ProcessUnity

The Ultimate Guide to Third-Party Risk Management Workflow

Table of Contents

Next-Level Techniques & Capabilities for Modern TPRM Programs 3
What to Look for in a TPRM Platform 4
Putting Your Platform to Work 7
Pre-Contract Workflows 7
Post-Contract Workflows 9
Advanced TPRM Workflows 11
Benefits of Automation 14
How ProcessUnity Can Help 15
The ProcessUnity Platform 16

Next-Level Techniques & Capabilities for Modern TPRM Programs

According to Gartner, 60% of organizations now work with more than 1,000 third parties. With ecosystems that large, third-party risk management (TPRM) teams are faced with the challenge of developing workflows that account for complexity without hampering their efficiency or allowing unwanted risk into the organization.

By automating their workflows, TPRM teams can streamline processes, ensure consistent and efficient risk assessments, and monitor their third-party relationships for control gaps and emerging threats.

Without workflow automation, managing third-party risks is a daunting and error-prone task, leading to overlooked risks, and endangering the organization's reputation, operational efficiency and compliance status. Hence, a well-planned workflow is not merely an operational need but a strategic imperative for effective TPRM.

This white paper will provide guidance for employing modern TPRM workflow automation to build a program that can more efficiently cover a larger volume of vendors and keep your organization safe.

Of course, you can only build an effective program with a flexible platform to suit your needs. Your chosen platform should provide foundational building blocks that help automate critical tasks throughout the third-party risk management lifecycle -- as early as vendor selection through eventual offboarding.

What to Look for in a TPRM Platform

When evaluating third-party risk management platforms, be sure to consider the following key components:

No-Code Configuration

No-code configuration enables your team to define and construct workflows without the need for complex coding or software development skills. With no-code configuration, you can quickly adapt the system to your organization's specific needs-- and quickly adjust to meet changing requirements.

By reducing the time and resources required to configure your TPRM platform, no-code configuration allows your team to focus on the actions that move the needle rather than spending hours attempting to marshal a piece of software to suit its needs. More importantly, the capacity to rapidly adjust to changing regulatory environments or business requirements enhances your organization's agility and, thus, its resilience.

Remember, in the dynamic world of third-party risk management, adjusting your workflows quickly and efficiently is not just an advantage - it's necessary.

Key Takeaway: A no-code third-party risk management platform empowers risk management teams to adjust their programs and processes without calling IT or paying for expensive consulting resources.

Hands-Free Automation

In an era characterized by more third parties and fewer resources, hands-free automation helps TPRM programs prevent a backlog by accelerating repetitive, mundane tasks. Third-party risk management is a time-consuming process, and finding the hours necessary to manually scope, distribute and gather assessments can be difficult. Hands-free automation ensures that repetitive tasks in your program are automated, freeing up your risk management professionals to cover more third parties and focus on more strategic aspects of TPRM.

Automation in TPRM can cover a broad spectrum of tasks, such as creating vendor records, sending out assessment forms, collating responses, calculating risk scores and generating reports. By automating these tasks, you can effectively eliminate human error, ensure consistency, enhance efficiency and expedite your risk management process.

More importantly, hands-free automation streamlines workflows across existing systems, improving visibility and standardization in your risk program. It ensures that all your third-party risk data is centralized, updated in real-time and easily accessible for audit and compliance purposes.

Key Takeaway: Hands-free automation does tedious administrative work, giving you greater bandwidth to achieve complete visibility and control over your third-party risks.

Reporting-as-a-Service

Another crucial component to consider in your TPRM workflow platform is Reporting-as-a-Service (RaaS). RaaS allows your organization to generate complex, real-time reports without additional technical expertise. RaaS simplifies the reporting process and enables organizations to quickly access, interpret and leverage data derived from their TPRM activities.

RaaS provides a comprehensive overview of third-party risks in a consolidated and user-friendly format, allowing decision-makers to understand their risk landscape completely. This functionality also supports regulatory compliance, as reports can be customized to meet the requirements of various regulatory bodies and audit types.

Moreover, using RaaS can make the risk management process more efficient. By automating report generation, organizations can free up time usually spent on manual report creation, allowing risk managers to focus more on risk mitigation strategies.

The ultimate benefit of RaaS lies in its ability to empower organizations with actionable insights, enabling them to make informed decisions regarding third-party risks. By reporting on metrics like Average Time to Onboard, organizations can determine how their TPRM policies impact their procurement procedures, providing critical context for future choices regarding assessment depth. Similarly, reporting on an organization's Third-Party Compliance rate helps executive leadership quickly understand the amount of regulatory risk brought into the organization via its third-party ecosystem.

Reporting-as-a-Service is not just a component of your TPRM workflow — it's a strategic tool that brings clarity, efficiency and intelligence to your third-party risk management efforts.

Key Takeaway: Leveraging Reporting-as-a-Service in your TPRM platform facilitates intelligent risk mitigation by providing real-time, comprehensive insights into third-party risks, enhancing regulatory compliance and streamlining risk management processes.

Integration with External Data Sources and Internal Systems

When a TPRM platform can easily integrate with enterprise systems and external data, your team can see further into its vendor ecosystem in greater detail. By supplementing internal risk assessments with external risk data, your team can achieve more comprehensive visibility. This could include financial stability data, cybersecurity ratings, or other industry-specific risk metrics, all contributing to a more robust risk profile for each of your third parties.

Equally important is the platform's ability to integrate with your internal enterprise systems. This allows for a centralized and unified view of all risk-related data, enabling cross-functional collaboration and ensuring all stakeholders access the same, up-to-date information. After all, every department has the systems they prefer to work with. By integrating with systems across the enterprise, a TPRM platform can help your teams help each other.

Seamless integration is a necessity in today's business environment. It affirms the platform's role as a central hub for all your third-party risk management activities, enabling more robust communication and visibility across the organization.

Key Takeaway: Integrating external data sources and internal enterprise systems into your TPRM platform allows for a more comprehensive understanding of third-party risks, fostering more effective and efficient risk management.

Artificial Intelligence

Artificial Intelligence (AI) is revolutionizing the TPRM landscape. By integrating AI into your TPRM processes, you can elevate performance within your team, enabling them to assess a larger vendor volume at a greater level of consistency.

One of the most impactful applications of AI in TPRM is automatic inherent risk calculation. Traditional methods of assessing inherent risk are prone to human error and can often consume valuable hours of your experts' time. By leveraging AI, organizations can automatically calculate inherent risk scores based on predefined criteria, speeding the process while ensuring a uniform scoring methodology.

Another way that AI will change TPRM is the creation of predictive risk profiles. AI algorithms can analyze historical risk data, identify patterns and trends, and make accurate predictions about large populations of third parties. This predictive capability enables organizations to score third parties that have yet to be assessed, reducing backlog and extending coverage to a greater percentage of the vendor portfolio.

Additionally, AI can automate your review of third-party security policies, freeing up valuable bandwidth so your analysts can direct their attention where it's needed most. In many organizations, policy reviews demand significant time and resources, overwhelming analysts and bogging down vendor onboarding. With AI-powered review tools, organizations can automatically review their vendors' policies based on appropriate frameworks, regulations and standards, highlighting the sections that demand human attention and verifying that a vendor's security controls align with your expectations.

Artificial Intelligence can transform your TPRM process, enabling your organization to scale its vendor assessment operations without sacrificing accuracy or consistency.

Key Takeaway: Leveraging artificial intelligence in your TPRM workflow can significantly enhance risk assessment accuracy and consistency, automate policy reviews and generate predictive data, elevating your team's performance and extending its reach to more third parties.

Risk Exchange Access

Risk exchanges, typically powered by a community of third parties and their customers, provide a vast repository of up-to-date third-party risk assessments that your organization can instantly utilize. By connecting to a risk exchange, your TPRM platform taps into a wealth of external risk data, allowing for a broader and more informed assessment of third-party risks.

Risk exchanges help your team work faster by reducing the need for redundant assessments. Instead of conducting separate assessments for the same third party, your organization can leverage assessments already shared on the risk exchange to gain instant access to standardized vendor data. This collaborative model makes the risk assessment process more efficient and enhances the comparisons across vendor profiles. Look for a risk exchange that uses a standardized questionnaire to ensure accessible, reliable comparisons between vendors' complete control sets.

Moreover, risk exchanges often encompass an expansive network of organizations and third parties, enabling your organization to identify industry benchmarks and best practices. This comparative data provides valuable insights into your performance compared to your industry peers, helping you determine where to direct efforts to improve your TPRM program.

Key Takeaway: Utilizing a risk exchange in your TPRM workflow reduces your team's assessment work volume. It gives you assessment data on the largest, hard-to-assess corporations that typically don't respond to assessment requests.

Putting Your Platform to Work

With the building blocks in place, it's time to put your TPRM platform to work. As we delve deeper into the following sections, we'll explore the key areas where workflow delivers value to key stakeholders, including internal groups like your TPRM team, procurement, information security, line-of-business users and external stakeholders like your vendors' corresponding teams. We'll start with the most frequently employed workflows for the most critical and time-consuming processes and work up to more advanced implementations for mature TPRM programs.

Pre-Contract Workflows

Inherent Risk Assessments

Inherent risk assessments, sent typically as part of the vendor request process, help TPRM teams determine which vendors are worth assessing, how often they should be assessed and at what level of depth. The inherent risk process involves thoroughly analyzing the third party's business model, operations, geographical location, regulatory environment, and the scope of the projected engagement. The risk factors identified during this stage are then rated based on their potential impact and likelihood without considering existing controls.

Inherent risk questionnaires and AI-based tools help teams streamline and enhance the risk assessment process by structuring data collection and analysis. The AI-based tools add a layer of sophistication to these assessments by automating data collection and evaluation and sifting through large volumes of data in a fraction of the time it would take a human analyst. Additionally, AI tools can learn from past outcomes, continuously improving their accuracy and enabling a more proactive approach to risk management.

The inherent risk process can also be improved by automating the collection and analysis of risk data. Automated workflows can streamline the process, ensuring consistent assessments across all third parties and reducing the time and resources required. By harnessing the power of automation, organizations can effectively assess the inherent risk posed by third parties, make informed decisions, and build robust risk management strategies.

Key Takeaway: Implementing automation in inherent risk assessments amplifies the process's speed and precision. It empowers organizations with far-reaching insights, paving the way for data-driven decision-making in third-party risk management.

Pre-Contract Due Diligence

Pre-contract due diligence is arguably the most critical pre-contract TPRM workflow because it presents the opportunity to identify risk before it can enter your business. This process thoroughly examines a prospective third party's cybersecurity policies, financial stability, operational resilience, compliance with relevant regulations and reputation before contract signature. The goal of due diligence is to validate the third party's trustworthiness and suitability as a business partner.

Without an automated platform, there isn't enough time to perform due diligence on every vendor that needs it. Risk analysts must collect adequate information from their vendors, but they also want to avoid fatiguing respondents with bloated questionnaires and irrelevant items. For this reason, risk management teams often spend countless hours manually building and scoping their assessments to fit the demands of a particular vendor—a process that reduces the strain placed on third parties and increases the amount placed on analysts. Once analysts have scoped and distributed assessments, they need to chase down responses, another step that soaks up valuable time when completed manually.

Automated workflows streamline the due diligence process, allowing organizations to reduce onboarding cycle times. While automated assessment scoping intelligently tailors question sets to match a vendor's inherent risk score, automated assessment distribution and response gathering remove the busywork from data collection. Leveraging automation, organizations can quickly gather information, analyze data and generate comprehensive due diligence reports, reducing the time spent on data collection and analysis, and producing a more efficient, less expensive process.

Key Takeaway: By applying automation to due diligence checks in the pre-contract phase, TPRM teams prevent risk from entering the company by working with the most substantial service providers.

Post-Contract Workflows

Post-contract workflows ensure that risk assessment and mitigation continue throughout the lifecycle of the third-party relationship. This phase includes three major components - post-contract due diligence, ongoing vendor monitoring, and offboarding.

Post-Contract Due Diligence

Post-contract due diligence continuously validates a third party's risk status, compliance and performance. Unlike its pre-contract counterpart, which focuses on the suitability of a potential partner, post-contract due diligence emphasizes the ongoing risk posed by a third party for the duration of the relationship.

This involves a routine examination of the third party's performance, financial stability, adherence to service level agreements (SLAs), compliance with relevant regulations and changes in their risk profile. It is a robust process that enables an organization to proactively identify and manage potential risks that might arise throughout a vendor relationship.

Automation makes post-contract due diligence faster and more consistent by systematically gathering and analyzing data, triggering alerts for significant changes or deviations and generating comprehensive reports. This eliminates manual tasks and ensures a timely and accurate evaluation of the third party's performance and risk status over the years.

By maintaining a rigorous post-contract due diligence process, an organization can ensure the suitability and reliability of its third parties, manage any emerging risks promptly and safeguard its interests and those of its third parties.

Key Takeaway: The use of automation in post-contract due diligence speeds the assessment process, reducing backlog and enabling the more effective treatment of emerging threats.

Ongoing Monitoring

Ongoing monitoring is the continuous surveillance of a third-party's operations to ensure compliance with contractual obligations and detect any changes in their risk profile.

This process relies heavily on external data sources – like cyber ratings, financial risk scores and more – for real-time insights into a vendor's performance and risk status. By supplementing post-contract risk assessments with data from a varied set of trusted suppliers, risk managers can fill in the gaps between questionnaires and make confident assumptions about the ongoing state of their vendor ecosystem.

Automated workflows can streamline collecting, analyzing, and integrating external data into the ongoing vendor monitoring process. By gathering external data into a single platform alongside questionnaire responses and other vendor information, an automated workflow makes comparing vendor status across the ecosystem easier than ever, enabling more robust risk prioritization and mitigation actions.

Automated alerts also provide immediate notification of significant changes or deviations in a vendor's risk posture, allowing organizations to mitigate potential risks swiftly. Furthermore, automated reporting capabilities can provide a clear, holistic picture of the vendor's performance and risk status at any time.

Key Takeaway: Leveraging automation in ongoing vendor monitoring provides real-time insights across risk domains, ensures proactive risk management and significantly enhances the sustainability of third-party relationships.

Vendor Offboarding

The final stage of the third-party relationship, vendor offboarding, is often critically overlooked. This phase ensures the termination of the relationship is managed safely and efficiently and reduces residual risks. It involves data retrieval, termination of access rights, settling financial obligations and a final performance assessment.

Automated workflows can streamline the closure process by ensuring all necessary actions are taken promptly and systematically. With a transparent offboarding process, organizations can mitigate the risks of data breaches, reputation damage, and financial losses associated with the uncontrolled termination of a third-party relationship.

Moreover, the vendor offboarding process allows organizations to review and assess the vendor's performance thoroughly. Automated workflows can generate comprehensive reports of the vendor's performance throughout the contract's lifecycle, providing valuable insights that can be used to inform future vendor selection and management decisions.

Key Takeaway: Automating the vendor offboarding process mitigates potential risks associated with terminating third-party relationships and provides valuable insights for future vendor selection and management strategies.

Advanced TPRM Workflows

As your third-party risk management strategy matures, more complex workflows can be incorporated further to increase the visibility of your third-party risk landscape. These workflows include RFx/Sourcing processes, vendor service reviews, service-level agreement (SLA) monitoring, zero-day vulnerability attack responses and connecting third-party controls to your internal controls.

Vendor Selection / RFx Processes

The start of any third-party relationship begins with the vendor selection process, often initiated by a Request for Proposal (RFP), Request for Information (RFI), or Request for Quotation (RFQ), collectively known as RFx processes. These processes are crucial for identifying potential vendors to meet the organization's requirements best.

The RFx process typically involves:

- Delivering a structured set of requirements and standards to potential vendors
- Evaluating the responses
- Selecting the most suitable vendor based on predefined criteria

This process can be complex and time-dependent, requiring rigorous data collection, analysis, and decision-making processes.

Automation can streamline this process, significantly reducing the time and resources required. Automated workflows enable organizations to identify the best vendor much faster and with far fewer labor hours by systematically gathering and comparing vendor responses, highlighting discrepancies and ranking vendors based on suitability.

Furthermore, automation in RFx creation and distribution also promotes transparency and fairness, as decisions are made based on a clear set of criteria, and every vendor is evaluated equally. This helps organizations make optimal vendor selection decisions, strengthen their compliance and reduce potential reputation risks.

Key Takeaway: Automation integration in RFx processes streamlines vendor selection and enhances transparency, compliance and the overall integrity of your onboarding process.

Contract Risk Management

Effective contract risk management means systematically mitigating the risks associated with third-party contracts. This encompasses the identification, assessment and monitoring of legal, financial, operational and reputational risks that can arise from unfavorable contract terms, non-compliance or the failure of a third party to meet their contractual obligations.

Automated workflows ensure that all contracts are thoroughly assessed for potential risks before signing them. They can also monitor contractual performance continuously, alerting organizations to any deviations or potential issues in real time. This allows for swift mitigation actions, reducing the potential impact of contract-related risks.

Moreover, an automated platform can provide a centralized repository for all contracts, ensuring transparency and easy access to essential documents. It can automatically track contract renewal dates, provide alerts regarding critical contractual milestones and generate comprehensive reports on overall contract risk.

Key Takeaway: Automation in contract risk management optimizes efficiency and bolsters compliance, safeguards organizational interests and enhances the value derived from third-party relationships.

Vendor Service Reviews

Regular, systematic service reviews are essential for maintaining healthy vendor relationships and ensuring that the organization receives the expected value from its third-party engagements.

An effective service review process includes periodic meetings with vendors to discuss performance metrics, contractual compliance, service issues and future plans. These reviews ensure vendor accountability and provide a platform for open dialogue and continuous improvement. By tracking the number of deliverables completed on time, the quality of the services rendered, and the price of the vendor relationship, a TPRM workflow platform can make it much easier to determine which vendors are serving an organization’s needs and which need to make improvements or be replaced.

Automated workflows can collect, analyze and report vendor performance data, transforming raw metrics into actionable insights. This enables organizations to objectively assess vendor performance, identify trends, and make informed decisions based on real-time data.

Moreover, automated vendor service reviews can monitor a third party’s compliance with Service Level Agreements (SLAs), alert organizations to deviations, and initiate corrective actions, ensuring continuous service quality and preventing potential issues before they escalate.

Key Takeaway: Embracing automation in vendor service reviews enhances relationship transparency and optimizes third-party value, ensuring your organization’s third-party relationships are maximally productive and risk averse.

Service Level Agreement (SLA) Monitoring

Service Level Agreement (SLA) Monitoring involves continuously tracking and evaluating a vendor's adherence to the service standards and performance metrics defined in the contractual agreement. This is essential to ensure that the services received align with the organization's expectations and contractual stipulations.

Automation plays a significant role in optimizing SLA monitoring processes. With automated workflows, organizations can understand which SLAs are assigned to each vendor, track service quality, detect deviations from agreed-upon standards and initiate corrective actions in real time. This ensures consistent performance and reduces the risk of SLA breaches, which can lead to service disruptions, financial penalties and reputational damage.

Automated SLA monitoring also enables organizations to maintain a comprehensive record of vendor performance over time. This valuable data source can be leveraged to assess vendor reliability, make informed decisions about contract renewals, and negotiate more favorable contract terms in future engagements.

Key Takeaway: Using automated workflows in SLA Monitoring not only bolsters the accuracy and efficiency of the process but also reinforces vendor accountability, safeguarding the quality of service and maximizing the return on third-party engagements.

Zero-Day Vulnerability Attack Responses

A zero-day vulnerability refers to a software security flaw unknown to those who should be mitigating it, including the affected software vendor. These vulnerabilities can allow malicious actors to bypass a system's access controls, leading to unauthorized access or significant data breaches.

Preparing to respond to such vulnerabilities means implementing robust and responsive control measures. By facilitating real-time detection and alert mechanisms, automated workflows ensure the timely identification of these vulnerabilities, enabling more effective, more immediate mitigation actions.

Once a zero-day vulnerability is detected, an automated system can initiate a pre-defined response protocol. This can include notifying the appropriate stakeholders, assessing the extent of the potential breach, kicking off a rapid assessment questionnaire to critical third parties, initiating corrective measures and reporting findings to executive management. Further, these workflows can automate the incident documentation and the response action. This step is crucial for audit purposes and for refining future risk management strategies.

Key Takeaway: Implementing automated workflows in response to zero-day vulnerabilities ensures a rapid, systematic approach to threat response, helping organizations mitigate risks and protect their critical data promptly.

Connecting Internal Controls to Third-Party Controls

Measuring third-party controls against your internal control framework provides a comprehensive view of internal and external risks, enabling a comprehensive approach to third-party risk management. This process involves mapping your organization's internal controls to the controls implemented by your third parties and measuring their effectiveness using targeted assessments.

Automated workflows can continuously monitor the adherence of both internal and third-party controls to regulatory standards, contractual stipulations and organizational policies. This real-time monitoring enables organizations to identify and address any deviations or potential risks promptly.

Moreover, integrating internal and third-party controls provides a unified view of risk across the organization and its third-party network. This facilitates a more informed and robust risk assessment and decision-making process. It enables organizations to identify potential risk interdependencies, mitigate systemic risks and strengthen overall risk resilience.

Key Takeaway: Utilizing automation to align internal and third-party controls provides a unified perspective on risk management and bolsters the organization's ability to anticipate, manage and mitigate risk.

Benefits of Automation

Implementing a third-party risk management workflow platform brings several benefits to organizations, including:

Time and Cost Savings

By automating time-consuming TPRM tasks, organizations can save considerable time and resources that would otherwise be spent on manual processes. This, in turn, allows them to focus on more critical tasks.

Increased Efficiency and Consistency

Automation reduces the risk of human error and ensures consistency in the evaluation process. Organizations can have a more efficient and accurate risk assessment process by using standardized assessment questionnaires and predefined parameters to flag risks.

Improved Risk Visibility

A workflow platform provides organizations with a centralized repository for all third-party risk information. This gives stakeholders better visibility into potential risks, remediation efforts and ongoing monitoring activities.

Enhanced Compliance

Third-party risk management is essential for ensuring compliance with industry regulations and standards. A workflow platform can help organizations stay on top of compliance requirements by automating the collection of relevant data and providing real-time alerts for potential risks.

How ProcessUnity Can Help

ProcessUnity is a leading provider of third-party risk management software solutions. Our platform is designed to automate key TPRM lifecycle phases, from initial onboarding and due diligence to continuous monitoring and offboarding.

ProcessUnity Third-Party Risk Management offers a highly configurable, easy-to-use platform that assists in identifying and assessing risks, managing and mitigating identified risks, and ensuring compliance across your third-party relationships. With built-in best practices and automated workflows, the solution can significantly reduce the time and effort required to manage third-party risks.

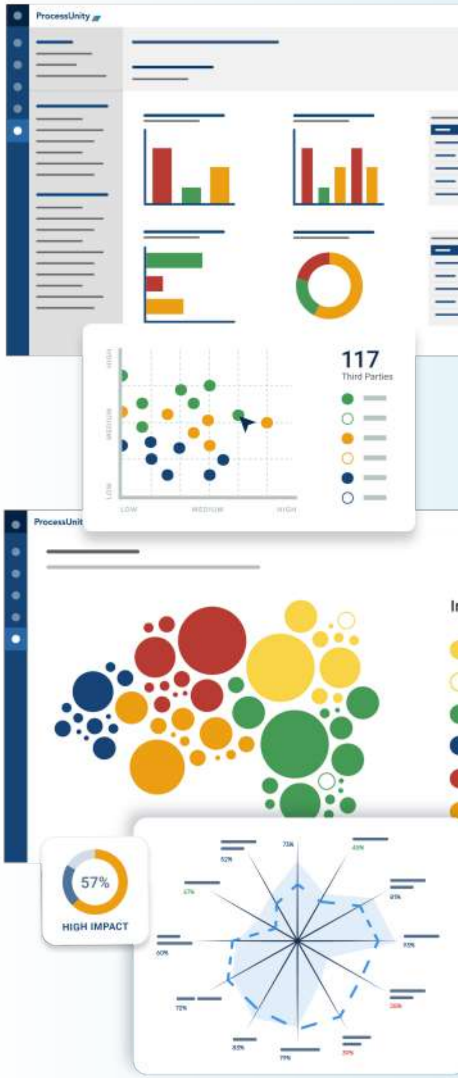
The platform also provides a centralized location for storing and managing all third-party risk data, ensuring enhanced visibility and facilitating informed decision-making. With automated alerts, real-time risk reports and advanced analytics, ProcessUnity empowers organizations to manage and mitigate third-party risks proactively.

Moreover, ProcessUnity ensures the continuous alignment of your third-party and internal controls, giving you a unified view of risk and facilitating holistic risk management. The platform is designed to evolve with changing industry regulations and standards, ensuring you remain compliant and prepared for any potential risks.

Key Takeaway: ProcessUnity's TPRM solution offers a comprehensive, automated, and proactive approach to managing third-party risks. By leveraging its capabilities, organizations can ensure efficient, accurate and consistent risk management, enhanced compliance and improved decision-making – ultimately driving business success.

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 like 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 15,000 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

Required reading:

- Closing Your Third-Party Risk Vulnerability Gap
- Third-Party Risk Management: AI-Powered Teams Elevate Human Performance
- Third-Party Risk is a Data Problem: Solve it with a Universal Data Core
- How the Assessment Exchange Model Revolutionizes Vendor Due Diligence

ProcessUnity

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
LinkedIn: processunity

WEBSITE
www.processunity.com

EMAIL
info@processunity.com