DATA SHEET

BEST PRACTICES CONFIGURATION

for ProcessUnity Vendor Risk Management

A Complete, Comprehensive & Proven Program to Reduce Third-Party Risk

ProcessUnity Vendor Risk Management (VRM) is a software-as-a-service (SaaS) application that identifies and remediates risks posed by third-party service providers. Combining a powerful vendor services catalog with risk process automation and dynamic reporting, ProcessUnity VRM streamlines third-party risk activities while capturing key supporting documentation that ensures compliance and fulfills regulatory requirements. ProcessUnity VRM provides powerful capabilities that automate tedious tasks and free risk managers to focus on higher-value mitigation strategies.

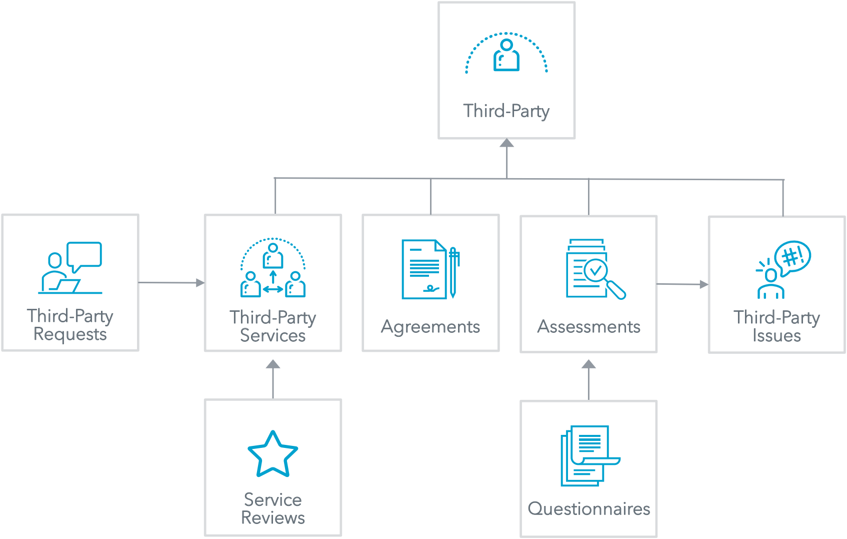
ProcessUnity Best Practices Configuration

Best Practices Configuration for ProcessUnity Vendor Risk Management (VRM) is a pre-configured third-party risk program with turn-key workflow, assessments, calculations, risk analysis and reporting. Developed by Third-Party Risk Management subject matter experts and perfected via hundreds of successful customer implementations, Best Practices Configuration delivers a complete, "out-of-the-box" program with a high-quality, systematic and repeatable assessment process that improves communication between lines of business, third-party risk analysts and third-party contacts to ultimately drive risk out of an organization. The low-touch, low-cost implementation gets customer programs up and running in no time. As a program changes and matures, customers can modify the pre-defined processes, calculations, roles and workflows via ProcessUnity's unparalleled platform configuration capabilities*.

Program Structure

ProcessUnity's Best Practice Configuration includes a sophisticated data model which includes pre-built relationships and workflows between key data elements and system users. The elements of the data model include:

- **Third Parties** – External vendors, suppliers and organizations from which services are contracted
- **Third-Party Requests** – Requests from LOB employees for new third-party services
- **Third-Party Services** – The specific service(s) contracted from various vendors and suppliers
- **Service Reviews** – Periodic evaluations on contracted third-party services
- **Agreements** – Contracts and other legal documents signed with third parties
- **Assessments** – Completed due diligence surveys from third parties
- **Questionnaires** – Pre-configured third-party surveys used to conduct due diligence
- **Third-Party Issues** – Issues identified during vendor onboarding or via ongoing monitoring



ProcessUnity's Third-Party Risk Management Data Model

ProcessUnity

Workflows & Assessments

Pre-configured workflows establish the repeatable processes necessary for effectively managing third-party risk – from initial service identification and onboarding, through contracts, ongoing vendor monitoring and termination.

Included workflows:

- Onboarding Request Workflow
  Capture a new service request, automatically determine inherent risk, perform due diligence, manage issues and sign agreements
- Ongoing Monitoring Workflows
  Conduct periodic service reviews to monitor inherent risk changes, remediate issues and perform ongoing due diligence

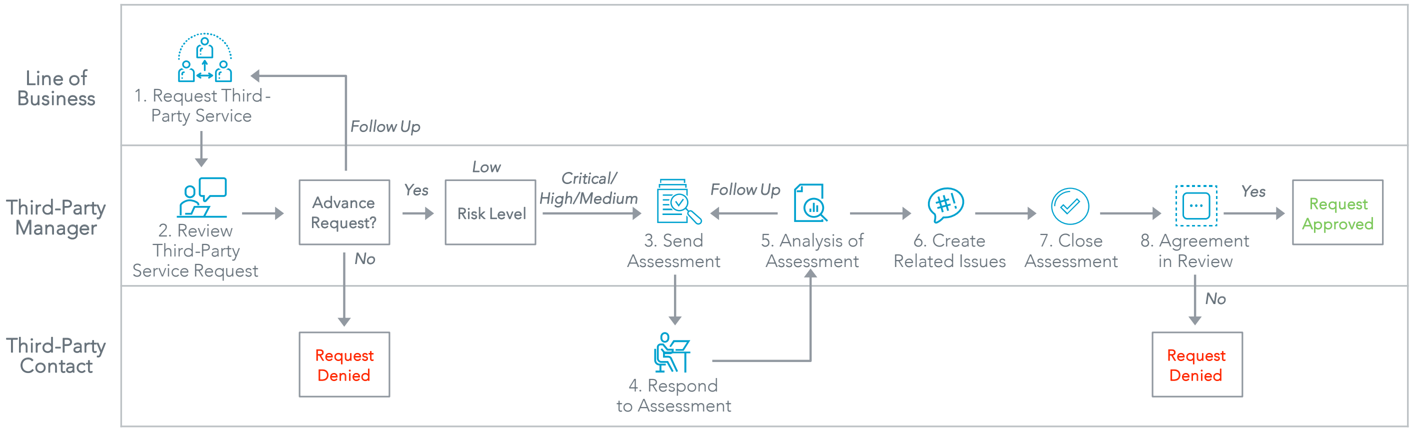
Automated questionnaires put an end to inefficient paper surveys and spreadsheets and simplify the assessment process for both organizations and their partners. Best Practices Configuration employs industry-standard questionnaires from Shared Assessments (SIG Core and SIG Lite) to further streamline the vendor assessment process.

Calculations & Scoring

Best Practices Configuration provides built-in calculations, rating tiers, scoring and other logic critical to an automated Third-Party Risk Program, including:

- Inherent Risk – Third-party responses to a pre-determined set of questions (that incorporate recommendations from the OCC and other governing bodies) determine a service's inherent risk.
- Automated Scoping – Based on the inherent risk score, ProcessUnity calculates the breadth and depth of the questions required for the initial third-party assessment.
- Assessment Review Rating – Every external assessment receives an Assessment Review Rating – a score calculated based on the number of High and Medium severity issues identified during the assessment process.
- Residual Risk – A third party's Inherent Risk Rating and most recent Assessment Review Rating determines a risk level based on how effectively each control performs.
- Ongoing Monitoring Schedules – Residual risk scores automatically determine ongoing due diligence frequency – annually, biennially or triennially.
- Issue Remediation – Issues identified during assessment analysis are assigned a severity rating. Based on the severity, the issues are assigned a remediation schedule.
- Preferred Response – Preferred/non-preferred response calculations allow for quick comparison against past questionnaires to quickly identify new risks in ongoing due diligence.

TPRM Onboarding Process Flow



ProcessUnity's Onboarding Request Workflow

Vendor Portal

ProcessUnity's Vendor Portal provides third parties with a secure, online environment to complete questionnaires, provide responses and comments, and attach supporting documentation. The easy-to-use interface, instructions and guidance improves vendor response time and response quality.

Interactive Dashboards & Reports

Built-in reports provide real-time visibility into the state of third-party risk and demonstrate to regulators the existence of a consistent, reliable and repeatable program. Interactive dashboards give visibility into ongoing risk assessment progress, the status of remediation activity and vendor ratings. Drill-down capabilities allow risk managers to quickly find the details in areas of concern. Best Practices Configuration contains 27 pre-built reports to track critical vendor and service-risk information, including:

- Vendor Criticality
- Vendor Assessment Status
- Assessment Findings
- Assessment History
- Issues
- Document Requests
- Action Items
- Compliance Ratings
- and more

Learn more about ProcessUnity VRM Best Practices Configuration. Contact us at info@processunity.com

Extensive custom reporting capabilities allow third-party managers to create management-level reports and individual dashboards through a simple-to-use interface*. With ProcessUnity, organizations gain program-level reporting that manual methods simply cannot provide.

Get Started

ProcessUnity's VRM Best Practices Configuration helps organizations effectively and efficiently identify and remediate the risks posed by third-party service providers. Combining ProcessUnity's single system for vendor-risk information and powerful automation with the pre-configured workflows, calculations, reporting and rapid deployment approach, organizations can quickly streamline their third-party risk management processes, reduce operational exposure, improve their vendor management and ensure the results of their VRM program will standup to regulatory scrutiny.

To learn more about ProcessUnity's VRM Best Practices Configuration, contact a ProcessUnity risk management expert at info@processunity.com or visit us online at www.processunity.com.

* *Configuration is not available for the Silver tier plan.*