



IT'S TIME TO CHANGE:

A Modern Approach to Third-Party Risk Assessments

Table of Contents

Introduction	3
Third-Party Risk is at a Tipping Point	4
The Third-Party Risk Vulnerability Gap	5
A TPRM Force Multiplier to Close Your Vulnerability Gap	6
TPRM Automation	7
Universal Data Core	8
Assessment Exchange	9
AI-Powered Teams	10
Modern, Efficient Vendor Risk Assessments	11
STEP 1: Tier / Classify Your Vendors via Inherent Risk	12
STEP 2: Scope and Schedule Your Assessments	13
STEP 3: Import Completed Assessments via an Assessment Exchange	14
STEP 4: Augment Your Exchange Data with Supplemental Questions	15
STEP 5: Complete Assessments via Your Assessment Engine & Vendor Portal	15
STEP 6: Confirm Your Responses with External Expert Data	16
STEP 7: Accelerate Your Policy Reviews	17
STEP 8: Employ AI to Assess & Monitor Lower-Risk Third Parties	18
STEP 9: Set Up Post-Contract Continuous Monitoring	19
STEP 10: Measure & Report	20
Vendor Assessments Reimagined	21
How ProcessUnity Can Help	24



Introduction

Third-Party Risk is at a Tipping Point

As we navigate the complexities of modern business, it's crucial to acknowledge that most security breaches today—54%, according to VentureBeat¹—occur through third-party relationships. This statistic underscores the pressing need for robust Third-Party Risk Management (TPRM) practices, particularly as 47% of organizations now elevate TPRM to the level of board oversight². It's clear that third-party risk is not just a compliance issue; it's a strategic concern that demands attention at the highest levels of management.

Even so, a staggering 77% of TPRM executives³ believe their existing operating models require a significant overhaul. This reality is confirmed by a recent Forrester survey indicating that 69% of risk decision-makers view their TPRM programs as largely manual⁴. Alarming, only 30% of organizations assess at least half of their existing third-party relationships, suggesting a critical gap in risk evaluation. As someone engaged in TPRM, it's vital to consider these insights and reflect on the effectiveness of your own program. Is it equipped to manage the evolving risks associated with third-party partnerships?

FORRESTER®

According to Forrester*, **69%** of risk decision-makers identified their TPRM program as manual. "Even more concerning: **Just 30%** indicated that their organization's TPRM program evaluates at least half of its existing third-party relationships."

¹ VentureBeat:
<https://venturebeat.com/security/report-54-of-organizations-breached-through-3rd-parties-in-last-12-months/>

² Deloitte:
<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gers-TPGRM.pdf>

³ KPMG:
<https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/01/third-party-risk-management-outlook-2022.pdf>

⁴ Forrester:
<https://www.forrester.com/report/the-third-party-risk-management-platforms-landscape-q4-2023/RES180070>

BOARD SCRUTINY

47%

of orgs say TPRM rises to board-level oversight

CYBER EXPOSURE

54%

breaches happen through third-parties

BUSINESS FUNCTION

77%

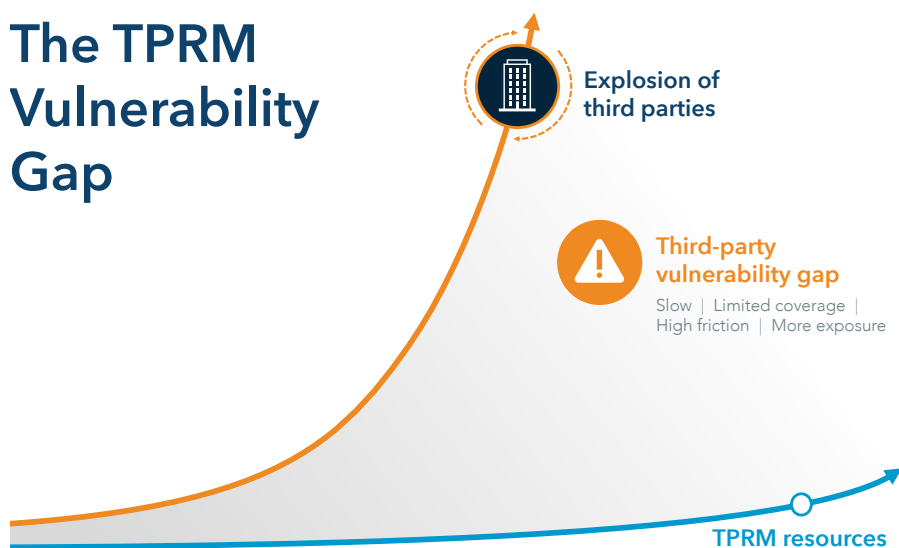
execs need to overhaul TPRM operating model

The Third-Party Risk Vulnerability Gap

The resources and budget you allocate for effective Third-Party Risk Management can't keep up with today's sheer volume of third-party relationships. Consequently, this imbalance creates a third-party risk vulnerability gap that negatively impacts your organization's ability to protect itself from disruption. It's important to recognize that every company faces a vulnerability gap, regardless of its size, although its composition may differ based on its unique operational structure.

For instance, you may experience long vendor onboarding cycles that hinder your ability to respond swiftly to emerging risks. You may also have backlogs in due diligence assessments, or a portion of your vendor population could be unassessed out of sheer necessity. The absence of a structured vendor tiering or prioritization system can further complicate your risk management efforts, making it more difficult to focus on the most critical partnerships.

The TPRM Vulnerability Gap



What Makes Up Your Gap?

- ▶ Onboarding Cycle Times
- ▶ Threat & Vulnerability Response
- ▶ Inadequate Portfolio Coverage
- ▶ Assessment Backlog
- ▶ Lack of Vendor Tiering / Prioritization
- ▶ Hard-to-Assess Vendors

With an ever-evolving threat landscape, any delay in responding to new vulnerabilities can expose your organization. Inadequate coverage of your vendor portfolio may prevent you from fully assessing the risks posed by all third parties, particularly larger organizations that are harder to evaluate.

As a TPRM decision-maker, you're required to navigate a complex balancing act to close this vulnerability gap. Each decision you make involves a trade-off between rigor and cycle times, consistency and flexibility, and portfolio coverage and available resources. Leveling out these dynamics is essential for developing a more robust TPRM strategy that meets the demands of today's risk environment.

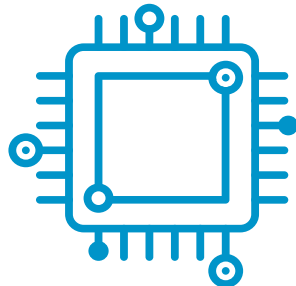
A TPRM Force Multiplier to Close Your Vulnerability Gap

To effectively close your TPRM vulnerability gap, you need to rethink outdated processes. You need a force multiplier that transforms the reality of limited resources into a modernized program, allowing you to eliminate difficult trade-off decisions and enhance your team's performance.

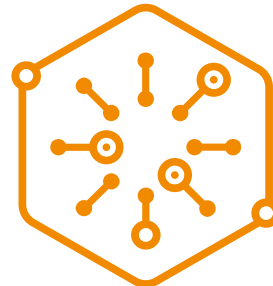
A force multiplier for TPRM is a strategy centered around four foundational components that are crucial for establishing effective and efficient TPRM processes:



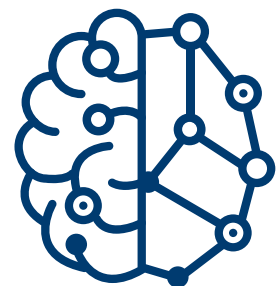
**TPRM
AUTOMATION**



**UNIVERSAL
DATA CORE**



**ASSESSMENT
EXCHANGE**



**AI-POWERED
TEAMS**

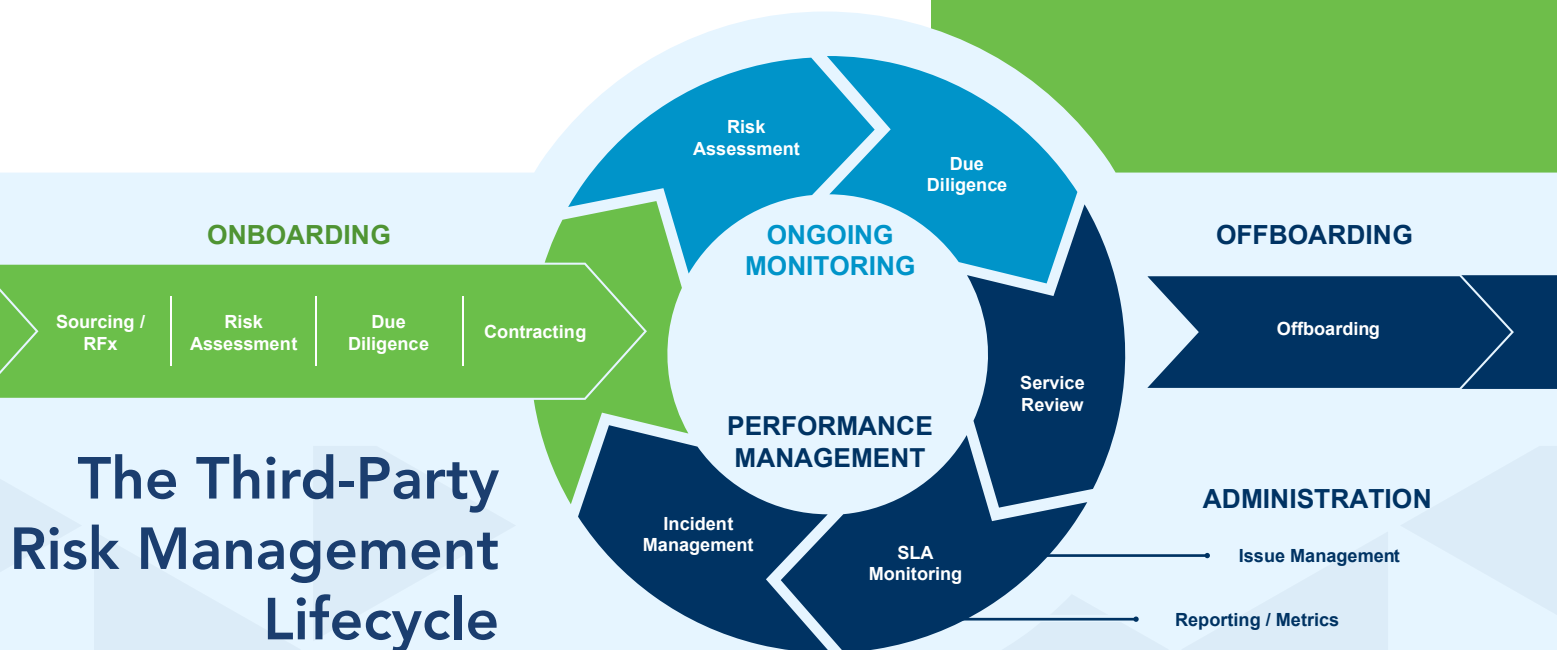
By focusing on these core elements, you can systematically address your organization's vulnerabilities and better safeguard your partnerships. In doing so, you'll empower your team to make informed decisions that bolster your overall risk management efforts, ensuring they can navigate the complexities of today's dynamic threat landscape.



TPRM Automation

Automation typically comes from a TPRM Platform. When selecting a TPRM platform, focusing on key features supporting your critical processes is essential. You need an assessment engine that enables you to configure assessments, distribute them to your vendors, and effectively score the results when they are returned. A vendor portal is vital as it fosters two-way communication between your organization and its third parties regarding assessments, supporting documentation, and any issues that arise during due diligence.

The system should also include scoring mechanisms to calculate key metrics such as inherent risk and assessment scores, and workflow capabilities that support various processes throughout the TPRM lifecycle. With no-code configuration, you can evolve your system over time as requirements change, enhancing functionality with enterprise systems integrations and external data feeds. Finally, strong reporting and dashboarding features are necessary for effective communication between team members, regulators, executives, and boards of directors.



Universal Data Core

Third-Party Risk Management is a data problem. Gathering information about a vendor from various sources often creates confusion and inconsistencies. You can solve this challenge by establishing a Universal Data Core, a single system of record for all third-party risk data.

A Universal Data Core typically lives in a TPRM platform. It connects relevant data across multiple systems, including Enterprise Resource Planning (ERP) systems, vendor management systems, business intelligence, and various compliance platforms, creating a comprehensive and cohesive data repository. Leveraging a Universal Data Core addresses the complexities of handling vast amounts of data associated with third-party risk.

For instance, 200 annual assessments comprising 200 questions each result in 40,000 data points for your team to review annually. The number more than doubles as you repeat the process the following year and add any new vendors to the mix. Coupled with additional data such as vendor profiles, policies, findings, and various performance metrics, the sheer volume of data you have to review quickly spirals out of control. A Universal Data Core organizes all of this data, so your team can efficiently navigate the review process.

A Single System of Record for TPRM

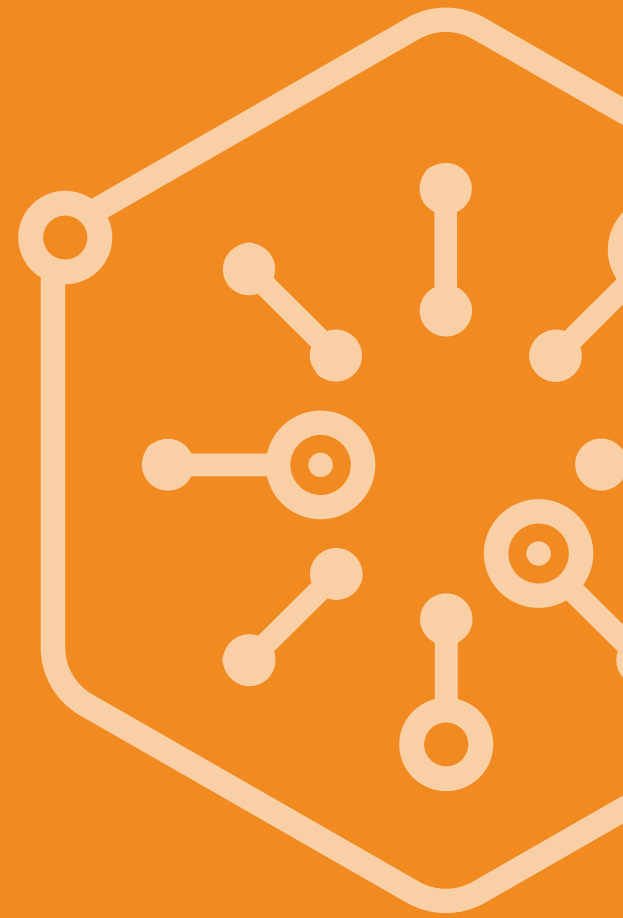
- + Governance, Risk & Compliance (GRC)
- + IT Risk Management
- + Contract Lifecycle Management (CLM)
- + Sourcing / Procurement Systems
- + Business Intelligence / Reporting Systems
- + Vendor Management Systems
- + Enterprise Resource Planning (ERP)
- + TPRM Assessment Exchange
- + External Ratings (Cyber, Financial, ESG, UBO, etc.)



Assessment Exchange

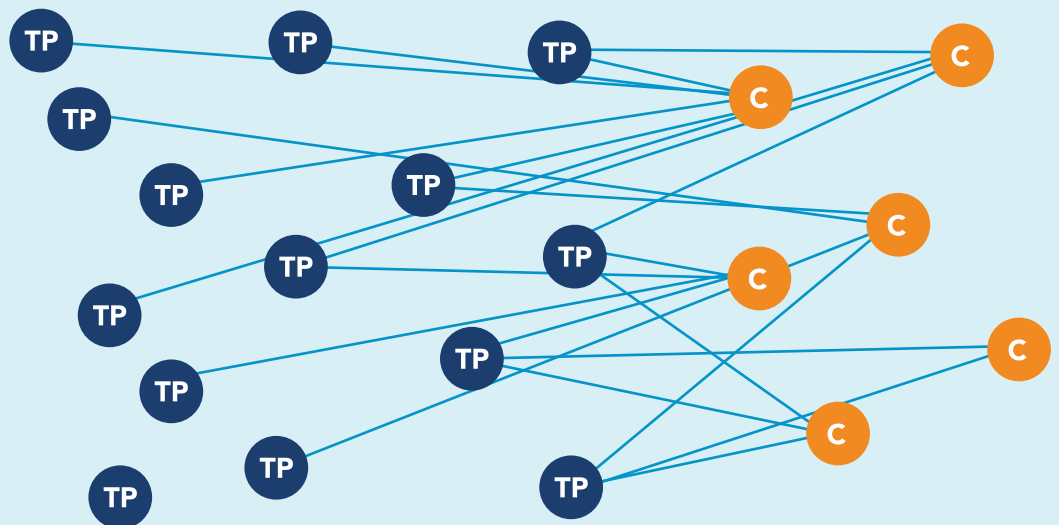
An assessment exchange is a significant advancement in TPRM that was borne by the significant burden placed on companies and their business partners to complete questionnaires. Facilitated via an online community, an exchange encourages the sharing of completed questionnaires among third parties and their customers, promoting an assess-once, share-many model.

By participating in an assessment exchange, third parties that typically don't respond to assessment requests can complete a single standard questionnaire and make it available to hundreds or even thousands of customers, thus streamlining the evaluation process. Customers benefit by receiving ready-to-use assessment information they don't have to collect independently. Moreover, as firms typically validate assessments, the credibility of the data is enhanced. When seeking an assessment exchange, prioritize participation from difficult-to-assess third parties, ensure a meaningful percentage of your vendor portfolio is represented, check the data refresh rate for up-to-date questionnaire information, and confirm that submissions are rigorously validated.



Features of an Assessment Exchange

- ▶ Assess Once / Share Many Model
- ▶ Completed, Attested, & Validated Assessments
- ▶ Assessments For Large Third Parties
- ▶ Analytics Based on Large Data Sets



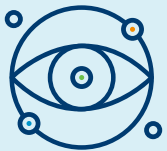
TP = Third Party

C = Customer

AI-Powered Teams

As new AI use cases emerge, incorporating Artificial Intelligence (AI) into your TPRM processes is imperative. AI can significantly enhance the performance of your human teams, allowing for increased efficiency and the ability to manage a larger number of vendors without sacrificing assessment quality. In some cases, AI can fill a gap in your program left open by limited resources, monitoring vendors, or reviewing documentation that human teams may not have the capacity to handle.

Specific use cases for AI in TPRM include conducting inherent risk assessments on vendor populations, creating automated risk profiles on third parties without requiring completed assessments, and accelerating the review of lengthy security policies. By leveraging these capabilities, you can streamline your processes and heighten the effectiveness of your TPRM initiatives.



Identify & Prioritize
Third-Parties



Expose Hidden Risks
with Automated Insights



Accelerate Vendor
Policy Reviews



Modern, Efficient Vendor Risk Assessments

Combining these four critical TPRM foundational components significantly enhances your approach to assessing third parties. This transformation allows you to streamline the vendor risk assessment process through a structured 10-step methodology. This modular approach can be implemented progressively, aligning with your organization's maturity level and available resources.

STEP 1:

Tier / Classify Your Vendors via Inherent Risk

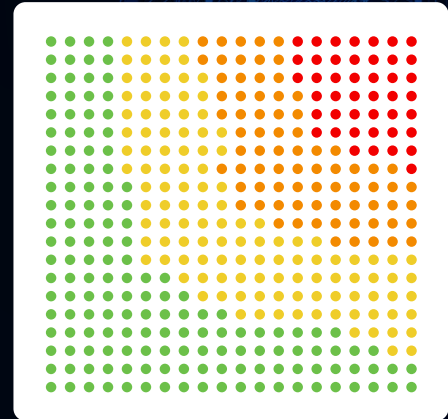
With limited TPRM resources, it's vital to prioritize the work effectively. To do this, consider implementing the first step: tiering or classifying your vendors based on inherent risk. Whether you have a few hundred or tens of thousands of third parties, categorizing them into criticality tiers—low-risk, medium-risk, high-risk, and critical-risk, for example—will help you focus on those that pose the most significant threats and are most essential to your business operations.

Modern TPRM approaches offer three methodologies for calculating inherent risk. First, consider using an Inherent Risk Questionnaire (IRQ), which is typically administered internally to the business users requesting vendor onboarding. The responses enable you to classify vendors into specific tiers based on their overall risk score.

Alternatively, you could leverage AI-based inherent risk calculations, which utilize machine learning to analyze large data sets, helping you identify the likelihood and potential impact of a breach based on vendor characteristics and service types. This AI-driven method provides a swift, effective means to prioritize the third-party ecosystem for organizations lacking inherent risk scores for a substantial number of vendors.

Lastly, some organizations adopt a hybrid model by combining AI and IRQ insights. In this scenario, AI is employed to validate responses from the IRQ, ensuring that third-party assessments are neither under nor overestimated. When discrepancies arise between the IRQ score and the AI-generated score, TPRM analysts can investigate further, thereby refining the risk assessment process.

YOUR PORTFOLIO PRIORITIZED BY **INHERENT RISK**

**CRITICAL****HIGH****MEDIUM****LOW****OPTION 1**

Inherent Risk Questionnaire

**OPTION 2**

AI-Based Inherent Risk Calculation

**OPTION 3**

IRQ + AI

STEP 2:

Scope and Schedule Your Assessments

Now that you have a tiered and prioritized vendor population, you can determine the scope and frequency of your post-contract due diligence assessments based on the tiering. As a general rule, more critical vendors should be assessed more frequently with a deeper scope of evaluation.

For example, scoping and scheduling based on inherent risk may result in the following decisions:

- The inherent risk tier is combined with the score from the most recent assessment to determine a residual risk score, which informs the scope and frequency of the next assessment.
- Any third party without a previous assessment should complete an evaluation as soon as possible.
- Critical third parties will undergo the most thorough due diligence annually.
- High-risk vendors will receive medium-level due diligence every other year.
- Medium-risk vendors will experience light assessments every three years.
- AI monitors the low-risk vendors. Due to bandwidth limitations, most organizations tend to take a lighter approach with low-risk vendors. We'll discuss AI monitoring in Step 8.
- Vendors performing well in their previous assessments may enjoy lighter due diligence or less frequent reviews.

Remember, scoping and scheduling should be tailored to your organization. It's essential to establish what works best for your operational needs.



STEP 3:

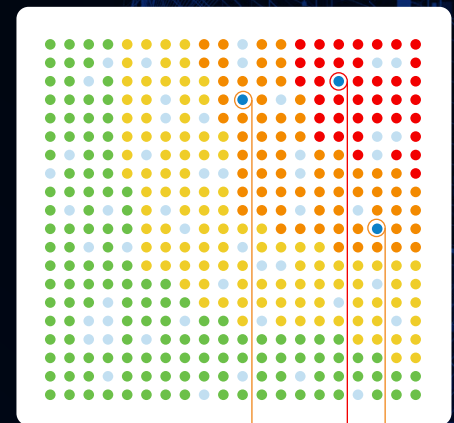
Import Completed Assessments via an Assessment Exchange

Imagine being able to reduce your assessment workload by anywhere from 25 to 40 percent. This is the promise of a TPRM assessment exchange, where some of your third parties have already completed a standard assessment. With a simple button click, you can request assessment data from these third parties. Upon their approval, the assessment data seamlessly integrates into your TPRM platform, enabling you to complete a portion of your assessment work with minimal effort.

Covering even 10 percent of assessments via an exchange represents significant cost savings for many organizations. In reality, this method typically covers around 25 to 40 percent of your vendor ecosystem. Even better, some of the assessments you access may come from large organizations that won't respond to your due diligence requests, including companies such as Salesforce, ADP, and Amazon Web Services. This means you gain access to critical assessment data that you might otherwise spend considerable time failing to obtain on your own.

25% to 45% Of your third parties may have an assessment in an exchange

● = Represents an assessed third party



...and Assess Large Third Parties

Large, hard-to-assess service providers prefer the exchange model to satisfy client due diligence demands

STEP 4:

Augment Your Exchange Data with Supplemental Questions

One of the primary considerations when deciding to use an assessment exchange is the standardized questionnaire being used. Will it align with your chosen framework? Will it address your unique requirements? Questionnaire mapping is essential to answering these questions.

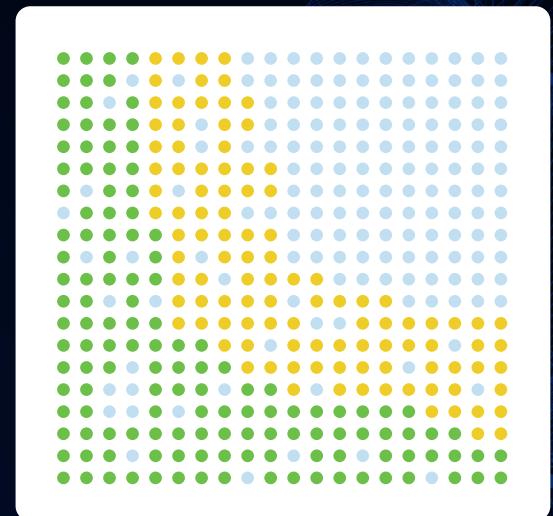
You should undertake a one-time exercise to map your questionnaire to the standard questionnaire used by the exchange you choose. By doing so, you can identify any gaps—specifically, questions in your assessment that are not represented by the exchange questionnaire. If gaps are found, you can construct an ancillary questionnaire that includes additional questions across various domains (such as ESG, financial, etc.). This approach allows you to send a much smaller and more focused assessment to the vendor, potentially reducing your query from hundreds of questions to maybe ten to twenty. This saves time for your vendors and streamlines the assessment process for you and your analysts, reducing vendor and analyst fatigue.

STEP 5:

Complete Assessments via Your Assessment Engine & Vendor Portal

For vendors not covered by the exchange, your TPRM team scopes and schedules an assessment using the assessment engine in your TPRM platform and collaborates with each vendor through an online vendor portal. As mentioned earlier, each vendor's inherent risk level determines the assessment's scope. Ensure your vendor portal accepts attachments so vendors can provide relevant policies, procedures, and other supporting documentation. You may also want to evaluate more advanced TPRM platforms and vendor portals that enable vendors to delegate questions to different stakeholders within their organization and score answers based on preferred responses defined by your TPRM team.

● = Represents an assessed third party



**Assess your remaining
CRITICAL or HIGH-RISK
third parties via your
assessment engine**

STEP 6:

Confirm Your Responses with External Expert Data

In this step, you will validate the assessment responses against your Universal Data Core that may incorporate data feeds from expert vendor intelligence providers, including cybersecurity ratings from RiskRecon, BitSight, and ProcessUnity (via the Global Risk Exchange), or Financial Health Scores from providers like Dun & Bradstreet and RapidRatings. Additionally, you can obtain Environmental, Social, and Governance (ESG) scores from EcoVadis and Anti-Bribery & Anti-Corruption (ABAC) data, Ultimate Beneficial Ownership insights, and Adverse Media feeds from LSEG (formerly Refinitiv) and Dun & Bradstreet.

It shouldn't come as a surprise that many companies present themselves as positively as possible in their questionnaire responses. Therefore, it's essential to cross-reference this information.

For instance, if an organization gave glowing responses to your vendor questionnaire, but RapidRatings returned a low financial health score of 72, and RiskRecon rated the vendor's cybersecurity as a 6.2 or a C rating, you should investigate these discrepancies further.

You may also find discrepancies between the various data providers. For example, if LSEG's World Check One reveals two positive results, but EcoVadis rates the vendor as low (30) for ethics, you may want to dig further. Cross-checking to confirm or affirm the data and third-party responses ensures a more accurate evaluation process.

Ensure your assessment responses are accurate with expert vendor intelligence from:



STEP 7:

Accelerate Your Policy Reviews

Reviewing policies is one of the most labor-intensive processes in Third-Party Risk Management. When it comes to reviewing policy documentation, you might find your TPRM team fitting into one of the following categories:

Skippers – You may choose not to review policy documentation during due diligence. While this tactic is fast and inexpensive, it can result in significant risk.

Skimmers – You might skim through policy documentation for key points. This approach is still quick and inexpensive, but it carries its own risks.

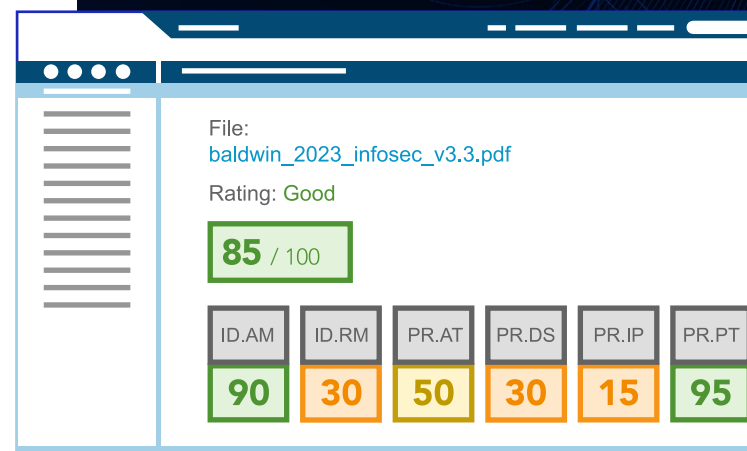
Readers - You could spend the time necessary to review all policy documentation comprehensively. While this is the least risky option, it is the slowest and most laborious.

Outsourcers – You might consider paying someone to fully review all policy documentation. While this can significantly reduce risk, it may be overly expensive.

What if you could leverage AI to streamline this review process?

For instance, you could include a question asking if the vendor has an information security policy. If the answer is yes, you can request that they attach it directly in the vendor portal so you don't have to chase it through email. Upon attachment, AI can read and assess the policy against a cybersecurity framework such as NIST, providing a score from 1 to 100. It can also provide detailed scores across each framework category, revealing additional areas of weakness.

For Skippers and Skimmers, AI offers insights they couldn't otherwise realize, given their minimal effort to review policies. For Readers, AI-driven policy reviews can save considerable time while ensuring consistency that may be difficult to achieve when multiple reviewers are involved. For Outsourcers, AI can significantly cut costs, allowing you to allocate funds to other critical areas of the program.

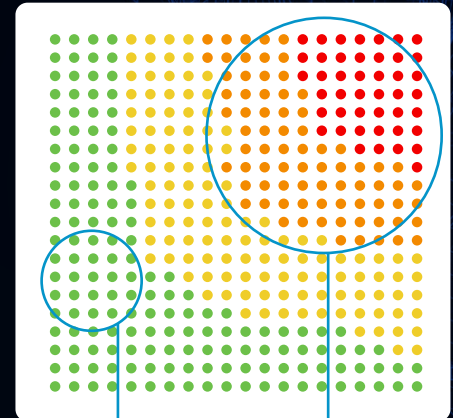


STEP 8:

Employ AI to Assess & Monitor Lower-Risk Third Parties

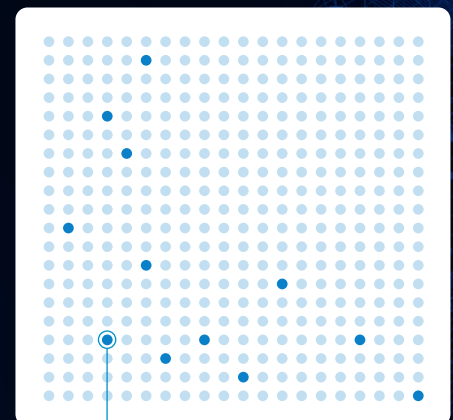
While TPRM teams rightly prioritize focusing on higher-risk vendors, it's important to remember that no third party is entirely without risk. Every business partner introduces potential challenges to your organization. However, most TPRM teams find themselves understaffed or underfunded to adequately assess medium- and low-risk vendors, leading to a "hope for the best" gamble with these relationships.

By leveraging AI, you can change this scenario. Using extensive datasets from TPRM assessment exchanges, AI can automatically construct remarkably accurate profiles for third parties by predicting how they would respond to an assessment questionnaire. Any vendor with a low confidence score warrants further evaluation through an actual assessment process. This approach enables you to achieve complete portfolio coverage, ensuring that every vendor is monitored effectively. For organizations struggling to assess a significant portion of their partner ecosystem, utilizing AI expands portfolio coverage, enhancing their overall risk management strategy.



**But
there's
risk here
too!**

**Your
area of
focus**



Low confidence score
Requires additional analysis

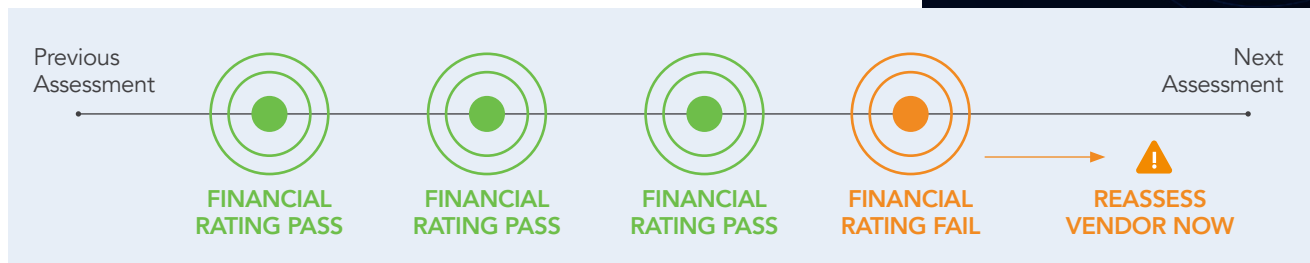
**AI anticipates with
high fidelity how a
third party will answer
assessment questions**

STEP 9:

Set Up Post-Contract Continuous Monitoring

Even if you assess your critical vendors annually, consider what could change during the 365 days between assessments. In this step, you should reintroduce continuous monitoring utilizing external expert data feeds that go beyond the regular post-contract assessment schedule. By combining external data feeds with the workflow in your TPRM platform, you can create a virtual watchdog that monitors all your vendors so your team can focus on active assessments. This combined workflow and data solution will:

- Review scores and ratings daily.
- Trigger alerts if a score falls below a predetermined threshold.
- Scope and send emergency assessments in response to alerts.
- Implement action plans when necessary.



This approach maintains your third-party vigilance, ensuring you are always aware of potential risks.

STEP 10:

Measure & Report

In the final step of the process, you will focus on measuring and reporting your progress—an often overlooked but critically important aspect. You should consider tracking metrics and key performance indicators, including:

- Average time to onboard
- Assessment completion rate
- Assessment backlog
- Due diligence completion time
- Portfolio assessment coverage
- Risk remediation time
- Service satisfaction rate
- Third-party compliance rate
- Third-party cost savings
- Third-party incident rate
- Third-party spend
- Vendor concentration
- Vendor diversity
- Overall program costs

You gain insights into areas that require improvement by consistently measuring and reporting your progress. This data will help you build compelling business cases to secure additional funding and enhance your position within the organization.

In a competitive environment with limited resources, those who present robust business cases are more likely to receive the necessary budget. As a forward-thinking TPRM leader, showcasing a strong program that yields tangible results can lead to greater opportunities within your organization, potentially advancing your career.



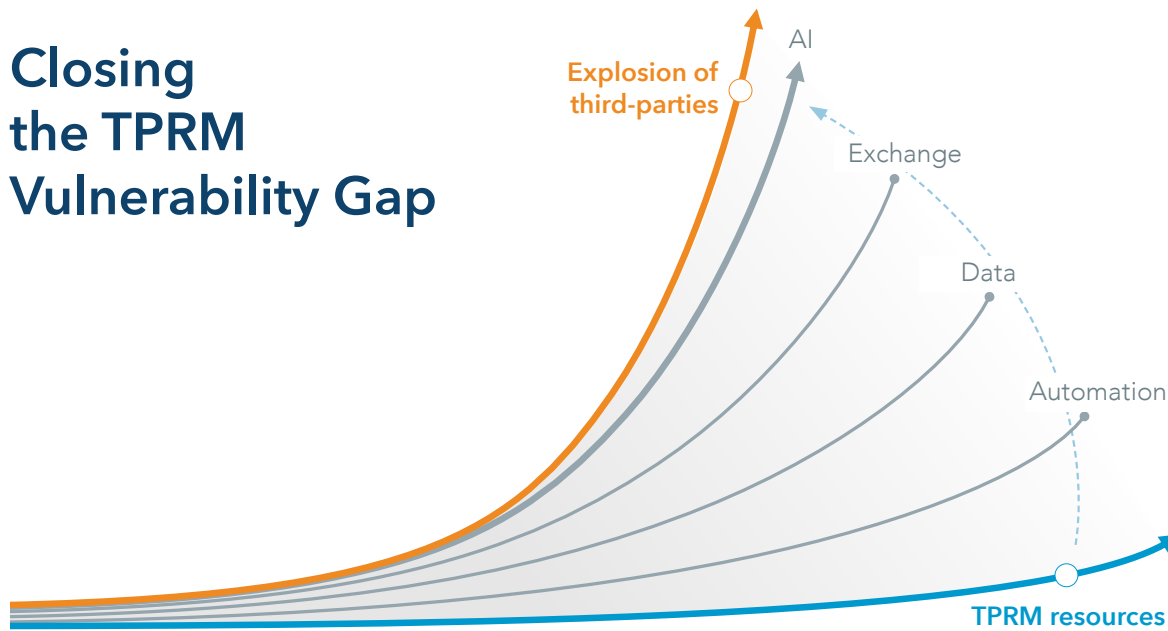
A woman with curly hair and glasses is looking at a computer screen. The image is overlaid with futuristic digital elements, including glowing yellow lines, a network diagram, and various data visualizations. The overall aesthetic is high-tech and modern.

Vendor Assessments Reimagined

Vendor Assessments Reimagined

In your journey toward modern vendor risk assessments, you'll notice how the four foundational pillars of Third-Party Risk Management manifest in each of the ten steps outlined in this report. Integrating automation, data, an assessment exchange, and artificial intelligence into your program will systematically address the holes in your Third-Party Risk Management program and significantly narrow your third-party risk vulnerability gap over time. With a mature TPRM approach, you significantly enhance your team's performance, enabling them to accelerate their processes without compromising quality.

Closing the TPRM Vulnerability Gap



This increased speed allows you to expand your vendor coverage significantly—from tens to hundreds or even thousands.

A world-class program should focus on:

- Prioritizing assessment work based on inherent risk
- Assessing traditionally hard-to-assess third parties
- Reducing the overall number of assessments performed
- Monitoring lower-risk vendors without necessitating additional resources
- Eliminating assessment backlog
- Demonstrating improvement across all key metrics

A Force Multiplier Across Your TPRM Program

INTEGRITY

Maximize confidence

COVERAGE

Scale from tens to hundreds to thousands

PEOPLE

Elevate human performance

SPEED

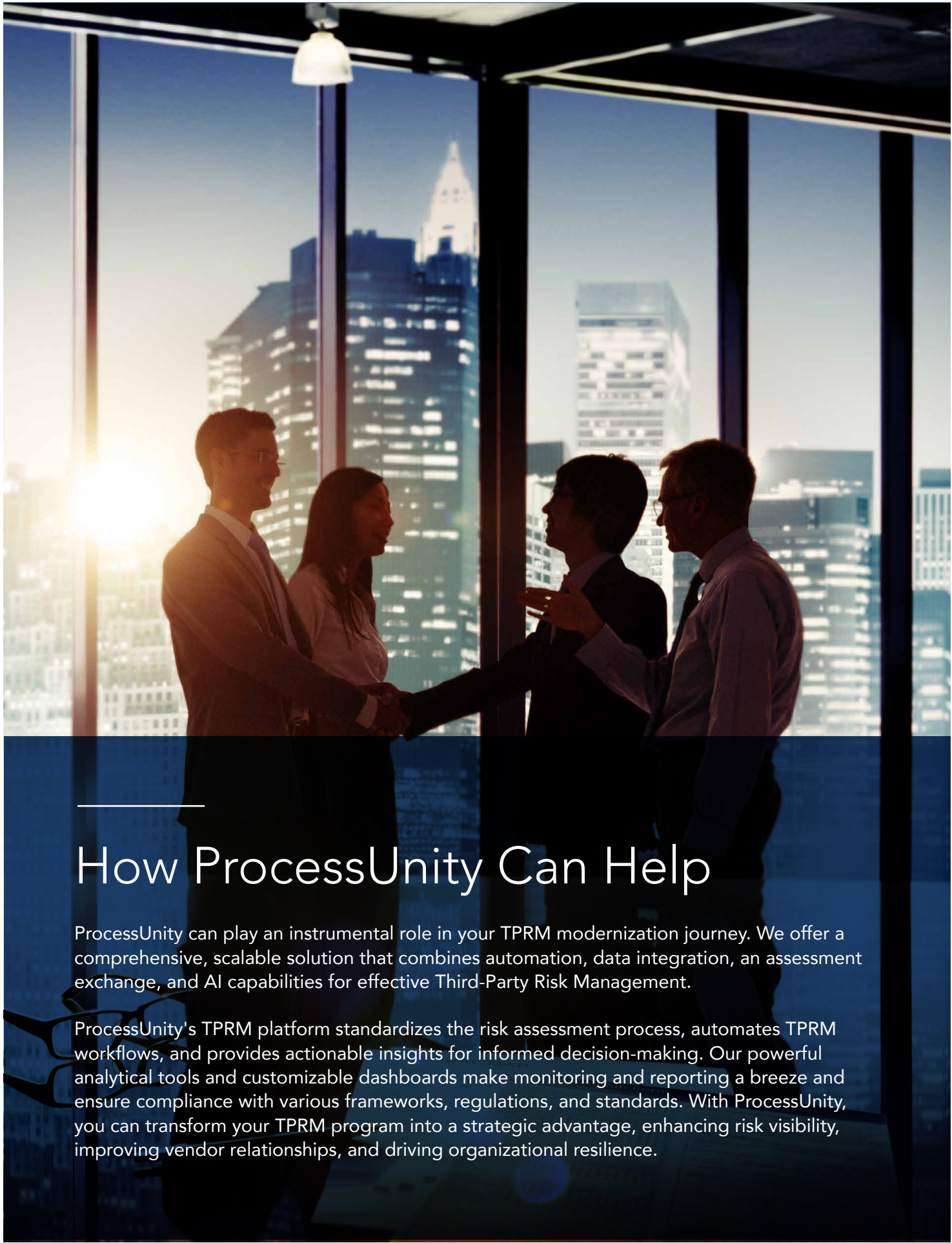
Accelerate diligence & actions

As you mature your program, you and your team will evolve from a reactive, point-in-time business prevention function into a strategic growth enabler, effectively closing any previously existing program gaps.

FROM
Managing Assessments

TO
Mitigating Risk

Compliance checklist	PURPOSE	Risk steward / growth enabler
Periodic	CADENCE	Continuous
Top tier	COVERAGE	Every third-party
Hundreds	VOLUME	Tens of thousands
Under-appreciated task	TPRM ROLE	Career-builder

A photograph of four business professionals (three men and one woman) in a modern office setting, standing near a large window with a view of a city skyline. The sun is low in the sky, creating a warm, golden glow. The professionals are dressed in business attire and appear to be in a collaborative discussion. The office interior features dark wood paneling and a modern light fixture.

How ProcessUnity Can Help

ProcessUnity can play an instrumental role in your TPRM modernization journey. We offer a comprehensive, scalable solution that combines automation, data integration, an assessment exchange, and AI capabilities for effective Third-Party Risk Management.

ProcessUnity's TPRM platform standardizes the risk assessment process, automates TPRM workflows, and provides actionable insights for informed decision-making. Our powerful analytical tools and customizable dashboards make monitoring and reporting a breeze and ensure compliance with various frameworks, regulations, and standards. With ProcessUnity, you can transform your TPRM program into a strategic advantage, enhancing risk visibility, improving vendor relationships, and driving organizational resilience.

The ProcessUnity Platform

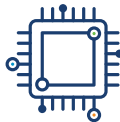
ProcessUnity offers the only all-in-one risk platform for modernizing Third-Party Risk Management.



TPRM Automation:

The ProcessUnity platform automates time-consuming tasks such as assessment scoping, distribution and response gathering so your TPRM team can direct their attention to the most critical actions. With the [workflow automation capability](#) ProcessUnity provides, your team can onboard vendors faster and generate configurable reports in real time.

LEARN MORE: [TPRM Automation](#)



Universal Data Core:

By gathering risk data from automated assessments and the Global Risk Exchange, as well as predictive insights and scores from trusted data partners, into a [single repository](#), ProcessUnity allows TPRM teams complete visibility into the state of their third-party ecosystem.

LEARN MORE: [Universal Data Core](#)



Global Risk Exchange:

With a repository of over 16,000 attested risk assessments, validated by our strategic audit partners, the [Global Risk Exchange](#) accelerates the TPRM process while enhancing its efficacy. By providing detailed insights into third-party risks, it eliminates the time-consuming task of assessing every third party individually.

LEARN MORE: [Global Risk Exchange](#)



AI-Powered Teams:

AI technology makes it easier to review policies at scale and make decisions based on accurate, real-time predictive insights into the broader third-party ecosystem. TPRM teams can multiply their efforts by partnering with [ProcessUnity's AI capabilities](#), achieving a more consistent TPRM process while reducing cycle times.

LEARN MORE: [AI Powered Teams](#)



Further Reading:

- [Closing Your Third-Party Risk Vulnerability Gap](#)
- [The Ultimate Guide to Third-Party Risk Management Workflow](#)
- [Third-Party Risk is a Data Problem: Solve it with a Universal Data Core](#)
- [Third-Party Risk Management: AI-Powered Teams Elevate Human Performance](#)
- [Third-Party Risk Management: How the Exchange Model will Revolutionize Vendor Due Diligence](#)



ABOUT PROCESSUNITY

ProcessUnity provides leading enterprises with comprehensive end-to-end cybersecurity and Third-Party Risk Management solutions. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest cyber risk exchange database, and powerful artificial intelligence capabilities, ProcessUnity enables organizations to quickly identify security gaps, reduce vendor onboarding and offboarding time, and proactively mitigate first- and third-party risks. As a result, organizations can more effectively safeguard their critical assets while lowering program costs. ProcessUnity is trusted by major brands around the globe and is backed by Marlin Equity Partners. To learn more or request a demo, visit www.processunity.com.

ADDRESS

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

SOCIALS

Twitter: [@processunity](https://twitter.com/processunity)
LinkedIn: [processunity](https://www.linkedin.com/company/processunity)

WEBSITE

www.processunity.com

EMAIL

info@processunity.com