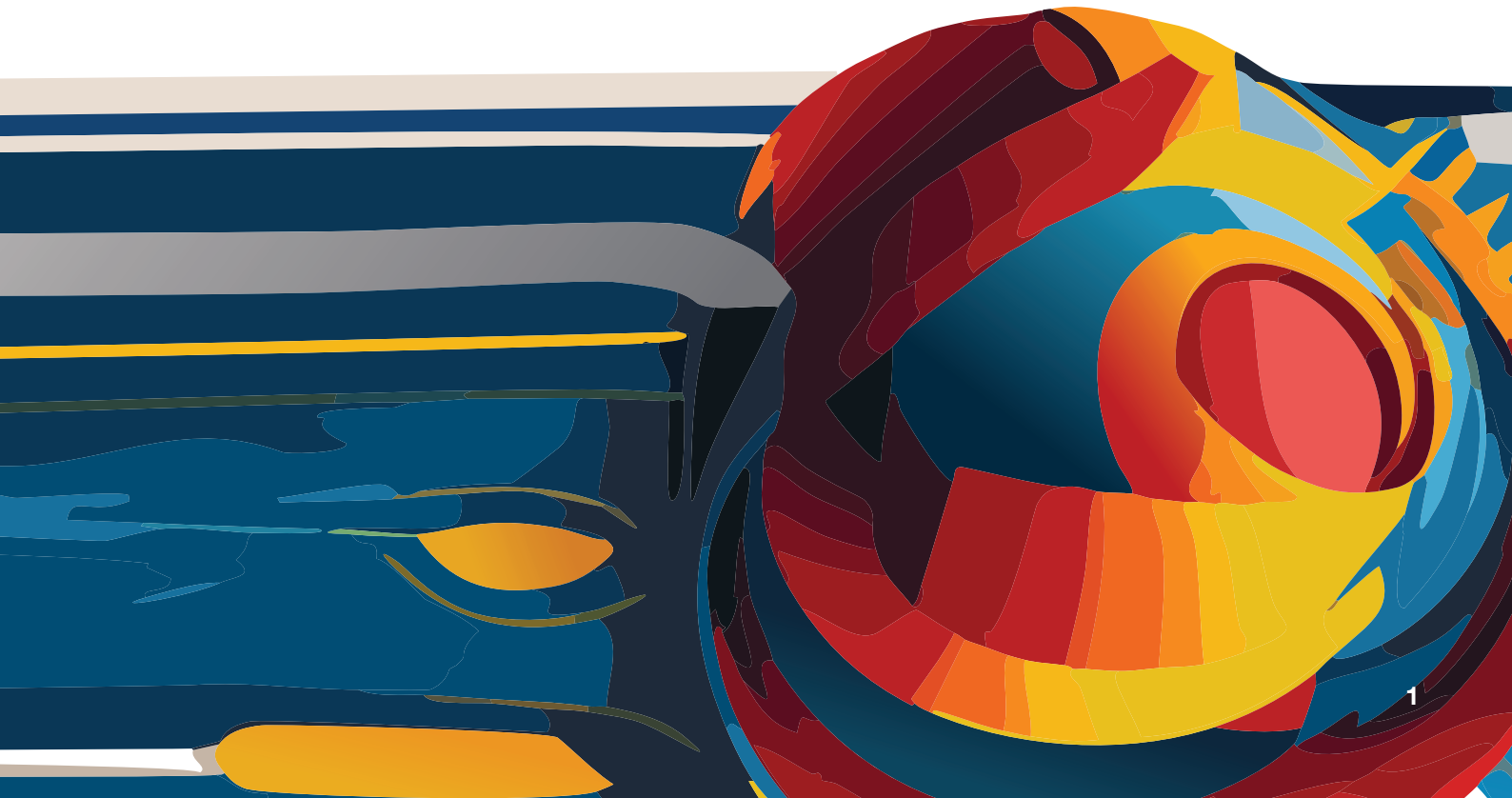
The Essential Guide to

Modern Third-Party Risk Management

whistic

Table of Contents



Introduction:
The Current State of Vendor Risk Management

Let's start with some numbers.

In our 2024 Third-Party Risk Management Impact Report, we surveyed more than 500 Information Security and Risk Management decision-makers. We found that:

- **68%** of respondents have experienced a recent breach (vs. 55% in 2023)
- **88%** report this breach was the result of a third-party vulnerability (vs. 77% in 2023)
- **50%** of companies work with 100 or more vendors (vs. 38% in 2023)

In short: more vendors, greater risk, and more breaches.

New kinds of threats and more sophisticated attackers are certainly factors in these trends. But it's also clear that the current approach to third-party risk management (TPRM) through questionnaire-based vendor assessments simply isn't working.

We call this the legacy approach to TPRM. In the legacy approach, companies devote finite time and headcount to highly manual, administrative tasks. This forces them to cut corners on the number and depth of their assessments and leaves few resources left over for actually mitigating risk. Legacy TPRM just can't keep up with accelerating third-party risk.

But Modern TPRM can.

Modern TPRM builds on the strong foundational elements of traditional risk management and integrates innovative Artificial Intelligence capabilities to make the process faster, more insight-rich, and more effective. Modern TPRM means you can perform more assessments, in greater detail—and save resources for actually mitigating risk and keeping your business more secure.

In short: better assessments, faster assessments, and less risk.

Ready to leave Legacy TPRM behind? You're in the right place.

Risky Business:
The Impact of Legacy TPRM

The majority of organizations conduct questionnaire-based vendor security assessments. This is a highly manual process: sending the questionnaire, the back-and-forth with the vendor, and sifting through information line-by-line—if there is a response at all.

Unintended consequences of Legacy TPRM:

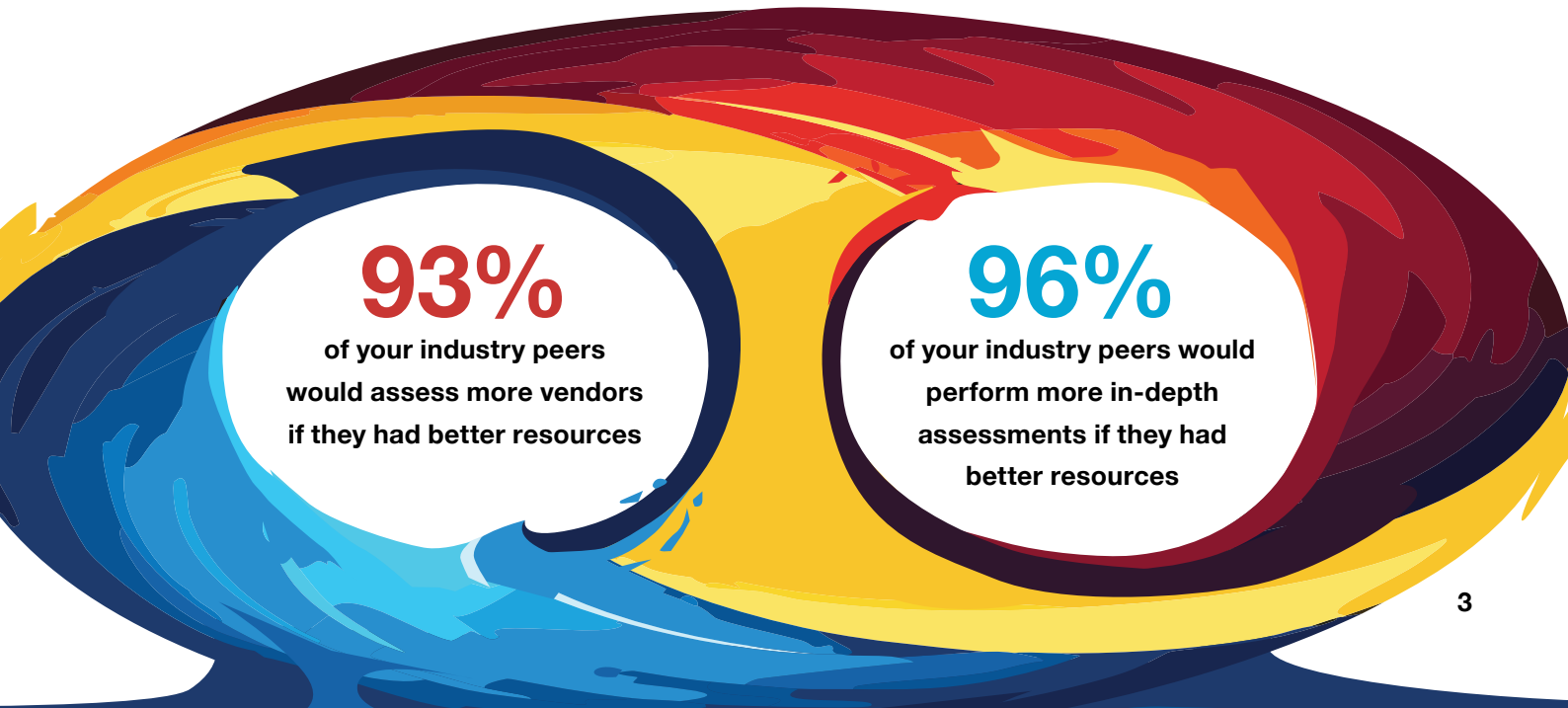
This approach has several important implications for the business:

- **Doesn't scale**—Manual processes make it impossible to keep up with increased demand.
- **Time and resource-consuming**—The bulk of your finite capacity goes to administrative tasks.
- **Longer purchasing process**—These delays mean it takes more time and energy to get business units the valuable tools they need.
- **Inability to leverage existing vendor info/ documents**—When your process is built entirely around questionnaire responses, it becomes difficult to incorporate a wider variety of security insights into your decision-making.
- **Vendor fatigue**—Vendors receive dozens, hundreds, or even thousands of questionnaire requests, and their own manual processes make it impossible to respond to every individual questionnaire, so you may never get all the answers you need.

And the biggest consequence of all:

More risk!

When resources are stretched to the breaking point by manual, administrative tasks, the actual work of assessing and mitigating risk loses out. In our 2024 TPRM Impact Report, we learned that the vast majority of organizations simply can't do the number of assessments or the quality of assessments they know they should. The result? They take on unnecessary, avoidable risks.



More, Better, Faster:
Making the Move to Modern TPRM

Modern TPRM shifts the focus away from administrative tasks and toward risk mitigation, so you can more effectively allocate your existing resources to higher-impact activities. The key outcomes of Modern TPRM are:

- **More assessments**—Stop cutting corners on the number of vendors you assess and taking on unnecessary risk.
- **More effective process**—Improve the efficiency and pace of your TPRM.
- **Reduce costs**—Greater efficiency reduces waste, and the increased pace of assessments mean your team can accomplish more without additional headcount.
- **More in-depth insights**—Access a wider range of security data to make smarter purchasing decisions.
- **More risk mitigation**—The time and resources saved on manual assessments can be applied to actually managing risk (instead of managing emails, links, and spreadsheets).

Brass tacks: How does Modern TPRM actually work?

Modern TPRM combines foundational processes, a seamless exchange of richer data sources, and the automation and analysis possible through a powerful AI engine to evolve the questionnaire-based legacy approach. Here's how the pieces fit:

Step 1: Utilize all available security information

Legacy TPRM is built to only work with specific questionnaire responses. But Whistic survey data shows that 72% of vendors proactively share some or all of their security posture publicly, while 95% of companies say this pre-existing information is enough to start an assessment. Modern TPRM makes it easier to collect, store, and and access these data types so you're not over-reliant on questionnaires.

Step 2: Reduce friction in your processes

TPRM is growing in complexity as the reliance on vendors increases; many companies are housing vendor information in numerous systems, including multiple teams in the process, and require more reporting metrics for senior leaders. Modern TPRM streamlines these workflows, centralizes information, and improves access management and controls.

Step 3: Integrate AI to automate assessments

AI is the single biggest development impacting our industry, and it is an essential part of Modern TPRM. AI capabilities are tuned to understand the specific security and compliance posture of you and your vendors. This, in combination with Large Language Models (LLMs) and generative AI, makes it possible to automate the assessment process and get detailed answers to security questions using pre-existing documentation.

If You Build It:
The Core Pillars of Modern TPRM

Vendors are willing to to share the security information you need to assess them; it just may be in the form of a SOC 2 or other document instead of a completed questionnaire. This adds the manual step of poring through the documentation to find the answers yourself. Modern TPRM gives you the processes and tools to capture and utilize that information in a fraction of the time. It starts with the foundational building blocks of a mature risk-management program, including:

Defined Workflows: Clearly defined roles and responsibilities coordinating all business units involved in the TPRM process, including InfoSec, IT, Procurement, Risk, and Compliance.

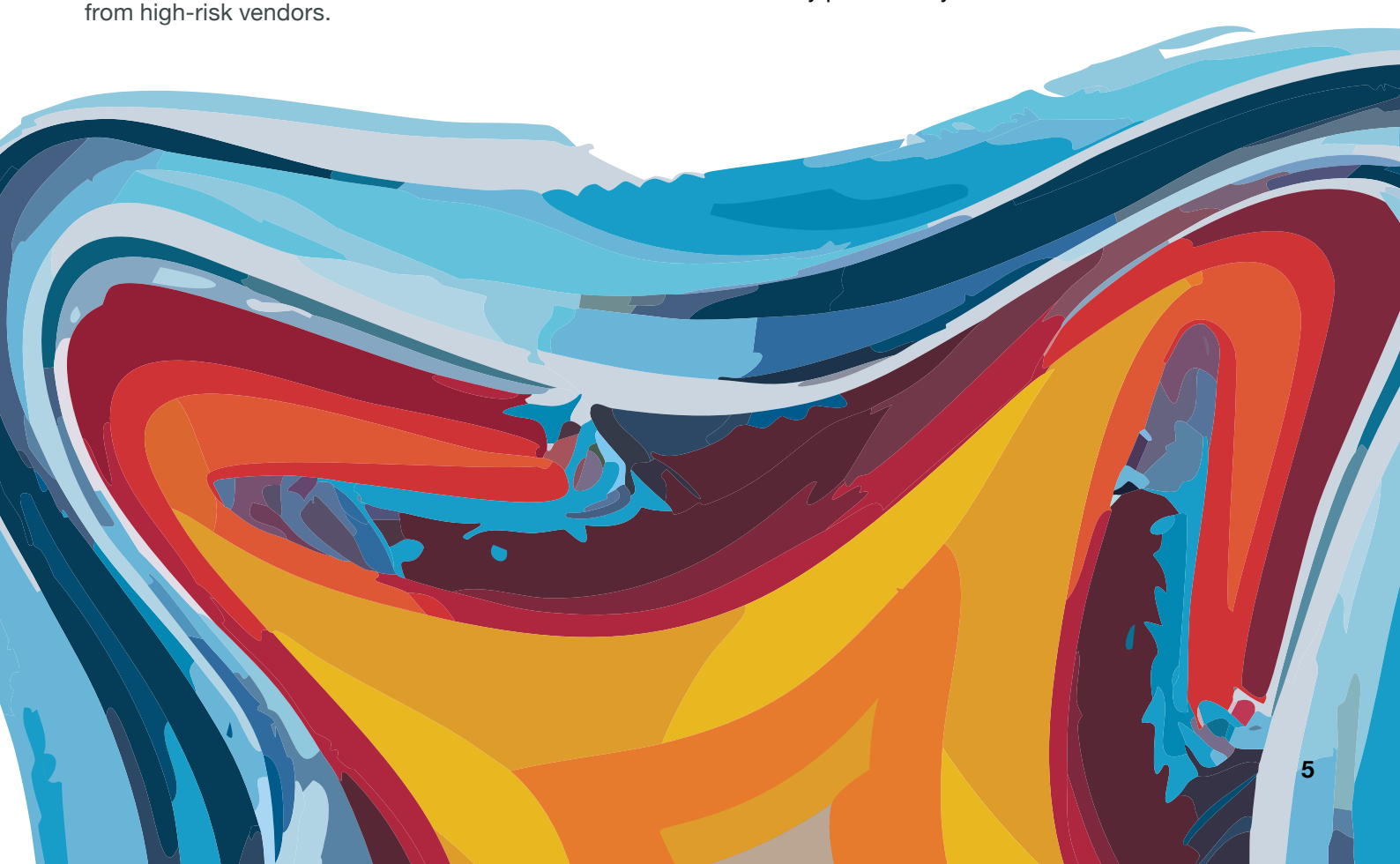
System of Record: Centralized information for easier communication and collaboration.

Continuous Monitoring: Move beyond the "point-in-time" view of the assessment and collect ongoing data from high-risk vendors.

Dual-Sided Information Exchange: Evolve past the questionnaire-only assessment to easily exchange public and private trust center data, security documentation like a SOC 2, and even responses to previously completed questionnaires proactively with your vendors.

Trained AI Models: The pipeline of information you create through a dual-sided exchange combines with your security controls and requirements to train AI-powered LLMs. Generative AI then makes collected documentation queryable in plain language.

Automated Assessment Engine: Import your customized questionnaires into the Modern TPRM framework, and AI can identify context-rich responses from myriad available data sources simultaneously. The AI engine also provides document citations and source materials; summarizes complex reports (so you don't have to manually); and analyzes the overall security posture of your vendor.



Modern TPRM in Action: **The AI Difference**

AI makes it possible to shift away from manual questionnaire response and utilize a wider variety of more readily available data sources. That greatly reduces the time and resources necessary for the TPRM process, so you can assess more of your vendors. AI also automates the analysis of these data sources, so you can access data-rich insights without poring line-by-line through documentation.

The Whistic Platform delivers an innovative suite of AI-powered capabilities for both buyers and their vendors. This dual-sided approach integrates seamlessly with every stage of the security assessment and response process to automate the heavy lifting—reducing manual work, driving insights, and boosting efficiency so you can focus on managing risk, not questionnaires.

Whistic AI foundation

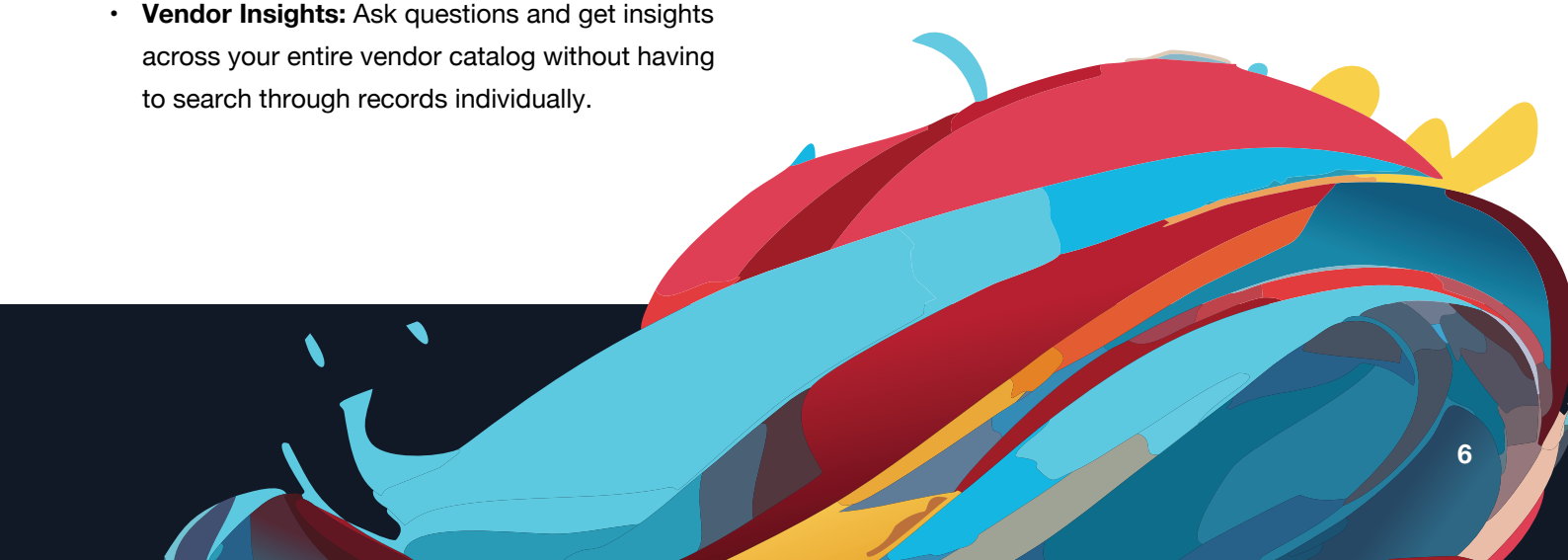
Whistic's AI approach comes standard with these ground-breaking capabilities:

- **Knowledge Base and Smart Search:** Find answers to questions fast—search your entire library of documentation and see the search results in context with links to sources and confidence levels.
- **Smart Response:** Reduce questionnaire response time from days or weeks to minutes with AI-generated responses to custom questionnaires. Review sources and confidence levels on auto-populated answers before sharing a completed questionnaire.
- **Smart Search for Vendors:** Quickly find answers to questions about a specific vendor using available information and vendor documentation.
- **Vendor Insights:** Ask questions and get insights across your entire vendor catalog without having to search through records individually.

Assessment Copilot

Whistic's Assessment Copilot builds on these foundational AI pillars with solutions focused entirely on a modern approach to vendor assessments:

- **SOC 2 Summary:** Create a summary with a click of a button to extract key details and risk insights from SOC 2 audits, eliminating the need to read lengthy reports.
- **Vendor Summary:** Using a vendor's documentation or trust center, quickly identify, assess, and measure risk and compliance against your controls.
- **Automated Review:** Click to generate a vendor's final assessment report, review the findings, and make a risk-based decision informed by AI insights and automation.



Turn legacy TPRM into a **Modern, Automated Assessment Engine**

If you're tired of taking on unnecessary risk, begging for questionnaire responses, and neglecting true risk mitigation because of endless manual administrative tasks, then you're ready for Modern TPRM.

Whistic's AI-powered platform works with both sides of the TPRM process, making it possible for buyers to assess all the vendors they want in greater detail, all without additional time or resources (use those to actually mitigate risk!). We also make it simpler for vendors to respond to more customers in a fraction of the time, building a stronger foundation of trust.

If you'd like to learn more about how Whistic's industry-leading AI can transform your TPRM, schedule a 30-minute demo and we'll show you the Whistic difference.

Schedule a Demo

Or contact Whistic today**: sales@whistic.com**