# Best Practices Configuration Methodology

## ProcessUnity Third-Party Risk Management

Updated February 13, 2020



ProcessUnity

# TABLE OF CONTENTS

# 1. ABOUT THIS DOCUMENT

The following pages provide an overview of the methodology powering the Best Practices Configuration of ProcessUnity's award-winning and industry-recognized Third-Party Risk Management automation platform. The focus of this document is not on the point-and-click steps required to use the ProcessUnity platform, but instead on how to effectively run a Third-Party Risk Management program. Technical guides and documentation are available in the ProcessUnity platform's help system.

The Best Practices Configuration provides customers with a complete, quick-to-deploy program that can be modified over time using ProcessUnity's unparalleled configuration capabilities. The processes, workflows, calculations and guidance described herein have been developed by Third-Party Risk Management subject matter experts and perfected via hundreds of successful ProcessUnity customer deployments. ProcessUnity's "out-of-the-box" program delivers 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 the organization.

# 2. KEY DEFINITIONS

The following terms and acronyms are used throughout this document:

| Term | Definition |
|---|---|
| Agreement | Agreement is a general term used to describe negotiated arrangements between an organization and its third parties. Agreements include real estate contracts, general commercial contracts, managed-service contracts, non-disclosure agreements, privacy agreements, service-level agreements (SLAs), statements of work and more. |
| Line of Business (LOB) | Line of Business (LOB) employees request new third-party services for the organization and own the relationship with third parties. LOB users are not responsible for managing vendor assessments. |
| Personally Identifiable Information (PII) | Personally Identifiable Information (PII) can be used alone or with other sources to uniquely identify, contact or locate a single individual. Examples of PII include names, dates of birth, driver's license numbers, Social Security numbers, digital identities, passport number and credit card numbers. |
| ProcessUnity Platform (Platform) | The ProcessUnity Platform (Platform) is cloud-based software used to automate Third-Party Risk Management processes in an organization. |

| | |
|---|---|
| Protected Health Information (PHI) | Protected Health Information (PHI), also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care. |
| Standardized Information Gathering (SIG) Questionnaire | The Standardized Information Gathering (SIG) Questionnaire is a survey used to determine how third parties, vendors and suppliers manage security across industry-recognized control areas (domains). |
| Third-Party Contact (TPC) | A Third-Party Contact (TPC) is the primary point of communication at a third-party organization. Typically, TPCs complete due diligence assigned by Third-Party Managers. |
| Third-Party Manager (TPM) | Third-Party Managers (TPM) are the primary operators of an organization's Third-Party Risk Management program. In smaller organizations, TPMs perform analysis and risk management activities on third parties and may also serve as the ProcessUnity Application Administrator. In larger organizations, TPMs support Third-Party Analysts. |
| Third-Party Risk Management (TPRM) Program | Third-Party Risk Management (TPRM) Program describes the activities and applications that comprise the process of identifying and remediating risk posed by third parties, vendors and suppliers. |

## 3. THE THIRD-PARTY RISK MANAGEMENT FUNCTION

The Third-Party Risk Management (TPRM) function within an organization identifies and manages the risks posed by third parties, vendors and suppliers throughout the life of a service provider's relationship with the organization. The key objectives of a TPRM program are:

- Work closely with Lines of Business (LOBs) to identify risk throughout third party, vendor or supplier lifecycles;
- Increase organizational awareness of potential risks posed by third parties and propose recommendations to manage the risks identified;
- Inform leadership to help communicate third-party risk and the steps taken to mitigate those risks; and,
- Facilitate discussions between LOBs and Third-Party Contacts (TPCs) throughout assessment processes and risk-mitigation activities.

Consisting of one or many Third-Party Managers (TPMs), the Third-Party Management team works with various LOB employees and teams to effectively and efficiently understand and mitigate risk prior to signing service contracts and throughout the vendor relationship.

TPMs typically:

- Perform risk assessments and due diligence on third parties to identify and assess risks before the establishment of a contractual relationship;
- Conduct and validate ongoing risk oversight and track any associated remediation activities;
- Collect, manage and report relevant data related to third-party relationships; and,
- Compile reports related to ongoing third-party oversight and performance.

Each time a LOB proposes a new third-party service, the third party must be evaluated using a systematic level of due diligence. This due diligence identifies the controls in place at the proposed third party to mitigate the Inherent Risk identified during the initial stages of the onboarding process. Once due diligence is completed, the TPM compiles recommendations used to identify gaps and create remediation plans to ensure appropriate controls are in place. Additionally, these reviews help shape initial contracts or improve existing vendor performance.

The TPM also performs additional activities such as administrative maintenance of all approved third parties and ongoing monitoring of events that may trigger changes in a third party's risk profile.

Ultimately, an effective TPRM team:

- Tracks inherent and residual risk for all third parties
- Scopes, schedules and performs initial and ongoing due diligence based on a third party's risk profile
- Conducts information security assessments
- Identifies and reports on issues found during assessment processes

# 4. PROGRAM STRUCTURE

ProcessUnity's Best Practices Configuration data model includes pre-built relationships and workflows between key data elements and system users.

## 4.1 Third-Party Risk Management Data Model & Key Elements

Figure 1 below provides an overview of the relationship among the data elements in the Best Practices program:

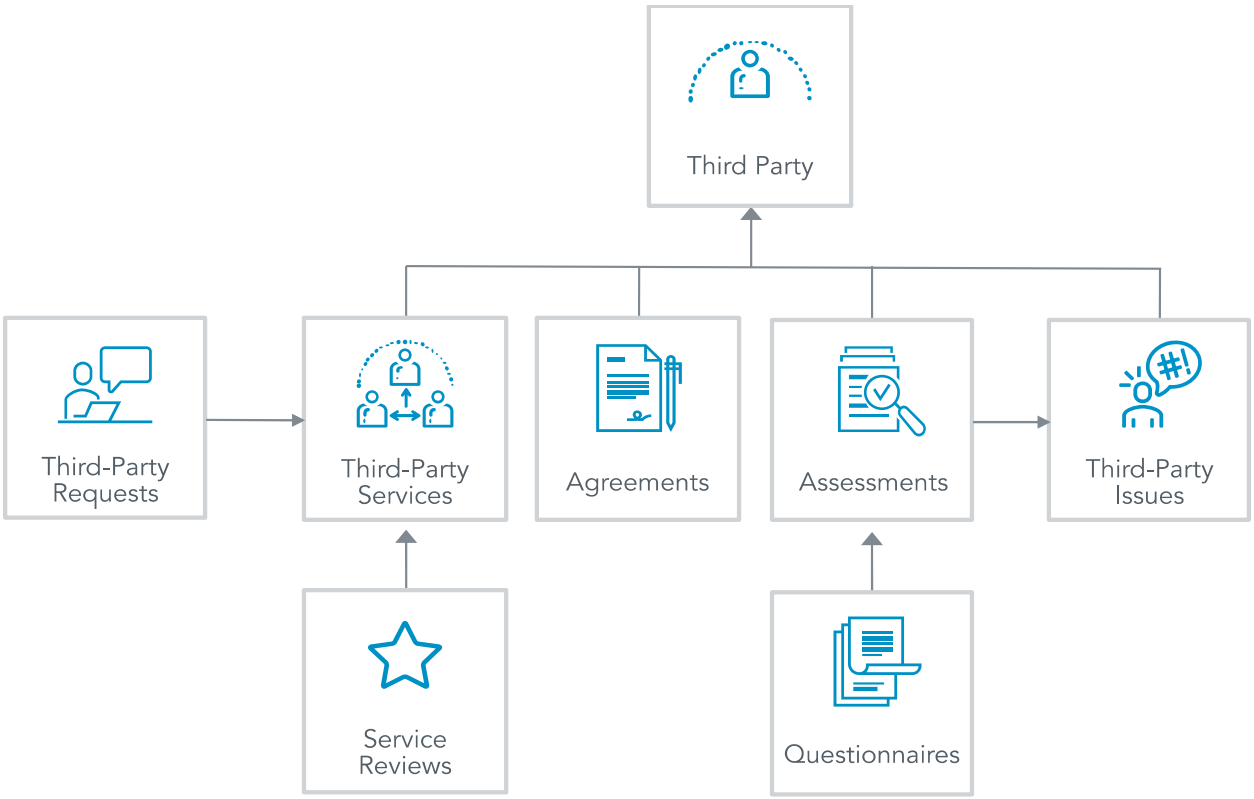


*Figure 1: The Third-Party Risk Management Data Model*

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

## 4.2 User Roles & Responsibilities

ProcessUnity's Best Practices Configuration includes four user types. Each role in the platform has the required permissions to complete key tasks throughout the TPRM lifecycle. The pre-configured system roles are:

| Role | Primary Responsibilities |
|---|---|
| Third-Party Manager (TPM) | Third-Party Managers are members of the TPRM team and are responsible for identifying and reducing risks posed by third parties, vendors and suppliers. |
| Line of Business (LOB) User | Line of Business Users request new third parties or services and manage relationships with their approved third parties. |
| Third-Party Contact (TPC) | Third-Party Contacts are the primary points of contact at third-party organizations. They typically complete the due diligence required by the TPRM team. |
| Application Administrator (ADM) | Application Administrators are responsible for maintenance and upkeep of the ProcessUnity TPRM platform. (Note: In smaller organizations, the Application Administrator can also be a Third-Party Manager.) |

The table below describes each system user's specific responsibilities at each phase in the TPRM program:

| R = Responsible, A = Accountable, C = Consulted, I = Informed | | | | | |
|---|---|---|---|---|---|
| Process Area | Process | ADM | LOB | TPM | TPC |
| Third-Party Requests | Complete and submit the third-party request form | - | R / A | C | - |
| | Review initial security assessment questions | - | C | R / A | - |
| | Confirm information is complete and accurate | - | C | R / A | - |
| | Send due diligence to TPC | - | I | R / A | I |
| Third-Party Due Diligence | Respond to SIG questionnaires | - | - | C | R / A |
| | Provide guidance to TPC while responding to SIG questionnaires | - | - | R / A | I |
| | Submit SIG questionnaire | - | - | I | R / A |
| | Review SIG questionnaires | - | - | R / A | C |
| | Identify issues | - | - | R / A | - |
| | Ensure responses are requested when needed | - | - | R | A |
| | Assign assessment review ratings | - | - | R / A | - |
| Third-Party Monitoring & Management | Resolve / mitigate issues | - | I | R / A | C |
| | Coordinate future assessments | - | - | R / A | - |
| | Update / manage third party and third-party service profiles | - | C | R / A | - |
| | Update / manage third-party contacts on third-party profiles | - | C | R / A | - |
| Agreements | Upload agreements and enter key dates | - | - | R / A | - |
| Third-Party Service Reviews | Send internal review of third-party services | - | I | R / A | - |
| | Respond to third-party service reviews | - | R / A | I | - |
| | Close third-party service reviews | - | R / A | I | - |
| TPRM Program Maintenance | Manage internal users | R / A | - | I | - |
| | Manage program configuration changes and updates | R / A | - | I | - |
| | Load / import data (if required) | R / A | - | I | - |
| | Maintain teams, roles and permissions | R / A | - | I | - |
| | Manage internal and external communications templates | R / A | - | I | - |

# 5. PROGRAM WORKFLOWS

Automation is critical to the success of an efficient and effective TPRM program. ProcessUnity's Best Practices Configuration includes numerous workflows that create a repeatable process for managing third-party risk – from initial service identification through contracts, ongoing vendor monitoring and termination.

## 5.1 Third-Party Onboarding Process

The onboarding process can require up to two reviews to make a "go" or "no-go" decision on a third-party service. The third-party service's Inherent Risk determines the level of initial due diligence. The assigned TPM decides if the Legal team needs to review agreements.

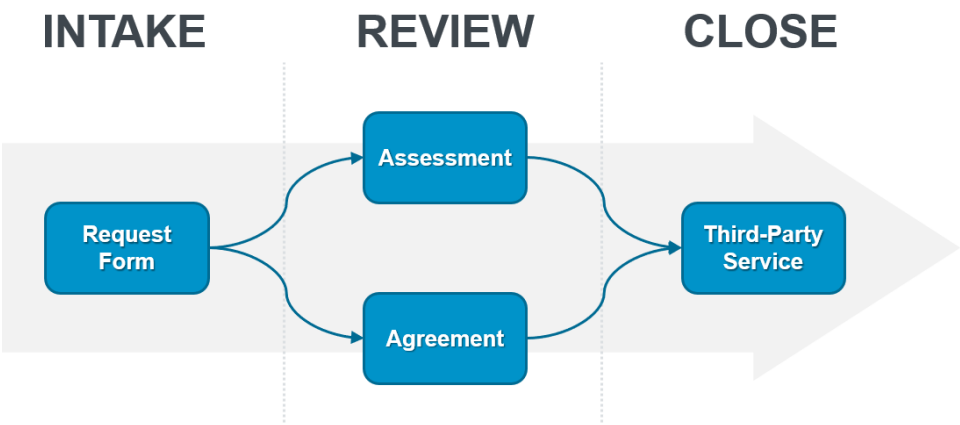


*Figure 2: The High-Level Onboarding Process*

Onboarding begins when the LOB emails or submits a request for a third-party service. Upon receiving the request, the TPM reviews it and determines the risk associated with the service. If the Third Party registers as **Medium**, **High** or **Critical** based on the Inherent Risk score, then the Third Party will be required to complete due diligence. The TPM sends the due diligence to the TPC and reviews the submitted responses. Based on the results, the TPM either approves or declines the service request.

Figure 3 below outlines the process flow for the third-party service onboarding process.

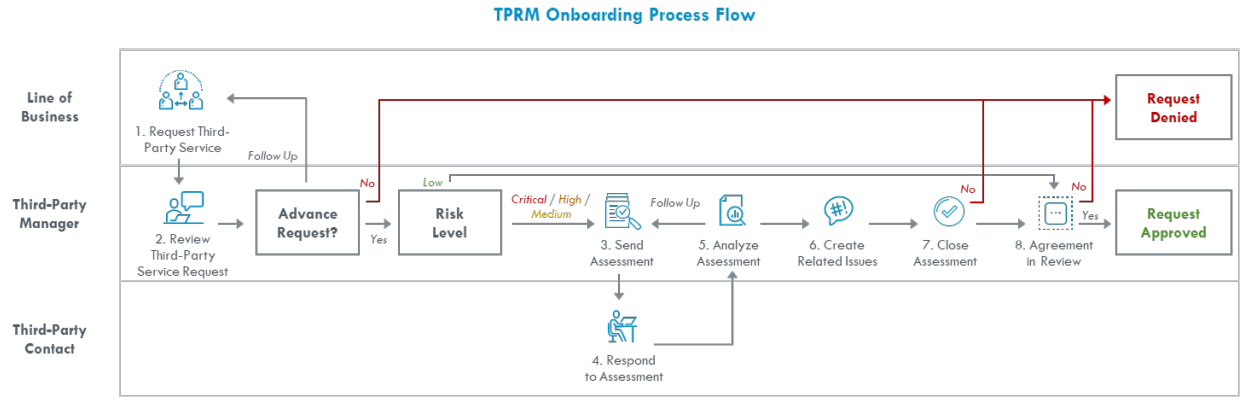


*Figure 3: Onboarding a Third-Party Service*

### 5.1.1 Submit Third-Party Service Request

To begin the third-party service request process, the LOB searches for all third parties managed by the TPM team to identify if an existing Third Party already provides a similar service. If the LOB cannot find the required service, they complete a third-party service request form within the ProcessUnity platform. The request form requires LOB users to answer a set of ten questions related to how the Third Party manages their security profile and their clients' data. (Refer to Section 6 of this document for a list of onboarding questions used to calculate Inherent Risk.) A TPM receives a notification when a third-party service request is submitted.

(Note: Organizations that do not choose to set up LOB users in the ProcessUnity platform typically email service requests to TPMs, who complete the third-party service request form on behalf of the business.)

### 5.1.2 Review Third-Party Service Request (and Scope Due Diligence)

Once received, the TPM reviews the third-party service request and determines whether to advance or decline the request. Based on scores resulting from selections on the service request form, ProcessUnity calculates the Inherent Risk of the requested service and automatically scopes the appropriate level of due diligence. (Refer to Section 6 of this document for the Inherent Risk calculation formula.) If the service's Inherent Risk is categorized as **Low**, it requires no further due diligence. If the third-party service is determined to be **Medium** or **High** risk, then due diligence is required (SIG Lite questionnaire). Intensive due diligence (SIG Core questionnaire) is required for third-party services deemed as **Critical** risk.

Please note that at this stage of the process, the TPM also determines if an agreement review will be required during the onboarding process. (For more details, see Section 5.1.8.)

### 5.1.3 Send Assessment

With due diligence properly scoped, the TPM sends the appropriate questionnaire using the ProcessUnity delivery system.

### 5.1.4 Complete Assessment

Via email, TPCs receive notification that they are required to respond to the due diligence request. A link in the email takes TPC directly to ProcessUnity's secure Vendor Portal where they can complete the questionnaire electronically. For new third-party services, TPCs are required to complete due diligence within 15 business days.

When TPCs submit the completed questionnaire, the TPM receives notification to begin the analysis of the assessment. At this point, no more changes can be made to the completed questionnaire.

### 5.1.5 Review Assessment

TPMs have 15 business days from the date it was submitted to review and analyze completed due diligence assessments. The assigned TPM ensures assessment completeness and accuracy. During the review, if the TPM determines one or more responses or documents do not meet the requirements of the business, the TPM initiates follow-up requests for further clarification from the TPC.

### 5.1.6 Create Issues

When TPMs identify risks to the business during assessment analysis and supporting documentation review, they create issues against the specific response or document. The TPM is responsible for logging the issue and assigning a severity based on the risk level.

### 5.1.7 Close the Assessment

After all issues are generated and analysis is completed, the TPM closes out the assessment. The ProcessUnity system generates an Assessment Review Rating based on the issues identified during analysis. The Assessment Review Rating, combined with the initial Inherent Risk tier, determines the third-party service's Residual Risk score, which establishes an ongoing assessment and due diligence cadence.

The TPM that managed the service assessment process remediates any identified issues against the required timeline.

After closing the assessment, the TPM generates a final assessment report and determines the next steps based on the organization's risk appetite and internal policies. At this point, a third-party service can be rejected, approved outright or approved via a leadership committee process. If an agreement is not required, ProcessUnity alerts the original LOB requestor of the final decision.

### 5.1.8 Review Agreements

If an agreement review is required, the TPM works with the organization's internal teams and the Third Party to negotiate and execute a contract. Once signed, the TPM loads the agreement into the ProcessUnity platform and logs the effective date and renewal date. The renewal date can automatically trigger notifications to allow proper time to perform internal checks before an agreement renewal.

## 5.2 Ongoing Program Processes

Third-Party Risk Management does not end with a signed contract for a new service – it is critical to continue to monitor third parties over time and throughout the business relationship. The TPRM team is responsible for identifying and logging changes as they occur. Figure 4 below outlines the three major process flows TPMs use to conduct ongoing due diligence – Third-Party Service Reviews, Issue Remediation and Third-Party Due Diligence.

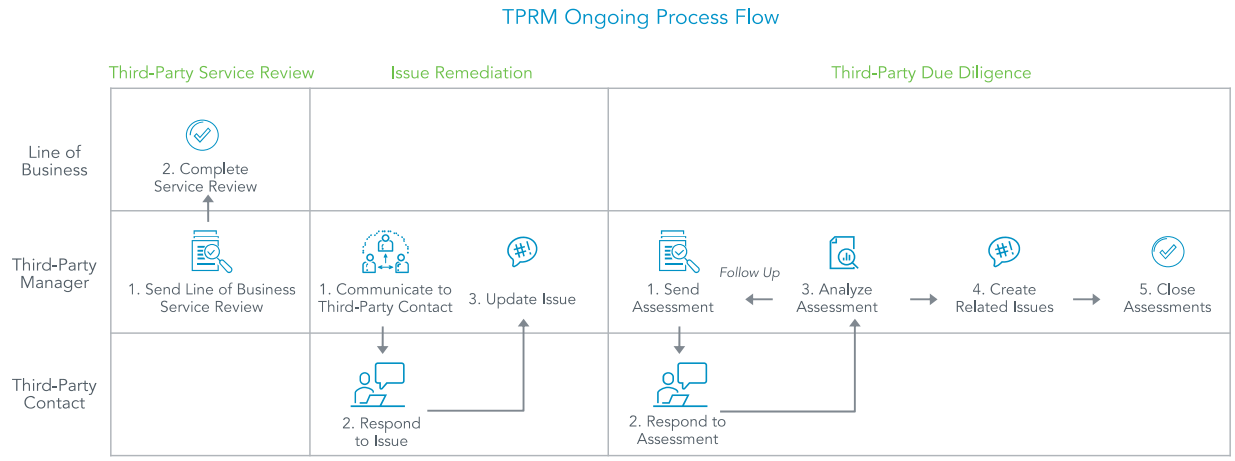


*Figure 4: Processes for Ongoing Monitoring*

### 5.2.1 Third-Party Service Reviews

Active third-party services are on an annual review cycle to monitor potential Inherent Risk changes. ProcessUnity sends notifications to appropriate LOBs requesting that they complete a third-party service review for each of their vendors. If the completed service review results in a change to the Third Party's Inherent Risk tier, the system will automatically change the due diligence scope and cadence and alert the TPRM team.

### 5.2.2 Issue Remediation

TPMs and TPCs work together to remediate any issues identified during due diligence processes. TPMs capture issues in the ProcessUnity platform and communicate them to TPCs for remediation. As the TPC takes steps to remediate the issues, the TPM receives confirmations and can accept or close the issue. If remediation is successful, an accepted issue reduces the identified risk level. Unsuccessfully remediated issues can also be accepted if the business agrees to acknowledge the risk and continue to use the service. The TPM monitors issue statuses until all issues have been resolved in line with the expected remediation plan.

### 5.2.3 Third-Party Due Diligence

Ongoing third-party due diligence process follows (and is similar to) the new service onboarding due diligence process described in Section 5.1.

As in the new service onboarding process, TPCs complete the assigned assessment questionnaire (SIG Lite or SIG Core) depending on the service's Inherent Risk. Third parties have 20 days to submit their completed due diligence. Once submitted, a system notification alerts the assigned TPM to perform the assessment analysis. The TPM reviews the submission to ensure completeness and accuracy. If one or more responses or documents are not satisfactory, the TPM logs a follow-up request for clarification.

The TPM can assign issues directly to assessment responses to indicate the risk(s) identified to the business. On a response-by-response basis, the TPM categorizes the severity of the identified issue. After completing the response analysis and identifying all of the issues, the TPM closes the assessment.

Completed assessments receive an Assessment Review Rating based on the issues identified in review. The Assessment Review Rating and the Third Party's Inherent Risk rating combine to determine a revised Residual Risk score, which reestablishes the assessment cadence and due diligence scope. All issues opened during the assessment appear on the third party's issue list for remediation. Issue ownership falls to the same TPM who managed the assessment process. The TPC is responsible for remediating the issues in the required timeframe.

The process flow ends with an automatically generated final assessment report that recommends whether a third-party service should be continued outright, continued with approval or terminated depending on the business' risk appetite and policies.

### 5.2.4 New Service Requests from Active Third Parties

In cases where a LOB requests a new or additional service from an active Third Party, any increase in assessment scope based on the Inherent Risk of the proposed service would require the Third Party to complete a new questionnaire. The cadence for ongoing due diligence would also be updated based on the calculations described in Section 6.1.

## 5.3 Service Termination

For third-party service terminations, the TPM updates the system record with a written attestation generated by the LOB owner. The attestation should detail that:

- The business has shared the intent to terminate with the Third Party;
- The TPC has acknowledged the receipt; and,
- The business confirms the TPC has executed all the applicable requirements for termination.

All termination documents are associated with the third-party service record in the ProcessUnity platform.

# 6. CALCULATIONS, RATINGS & REVIEW FREQUENCIES

This section outlines the various calculations, ratings tiers and other built-in logic featured in ProcessUnity's Best Practices Configuration.

## 6.1 Inherent Risk

Inherent Risk is automatically calculated during the new third-party service onboarding process. A service's Inherent Risk tier is determined by the answers to a set of questions in ProcessUnity's Request for Third-Party Service Form. The ten questions consider factors relating to Confidentiality, Criticality, Geography and Spend. Each question is assigned a point score based on the LOB's answer. The questions and scoring system are as follows:

| Question | Scoring |
|---|---|
| Is the service essential to the business operations of our company? | ▪ Yes – 12 points<br>▪ No – 0 points |
| What is the expected annual financial contract amount of the third-party service? | ▪ Greater than $500,000 – 6 points<br>▪ Less than $500,000 – 0 points |
| Will all parts of the service be performed domestically? | ▪ Yes – 0 points<br>▪ No – 2 points |
| How difficult would it be to replace this service with an alternative? | ▪ Difficult – 2 points<br>▪ Easy – 0 points |
| What is the expected annual volume of records that will be accessed, processed, stored or transmitted by this Third Party? | ▪ More than 50,000 – 2 points<br>▪ Less than 50,000 – 1 point<br>▪ N/A – 0 point |
| Is any part of the third-party service being provided subject to any regulatory or compliance requirements? | ▪ Yes – 2 points<br>▪ No – 0 points |
| Does this Third Party store, process or transmit Personally Identifiable Information (PII) or Protected Health Information (PHI) as a part of this service? | ▪ Yes – 2 points<br>▪ No – 0 points |
| As a part of this service, will any of our data be stored in the cloud? | ▪ Yes – 2 points<br>▪ No – 0 points |
| As a part of this service, will the Third Party have access to our IT network or technical infrastructure? | ▪ Yes – 2 points<br>▪ No – 0 points |
| Will any part of the service be outsourced as part of this agreement? | ▪ Yes – 2 points<br>▪ No – 0 points |

Based on the total sum score resulting from the service request form, ProcessUnity will automatically determine the Inherent Risk classification – **Critical**, **High**, **Medium**, or **Low**:

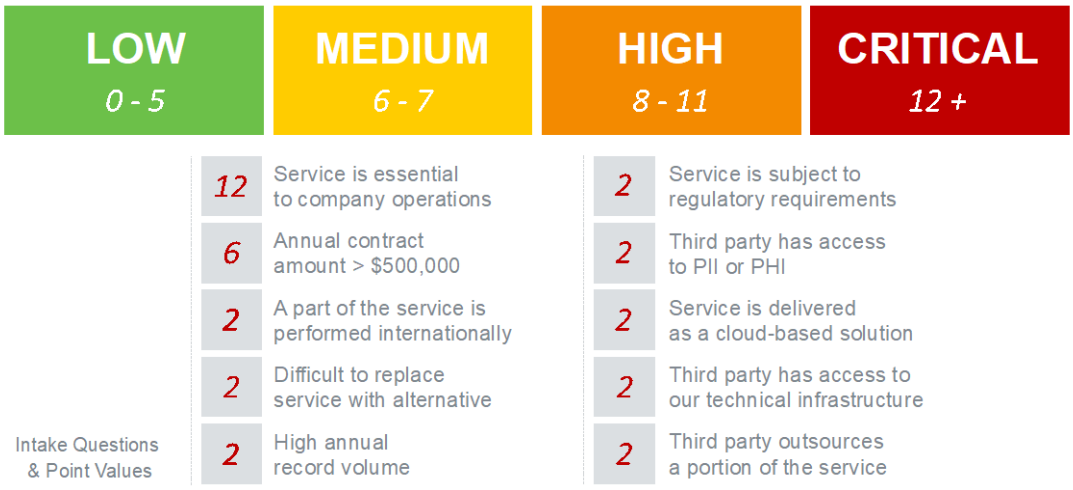


*Figure 5: Inherent Risk Scoring*

The Inherent Risk calculation plays a key role in scoping assessments, calculating Residual Risk and determining assessment frequency. Figure 6 details ProcessUnity's methodology:

| Inherent Risk | | Previous Assessment Review Rating | | Residual Risk | Assessment Scope | Assessment Frequency |
|---|---|---|---|---|---|---|
| CRITICAL | + | No Prior Review | = | Critical | SIG Core | ASAP |
| | | Unsatisfactory | | Critical | SIG Core | Annual |
| | | Needs Improvement | | Critical | SIG Core | Annual |
| | | Satisfactory | | High | SIG Lite | Annual |
| HIGH | + | No Prior Review | = | High | SIG Lite | ASAP |
| | | Unsatisfactory | | High | SIG Lite | Biennial |
| | | Needs Improvement | | High | SIG Lite | Biennial |
| | | Satisfactory | | Medium | SIG Lite | Biennial |
| MEDIUM | + | No Prior Review | = | Medium | SIG Lite | ASAP |
| | | Unsatisfactory | | Medium | SIG Lite | Biennial |
| | | Needs Improvement | | Medium | SIG Lite | Biennial |
| | | Satisfactory | | Low | SIG Lite | Triennial |
| LOW | + | N/A | = | Low | N/A | N/A |
| | | N/A | | Low | N/A | N/A |
| | | N/A | | Low | N/A | N/A |
| | | N/A | | Low | N/A | N/A |

*Figure 6: Inherent Risk Determines Residual Risk, Assessment Scope and Assessment Frequency*

Additional notes:

- When calculating the Inherent Risk of a Third Party that provides multiple services, Inherent Risk defaults to the highest Inherent Risk of all active services provided.
- If no previous Assessment Review Rating exists for a Third Party, the Residual Risk will default to the Inherent Risk. This situation can occur if the Third Party is active, but no due diligence was performed prior to the formation of a formal TPRM program. Since there was no prior due diligence, the TPM decides the next due diligence date.
- If a new assessment is performed on an existing Third Party as a result of an additional third-party service being requested, the Inherent Risk of the new service will be factored into the Third Party's risk.

## 6.2 Assessment Review Rating

Every external assessment receives an Assessment Review Rating which is calculated based on the number of **High** and **Medium** severity issues identified during the assessment process. There are three possible Assessment Review Ratings:

- **Satisfactory**: Given to an assessment when there are zero high-severity issues and only one medium-severity issue. Controls evaluated are reasonably adequate, appropriate and effective to manage risks and meet information security objectives.

- **Needs Improvement:** Given to an assessment when there is one high-severity issue or up to five medium-severity issues. Although specific control weaknesses were noted, the controls evaluated are adequate, appropriate and effective to manage risks and meet information security objectives.

- **Unsatisfactory:** Given to an assessment when there are two or more high-severity issues or greater than five medium-severity issues. Controls evaluated are not adequate, appropriate or effective to manage risks and meet information security objectives.

## 6.3 Residual Risk

Due diligence is performed continuously throughout the lifecycle of a Third Party. The frequency and scoping of the third-party assessments are based on Residual Risk, which is calculated using the Third Party's Inherent Risk score and most recent Assessment Review Rating. The Residual Risk can be categorized as **Critical**, **High**, **Medium** or **Low**.

There are three ways a Third Party can be categorized with **Critical** Residual Risk:

1. The Inherent Risk is **Critical** and the last Assessment Review Rating is categorized as **Unsatisfactory**.
2. The Inherent Risk is **Critical** and the last Assessment Review Rating is categorized as **Needs Improvement**.
3. The Inherent Risk is **Critical** and no prior review was ever performed on the Third Party.

There are four ways a Third Party can be categorized with **High** Residual Risk:

1. The Inherent Risk is **Critical** and the last Assessment Review Rating is categorized as **Satisfactory**.
2. The Inherent Risk is **High** and the last Assessment Review Rating is categorized as **Unsatisfactory**.
3. The Inherent Risk is **High** and the last Assessment Review Rating is categorized as **Needs Improvement**.
4. The Inherent Risk is **High** and no prior review was ever performed on the Third Party.

There are four ways a Third Party can be categorized with **Medium** Residual Risk:

1. The Inherent Risk is **High** and the last Assessment Review Rating is categorized as **Satisfactory**.
2. The Inherent Risk is **Medium** and the last Assessment Review Rating is categorized as **Unsatisfactory**.
3. The Inherent Risk is **Medium** and the last Assessment Review Rating is categorized as **Needs Improvement**.
4. The Inherent Risk is **Medium** and no prior review was ever performed on the Third Party.

There are two ways a Third Party can be categorized with **Low** Residual Risk:

1. The Inherent Risk is **Medium** and the last Assessment Review Rating is categorized as **Satisfactory**.
2. The Inherent Risk is categorized as **Low**.

## 6.4 Ongoing Due Diligence Frequency

Due diligence is performed continuously throughout the lifecycle of most third parties. Due diligence frequency – **annually**, **biennially** or **triennially** – is calculated based on a Third Party's Residual Risk score.

- If the Residual Risk is **Critical**, then external due diligence is performed **annually**.
- If the Residual Risk is **High**, then external due diligence is performed **biennially**.
- If the Residual Risk is **Medium** and the previous Assessment Review Rating is **Unsatisfactory** or **Needs Improvement**, then external due diligence is performed **biennially**.
- If the Residual Risk is **Medium** and the previous Assessment Review Rating is **Satisfactory**, then the external due diligence is performed **triennially.**
- If the Inherent Risk is **Low**, then **no external due diligence** is required.

## 6.5 Ongoing Due Diligence Scoping

Before sending ongoing external due diligence to a Third Party, the assessment type needs to be determined. When a Third Party is initially approved, the ProcessUnity platform decides which assessment scope will be sent in future assessments. The scope is driven by the Third Party's Inherent Risk and Residual Risk:

- If the Residual Risk is **Critical**, the Third Party will receive the maximum-scoped due diligence (SIG Core).
- If the Residual Risk is **High** or **Medium**, the Third Party will receive the minimally scoped due diligence (SIG Lite).
- If the Residual Risk is **Low** and the Inherent Risk is **Medium**, the Third Party will receive the minimally scoped due diligence (SIG Lite).
- If the Residual Risk is **Low** and the Inherent Risk is **Low**, the Third Party will not receive any due diligence.

## 6.6 Issue Severity Ratings

Issues identified during assessment analysis are assigned a severity rating by the TPM. Based on these severities, the issues are assigned to the following remediation schedule:

- **High** severity issues must be addressed and remediated within 12 months of discovery.
- **Medium** severity issues must be addressed and remediated within 18 months of discovery.
- **Low** severity issues are documented and an action is recommended but not required.

# 7. For More Information

For additional information or questions on ProcessUnity's Best Practice Configuration, please contact your ProcessUnity Account Manager or email us at info@processunity.com.