

# THIRD-PARTY RISK MANAGEMENT BEST PRACTICES

Expert Advice for an Effective & Efficient Program



# CONTENTS






- 03 Introduction
- 06 Program Building Blocks: Onboarding & Ongoing Monitoring
- 10 Inherent Risk Best Practices
- 15 Residual Risk and Review Cadences
- 17 Getting Outside Help: External Content and Managed Services
- 19 Assessing Your Program's Maturity and Identifying Steps to Improve



# 1. INTRODUCTION

ProcessUnity specializes in helping its clients automate their Third-Party Risk Management (TPRM) programs. Through the years, we have helped hundreds of customers implement efficient and effective processes that drive risk out of their businesses. Our team developed this guide to showcase a number of the best practices we see in modern TPRM programs. Our hope is that you find a few “nuggets of wisdom” that you can take back to your company, program and team and continue to mature your TPRM processes.

In the following pages, this document will:

-  Define the building blocks of TPRM programs – both pre- and post-contract
-  Examine the importance of inherent risk calculations
-  Demonstrate how residual risk helps determine ongoing review cadences
-  Outline how to augment your team with external expert content and managed services
-  Help you rate your program’s maturity and provide next steps for improvement

## Getting Grounded: Third-Party Risk Management Defined

Before we get into the meat of this guide, let’s take a minute to get on the same page regarding TPRM.

Most companies have some semblance of Governance, Risk and Compliance (GRC) management in place today. Governance is all about setting goals and objectives for the organizations and setting the tone from the executive team and board of directors.

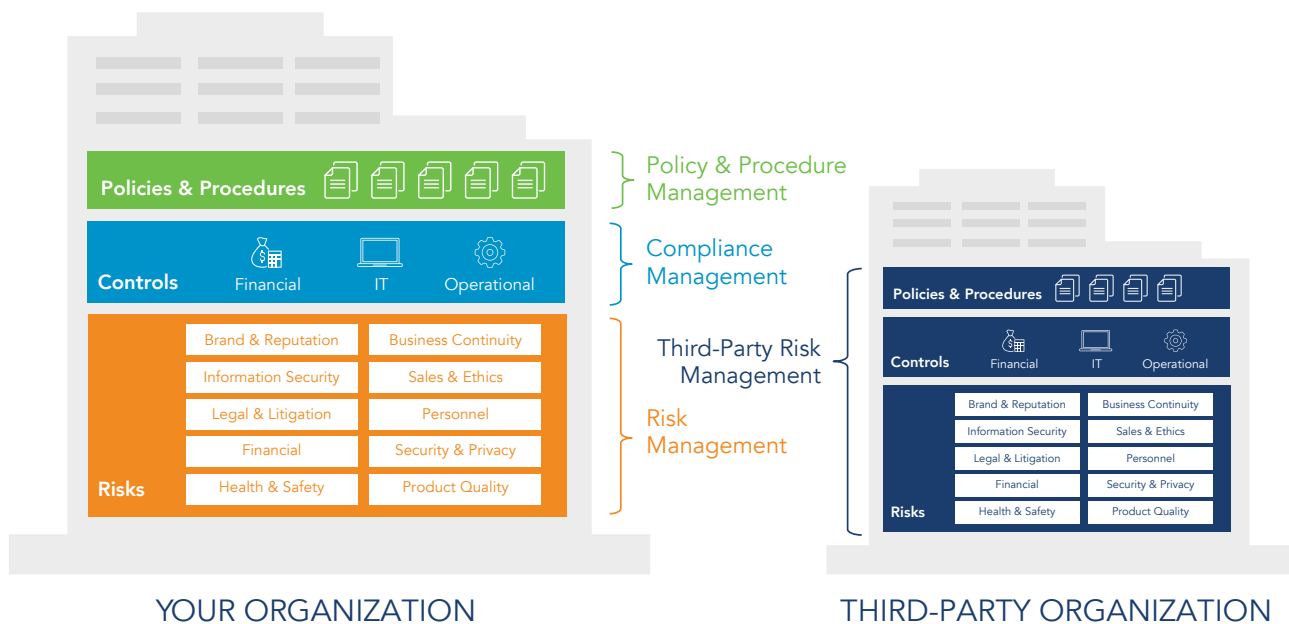


Figure 1.1 – Third-Party Risk Management

Risk Management examines what could go wrong and potentially prevent the organization from achieving its goals. Wherever possible, companies put controls in place to mitigate those risks to protect against negative outcomes.

Compliance is all about following the rules – whether they be laws, regulations, standards or operating guidelines outlined by government or industry regulators. Companies establish policies and procedures to ensure that employees follow proper steps for everyday business operations.

These days, organizations work with many outside vendors, third parties and suppliers. It’s important to make sure that any outside business partner has its act together in terms of governance, risk and compliance. If they don’t, their actions (or lack thereof) could come back to bite you. Third-Party Risk Management is putting a spotlight on the policies, procedures, risks and controls of the outside companies you work with.

It’s important for third parties to be just as buttoned up and conscientious as your organization is. A history of effective collaboration and strong relationships isn’t enough. Companies need to examine the businesses of their partners to ensure those vendors are doing things as they should. Trust, but verify.

“People don’t do what you **expect** but what you **inspect**.”

- Louis V. Gerstner, Jr.

Ultimately, your company will be held accountable for the missteps or failures of your business partners, and the responsibility to ensure your third parties are conducting business responsibly is yours.

Monitoring and inspecting your third parties is increasingly important to good corporate governance.

### The Third-Party Risk Lifecycle

There are three primary components required to launch a successful program:

1. Onboarding
2. Due diligence
3. Ongoing monitoring



Figure 1.2 – The Third-Party Risk Management Lifecycle

Most organizations struggle with the administration heavy burdens associated with initial onboarding and due diligence that happens pre-contract, and with ongoing monitoring that happens post-contract.

The cumbersome administrative tasks associated with these key steps bogs many companies down, especially companies with smaller risk management teams.

Teams that overcome the challenges of these initial lifecycle steps can expand their program and potentially transform their organization's TPRM efforts from a cost center into an ROI center where:

- Underperforming vendors can be weeded out and swapped for higher performing partners;
- More favorable contracts can be negotiated to improve service and lower costs; and,
- SLA violations can be easily identified, penalties collected, and that information can be used in future negotiations.

When the onboarding, due diligence and ongoing monitoring building blocks are complete, teams can easily transition into more mature activities that generate real value and make their program shine.

## TPRM Challenges Organizations Face Today

Companies face myriad challenges today related to TPRM. A few of them include:

- **Tiering Vendors:** Which vendors are the most critical? The riskiest?
- **Engaging the Business:** How can you involve lines-of-business, executives and board members in TPRM processes?
- **Storage:** What's the best way to organize and store the data required to properly vet your vendors?
- **Depth:** Where do you draw the line? Fourth parties? Fifth?

It's not going to get easier:

- Companies work with more third- and fourth-party vendors than ever before.
- Hackers and malicious actors keep inventing new ways to harm businesses.
- New regulations keep popping up – and existing ones continue to evolve.
- Vendors are buckling from the sheer volume of due diligence requests.

The bottom line: Organizations need to pay a great deal of attention to third-party risk, and they need to implement a program that reduces inefficiencies to drive out as much risk as possible. In the next section, we'll introduce foundational building blocks to a world-class TPRM program.

## 2.

# PROGRAM BUILDING BLOCKS: ONBOARDING & ONGOING MONITORING

When building or up-leveling a TPRM program, it's important to recognize that work happens both before and after signing a contract.

- **The pre-contract onboarding process:** usually consisting of an inherent risk assessment and initial due diligence review – is designed to keep as much risk out from the start.
- **Post-contract processes:** ongoing monitoring and service reviews – are put in place to make sure nothing has changed with vendors over time and to check that vendors are delivering their services in accordance with expectations.

Throughout pre- and post-contract work, there will be issues that arise. TPRM teams need capabilities to identify, track and remediate those issues appropriately.

**An important note:** The base process flows described in the coming pages will vary from organization to organization based on company size, the maturity of the program, industry and more. There is no "one-size-fits-all approach," and TPRM teams should adapt these models to fit their specific business requirements.

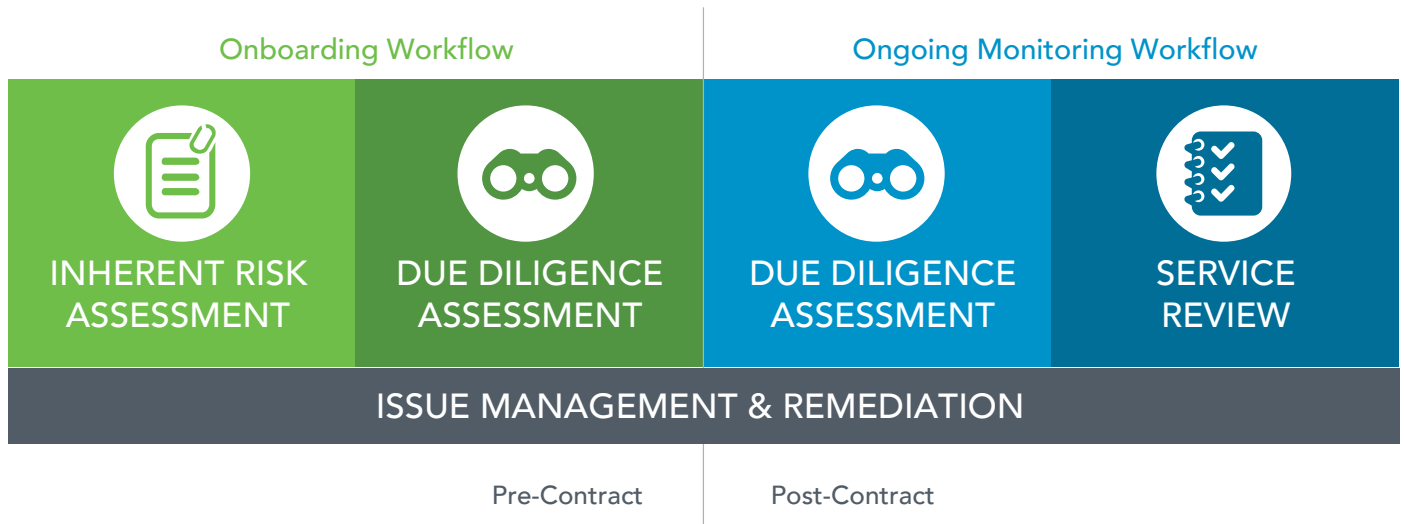


Figure 2.1 – Pre- and post-contract TPRM process flows

## Vendor Onboarding Workflow

There are three primary actors in the vendor onboarding workflow:

**1. Line-of-Business (LOB) User:** A member of the organization (HR, finance, legal, etc.) who needs to onboard a new vendor

**2. Third-Party Manager:** The person or team that vets the vendors, responsible for keeping as much risk out of the organization as possible

**3. Third-Party Contact:** The vendors' representative(s) that respond(s) to due diligence and assessment requests throughout the process

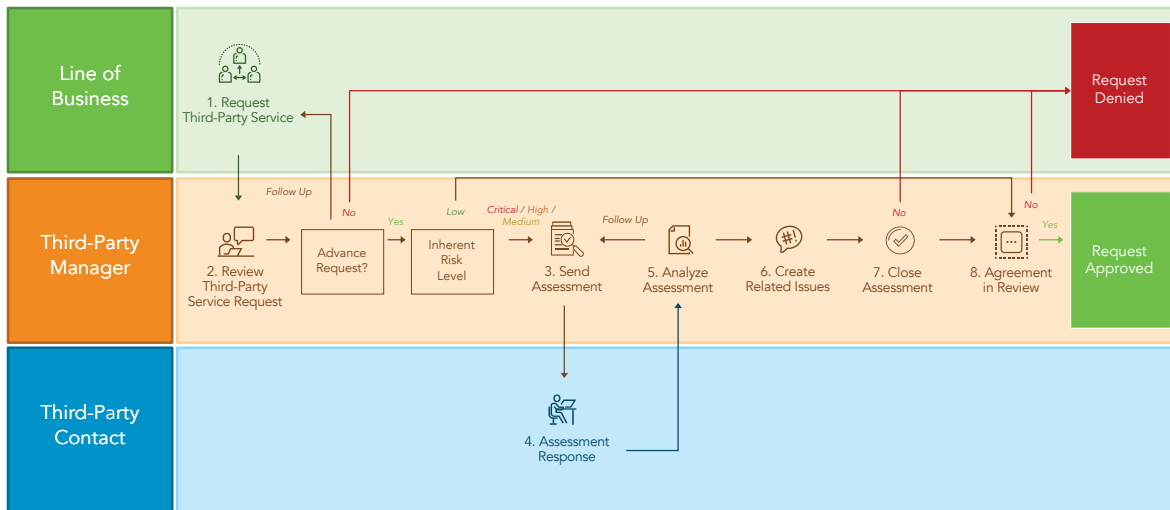


Figure 2.2 – The vendor onboarding workflow

The onboarding workflow triggers when the organization needs to contract with a new vendor. Here's how the process works:

1. A new office is opening in the EU, and there is a need for a payroll provider who can pay the employees internationally. [Step 1] A payroll or HR person (LOB user) initiates a request to the third-party risk management team.
2. [Step 2] The third-party manager works with the LOB user to determine how much risk there is in working with the vendor (inherent risk assessment) and checks to see if a similar service or vendor is already under contract (to avoid duplication).
3. Based on the initial inherent risk rating, an assessment questionnaire [Step 3] is sent to the vendor requesting it provide more in-depth information [Step 4] for the organization to analyze and evaluate.

- a. Not all vendors will have to go through the entire process. The inherent risk some vendors pose may be determined to be low. Lower-risk vendors may not have to respond to due diligence questionnaires.
- b. More risky vendors will need to go through a deeper assessment process.
4. The completed assessment is received and analyzed [Step 5], issues are then created [Step 6], and the assessment is closed [Step 7].
5. Ideally everything is good, the request is approved, and contracts and agreements are executed [Step 8].

The details of the onboarding workflow process will vary among companies based on each individual company's risk profile. Some companies may have additional steps that include routing specific assessment responses to subject matter experts (SMEs) for cybersecurity or to a financial specialist to determine that a vendor's financial viability is acceptable. Different paths exist for different organizations.

## Ongoing Monitoring Workflow: Periodic Due Diligence

Following the signing of contracts, the due diligence process repeats periodically to make sure the vendor continues to operate within acceptable risk levels. The ongoing monitoring flow is a subset of the onboarding process minus the interaction with LOB user and contract signatures. The duration of time between assessments varies greatly for different third parties depending on business type, risk profile and how risky vendors are. (We'll discuss how residual risk can determine ongoing review cadences later in this guide.)

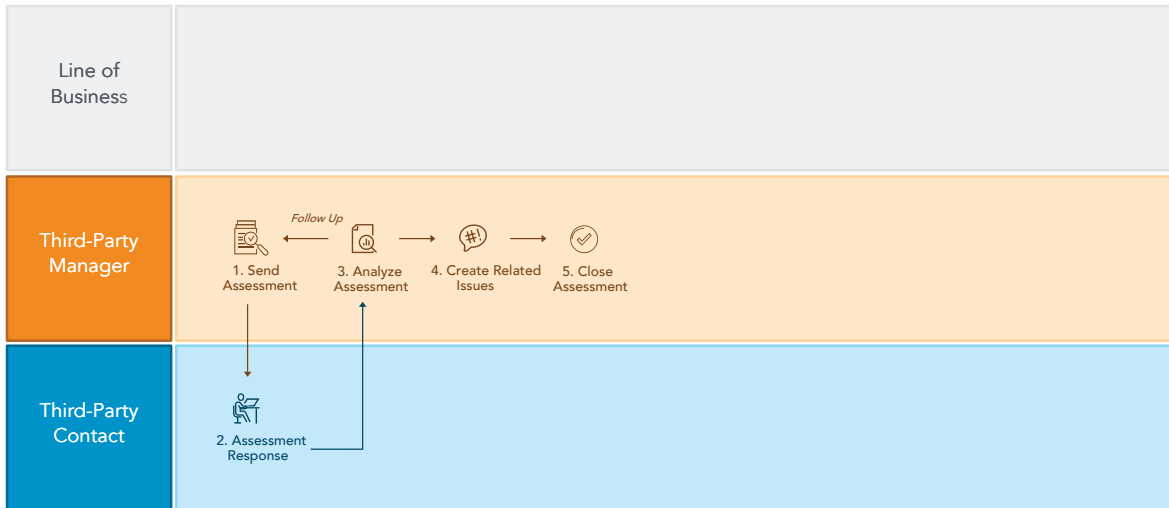


Figure 2.3 – The ongoing monitoring process flow

## Vendor Service Reviews

Performed periodically, vendor service reviews help organizations determine if third parties are performing as expected. Sometimes service reviews reveal opportunities to renegotiate contracts or switch to vendors that are a better organizational fit. This process is a two-way conversation between the third-party manager and the team or department consuming the vendor service.

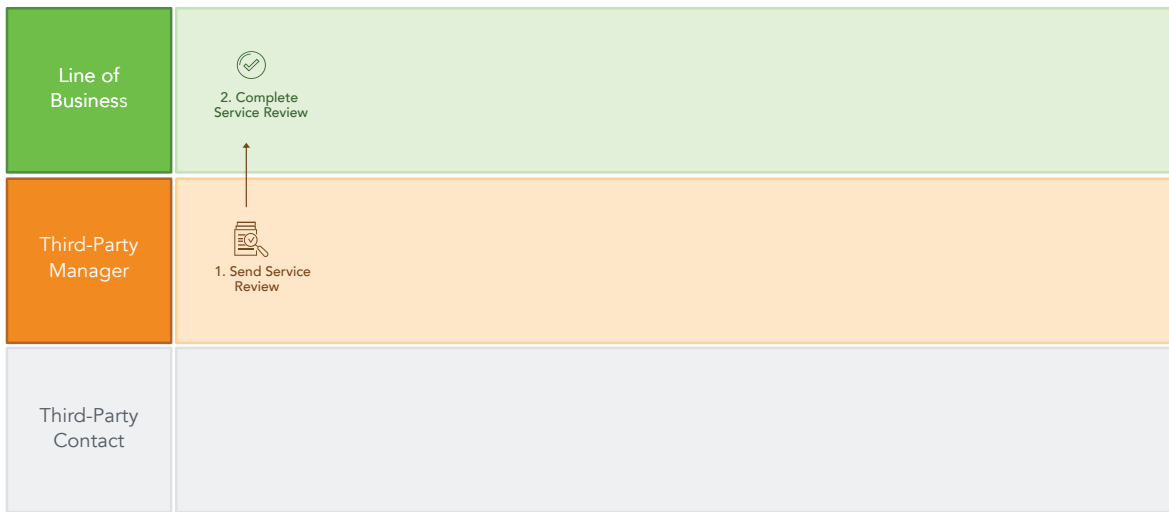


Figure 2.4 – The vendor service review workflow

## Issue Management and Remediation

Interaction between an organization’s team and vendors provides opportunities to flag existing and latent issues, revisit them during reviews and contract negotiations, and use them to help put things into future contracts and service level agreements (SLAs) that will help protect the organization.

# 3.

## INHERENT RISK BEST PRACTICES

Determining a vendor's inherent risk level is a critical step in determining how much initial due diligence is required during initial onboarding and how often periodic assessments are performed for ongoing monitoring. Riskier vendors should get more attention and inherent risk calculations determine who warrants that extra attention.

### Risk Domains Help Define Inherent Risk Questions

Typically, inherent risk is determined via communication between the LOB user requesting a vendor service and the third-party manager. There is usually some sort of short questionnaire or form completed by the requestor. There are nine risk domains TPRM teams can look at to determine the right mix of inherent risk questions for their company:

- **Identity:** Is this vendor who it says it is? Is it a real company?
- **Information security:** Is the vendor handling sensitive information/data?
- **Geographic:** Where is the vendor located? Could its location lead to a supply chain disruption?
- **Financial:** Is the vendor paying its bills? Will it continue to be in business in a year?
- **Business Continuity:** Does vendor have a plan in place in case something goes wrong?
- **Fourth Party:** Is the vendor working with fourth parties? What risk do its fourth parties present?
- **Reputation:** Is there negative news about the vendor that may cause reputational and brand damage by associating with them?
- **Compliance:** Is the vendor in compliance with rules and regulations?
- **Conflict of interest:** Are there any personal conflicts of interest with vendor personnel? Does the business have Unidentified Beneficial Owners to consider?

### Build Your Inherent Risk Questionnaire:

Based on the type of business they're in, organizations should craft a set of questions using these risk domains that will ultimately help calculate vendors' risk level. Here's a sample of ten common questions third-party managers can ask their LOB users:

1. What is the expected annual contract amount? *(Risk domains: financial, business continuity)*
2. Is the third-party service performed domestically? *(Risk domain: geographic)*
3. Is the service essential to the operations of the company? *(Risk domain: business continuity)*
4. How difficult would it be to replace this service? *(Risk domain: business continuity)*
5. What is the expected annual volume of records that will be accessed, processed, stored, or transmitted by this third party? *(Risk domain: information security)*
6. Is any part of the third-party service being provided subject to any regulatory and/or compliance requirements? *(Risk domain: compliance)*
7. Does this third-party store, process, or transmit personally identifiable information (PII) or protected health information (PHI) as part of this service? *(Risk domain: information security)*
8. Is the service delivered as a cloud-based solution? *(Risk domain: information security)*
9. Does this third party have access to our IT network or technical infrastructure? *(Risk domain: information security)*
10. Does the third party outsource any part of the service? *(Risk domains: information security, geographic)*

## Define Your Risk Tiers

The questions asked and answers obtained will ultimately result in an inherent risk score. That score should fit into a category or tier. Tiering systems across organizations will vary based on the unique identity of each organization. Examples of common inherent risk tiering systems include:

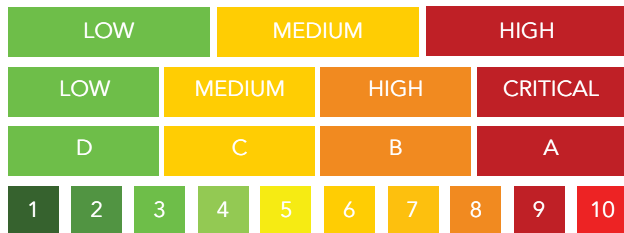


Figure 3.1 – Risk tier examples

## Build a Scoring System

Once a risk tier system is determined (we'll use Low, Medium, High and Critical for our purposes), work needs to be done to assign points to the risk domain questions so that vendors can be scored and designated into appropriate risk tiers.

When reviewing the ten sample questions outlined previously, Question 3 jumps out as the most important.

### Question 3: Is the service essential to the operations of the company?

Clearly, if the answer to this is yes, the vendor should be placed in the Critical inherent risk tier.

But things get trickier with the other nine questions. Many organizations establish structures where the combination of answers in conjunction with each other lead to tier designations. Establishing a system like this can take a lot of time in online meetings and conference rooms – it's important to take the time to get it right because inherent risk plays a big role throughout your program.

So, the answer to one question may mean an automatic Critical designation, and answers to a number of other questions in conjunction with each other may also add up to Critical designation.

To explore this a bit further. If the answer to Question 3, "Is the service essential to the operations of the company?" is yes, it is assigned 12 points, and reaches the Critical threshold. A vendor would also be deemed critical if the answers to six different questions each generate 2 points.

2 Points	How difficult would it be to replace this service with an alternative?
2 Points	Is any part of the third-party service being provided subject to any regulatory / compliance requirements?
2 Points	Does this third-party store, process or transmit PII or PHI as part of this service?
2 Points	Is the service delivered as a cloud-based solution?
2 Points	Does this third party have access to our IT network or technical infrastructure?
+ 2 Points	Does the third party outsource any part of the service?
<hr/>	
= 12 Points	Is the service essential to the operations of the company?

Figure 3.2 – Assigning point values to inherent risk questions

In this example, the scoring system is clearly and logically structured, and was designed with the organization's specific needs and considerations at the forefront during development.

RISK CLASSIFICATION VALUES

RISK CLASSIFICATION VALUES	
Low: 0-5	Medium: 6-7
High: 8-11	Critical: 12+
Intake Questions	Point Values
Service is essential to company operations	12
Annual contract amount >\$500,000	6
A part of the service is performed internationally	2
Difficult to replace service with alternative	2
High annual record volume	2
Service is subject to regulatory requirements	2
Third party has access to PII or PHI	2
Service is delivered as a cloud-based solution	2
Third party has access to our technical infrastructure	2
Third party outsources a portion of the service	2

Figure 3.3 – Building an inherent risk scoring system

Before deploying the scoring system, it's important to check the math against a sampling of your vendor population.

	MAJOR BANK	RECORDS SHREDDER	LANDSCAPING CONTRACTOR
Essential to operations	YES (12 Points)	NO	NO
Contract > \$500,000		NO	NO
Performed internationally		NO	NO
Difficult to replace		YES (2 Points)	NO
High record volume		YES (2 Points)	NO
Subject to regulatory requirements		YES (2 Points)	NO
Access to PII or PHI		YES (2 Points)	NO
Cloud-based solution		NO	NO
Access to technical infrastructure		NO	NO
Outsources a portion of the service		NO	YES (2 Points)
<b>TOTAL SCORE</b>	<b>12</b>	<b>8</b>	<b>2</b>
<b>RISK TIER</b>	<b>CRITICAL</b>	<b>HIGH</b>	<b>LOW</b>

Figure 3.4 – Testing an inherent risk scoring system

Testing is a key part of the scoring system development process, and answers the question, “Does this make sense for us?”

In test scenarios, a major bank, a records shredder and a landscaping contractor are all scored. The company's bank is essential to operations and therefore deemed a Critical vendor. The answers to the remaining questions aren't even needed.

The records shredder is a little different. It's not essential, not a big contract, and performed domestically. However, the vendor is difficult to replace, it will touch a high volume of records, have personal identifiable information to shred, and there will be regulatory issues to consider. All of these answers lead to 8 points, which leads to a High-risk designation.

At the other end of the spectrum is the company responsible for snow plowing in the winter and facility landscaping during warmer months. The only points they scored were earned because they outsource to a vendor that plants flowers in the spring. The vendor is not a risk to the company and designated in the Low risk tier.

The system was designed and successfully tested, and now the low, medium, high, and critical designations can be used to scope the amount of due diligence for vendors—the due diligence depth the company does with each vendor.

LOW 0 - 5	MEDIUM 6 - 7	HIGH 8 - 11	CRITICAL 12 +
No Further Due Diligence Required	Light Due Diligence Required	Medium Due Diligence Required	Intensive Due Diligence Required

Figure 3.5 – Use inherent risk scores to auto-scope due diligence

For a low risk vendor, no due diligence is required; the contract is signed, and business engaged.

As the organization engages with medium, high, and critical risk vendors more time will be spent on and a deeper intensity will be part of the assessments.

## Learn More About Inherent Risk

For a deeper dive into inherent risk best practices, download ProcessUnity's guide, [How to Quantify and Manage Inherent Risk for Third Parties](#).

[Click Here](#)

### QUESTIONNAIRES

There have been interesting changes to assessment questionnaires over the past few years.

In the early days of TPRM, companies would have a single assessment for all vendors – a **one-size-fits-all** approach. The questionnaires were long and used to assess all vendors regardless of the risk they posed. It was overkill for low-risk and small vendors; it was not enough for critical vendors.

Because the one size fits all approach did not work well, companies evolved to have **multiple questionnaires** – this was more of a small, medium, large approach. Deep questionnaires were sent to high-risk vendors and lighter questionnaires were reserved for lower-risk vendors. There were issues with maintaining multiple question sets, however.

**Self-scoping** questionnaires followed the small, medium, large approach. These questionnaires scoped automatically based on the risk tiers or changed on the fly based on vendors' answers to questions. These smart questionnaires can show or hide questions or sections of questions based on inherent risk tier and answers to previous questions. Self-scoping questionnaires help minimize the number of questions that need to be answered by the vendor and analyzed by the TPRM team.

Most recently, **self-scoring** questionnaires have been enhanced with self-scoring capabilities where the questionnaire is assessed in real time. These questionnaires, through an automation process and a set of preferred responses, generate issues and follow-up tasks that help the third-party management team focus on what is most important.

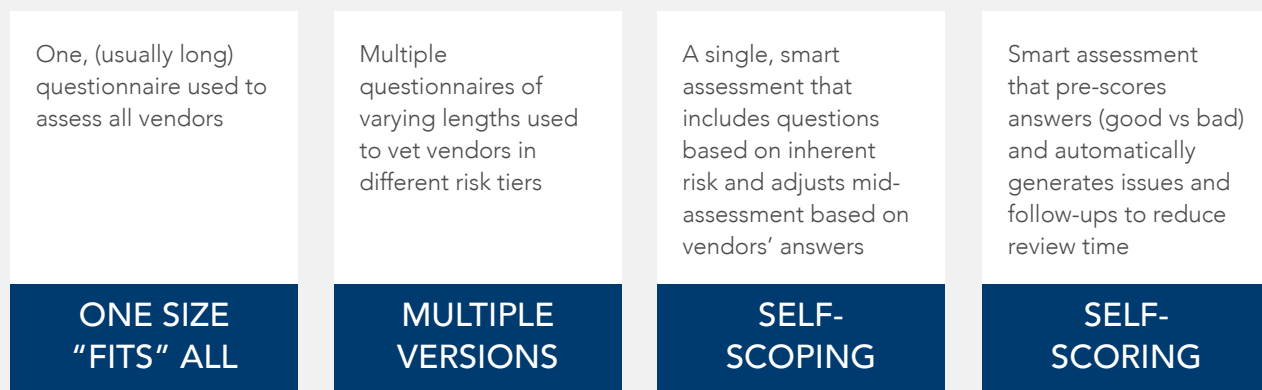


Figure 3.6 – The evolution of the TPRM assessment questionnaire

For a more in-depth look at how assessment tools have evolved, download [ProcessUnity's guide, The Evolution of the Third-Party Due Diligence Questionnaire](#).

# 4.

## RESIDUAL RISK AND REVIEW CADENCES

With the inherent risk scoring system in place, it can be used to determine residual risk, and to set up the organization's post-contract review cadences, defining how often and how deep the company needs to go with ongoing monitoring moving forward.

### Residual Risk Determines Scope and Frequency

Take the vendor's initial inherent risk score and combine it with the score from the previous assessment.

#### Inherent Risk Categories

- Critical
- High
- Medium
- Low

#### Assessment Review Rating

- **No Prior Review:** Company is a new vendor or has never completed an assessment review
- **Unsatisfactory:** Company performed poorly in last assessment review
- **Needs Improvement:** Company did okay, but needs to improve
- **Satisfactory:** Company passed and performed well in most recent assessment

Combining the inherent risk rating and the assessment review rating determines a residual risk score. This will determine how often assessments need to be performed and how deep the assessment needs to be.

Let's look at what this means for critical vendors. A critical vendor with:

- **No Prior Review** will be rated Critical for residual risk, required to submit to the deepest due diligence, and the assessment will be required immediately.
- An **Unsatisfactory** review will be rated Critical for residual risk, required to submit the deepest due diligence, and the assessment will be required annually.
- A **Needs Improvement** rating will be rated Critical for residual risk, required to submit the deepest due diligence, and the assessment will be required annually.
- A **Satisfactory** assessment will have its residual risk rating lowered to High and will be required to submit less-intense due diligence annually.

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

Figure 4.1 – Residual risk calculation for critical vendors

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 4.2 – Residual risk determines scope and frequency of periodic due diligence

As vendors perform better compared with their previous assessment ratings, their residual risk score gets dropped down, and their assessments become lighter and less frequent.

Many third-party management teams are small and have limited resources but want to improve their programs and expand their abilities or team. There's help: third-party risk management programs can be augmented with external expert content and managed services.

SIG: A standard information gathering questionnaire published by the [Santa Fe Group's](#) global industry membership organization [Shared Assessments](#). There are two standard versions of the questionnaire, the in-depth SIG Core with 850 questions and the less intrusive SIG Lite with 350 questions. SIG questionnaires are updated annually to address emerging security and privacy challenges, regulatory changes, new trends, and updated best practices in third-party risk management.

# 5.

## GETTING OUTSIDE HELP: EXTERNAL CONTENT AND MANAGED SERVICES

### Expert Content

There are a number of organizations providing expert content that can be included into third-party management programs. Increasingly, organizations are pulling information from cybersecurity ratings services and financial health scores to validate what vendors are saying in their assessments. Examples of expert content include:

**Cybersecurity ratings:** Companies like BitSight, RiskRecon and SecurityScorecard ping vendors' infrastructures, look for holes, and assign scores.

**Financial health scores:** RapidRatings and Dun & Bradstreet examine companies' finances to determine if they pay their bills (on time or at all) and assign scores.

**Negative news feeds:** To address reputational risk, Refinitiv examines if companies are in the news for reasons they shouldn't be.

**Anti-money laundering (AML) and terrorism financing:** Refinitiv provides insight into these issues.

**Assessment questionnaires:** Shared Assessments is a non-profit that provides the SIG Core and SIG Lite

questionnaires, which are the industry standard. A consortium of organizations have come together to agree on an industry standard assessment template and many vendors have standardized their answers on the template to make the process easier.

**Assessment Databases/Utilities:** Organizations like TruSight, which is focused on banking assess the vendors that frequently work for banks and then provides completed assessments for a fee, relieving banks of the necessity to perform that work themselves – essentially outsourced assessment services.

By incorporating outside resources, TPRM teams gain virtual analysts that can compare expert ratings against submitted due diligence and shine a light on a discrepancy before it becomes a real issue. Score or ratings changes can also be used post-contract, especially in between periodic due diligence. TPRM teams can set alerts when changes occur across any of these content sources to serve as virtual watchdogs to keep an eye on vendors for continuous ongoing monitoring.

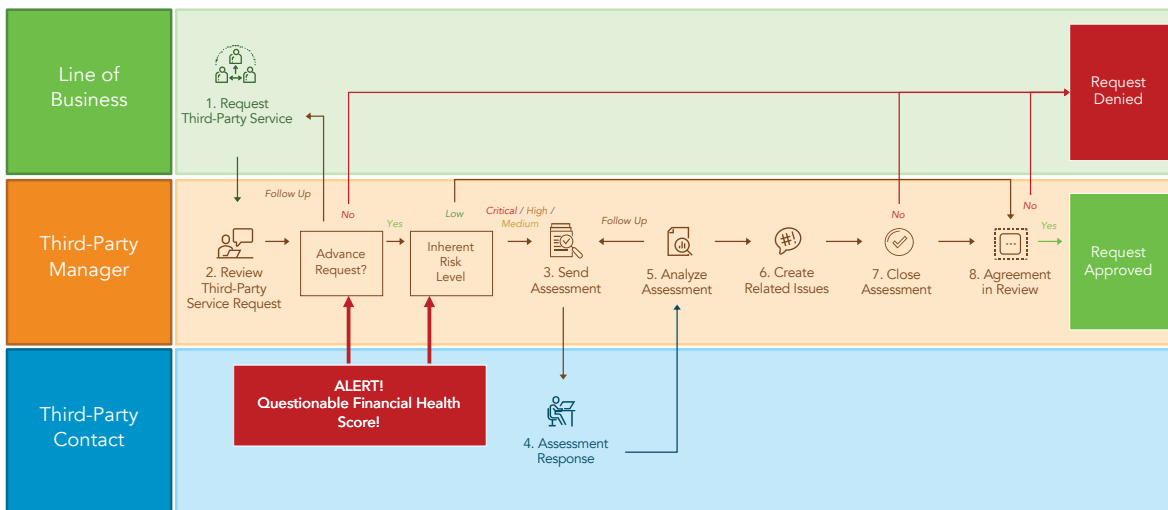


Figure 5.1 – Expert content serves as a virtual assistant during the onboarding process

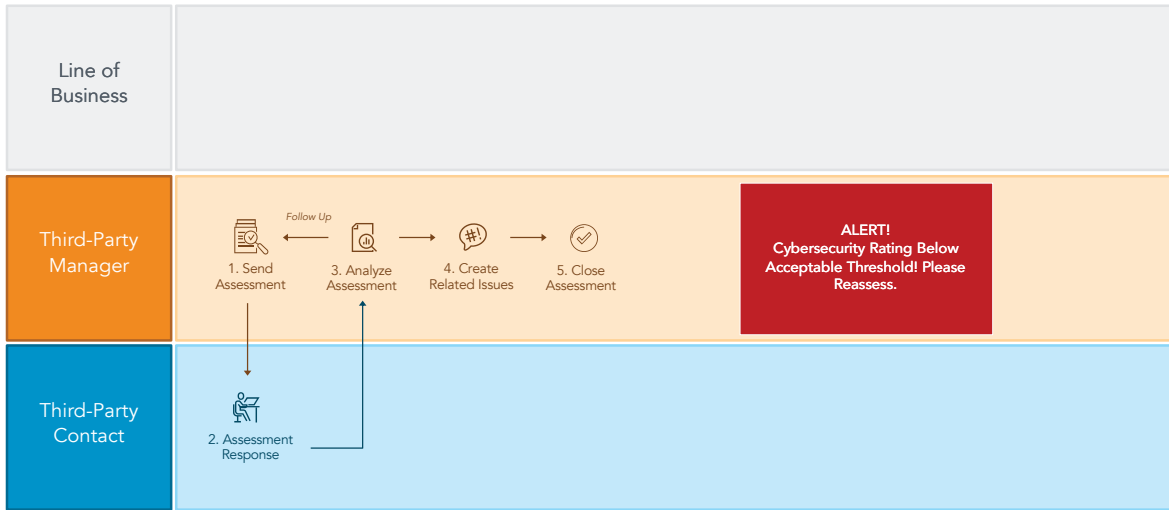


Figure 5.2 – Expert content alerts TPRM teams to changes in vendor status in between periodic due diligence

## Managed Services

Another way organizations are augmenting their team is through managed services. Companies work with consulting partners, typically organizations such as EY, Crowe or Grant Thornton, or boutique firms like CastleHill Risk Solutions in the USA or DVV or Cybersel in Europe that provide outsourced assessments for a portion of an organization's vendor population.

## Ultimately, However, You Own The Risk!

Even though assessment work is being performed by another organization, work still needs to be done and their findings need to be inspected.

# 6.

## ASSESSING YOUR PROGRAM'S MATURITY AND IDENTIFYING STEPS TO IMPROVE

Programs cannot be improved without understanding where you are today and defining where you want to go in the future.

### Determining Where You Are on the Maturity Curve

**Informal programs:** Heavy on spreadsheets and no involvement of LOB users.

**Reactive programs:** A small team that leverages a one-size-fits-all questionnaire and has only minor involvement from LOB users and little executive support.

**Proactive programs:** A formal team, with a defined program that performs some inherent risk calculations and uses inherent risk calculations to scope assessments and assign scores. Proactive programs use inherent risk to determine residual risk, they capture, manage, and track issues throughout the process, and they incorporate automation to streamline administration tasks.

**Optimized programs:** Mature programs with a high level of engagement with LOB users and executives that executes vendor service reviews, incorporates fully automated processes, trend analyses, and reporting. These programs perform ROI-based activities such as negotiating better contracts, adding SLAs into contracts, tracking SLAs, and bringing in external data to augment the program and help create more holistic views of vendors. Optimized programs incorporate continuous improvements to increase efficiency and manage the changing landscape.

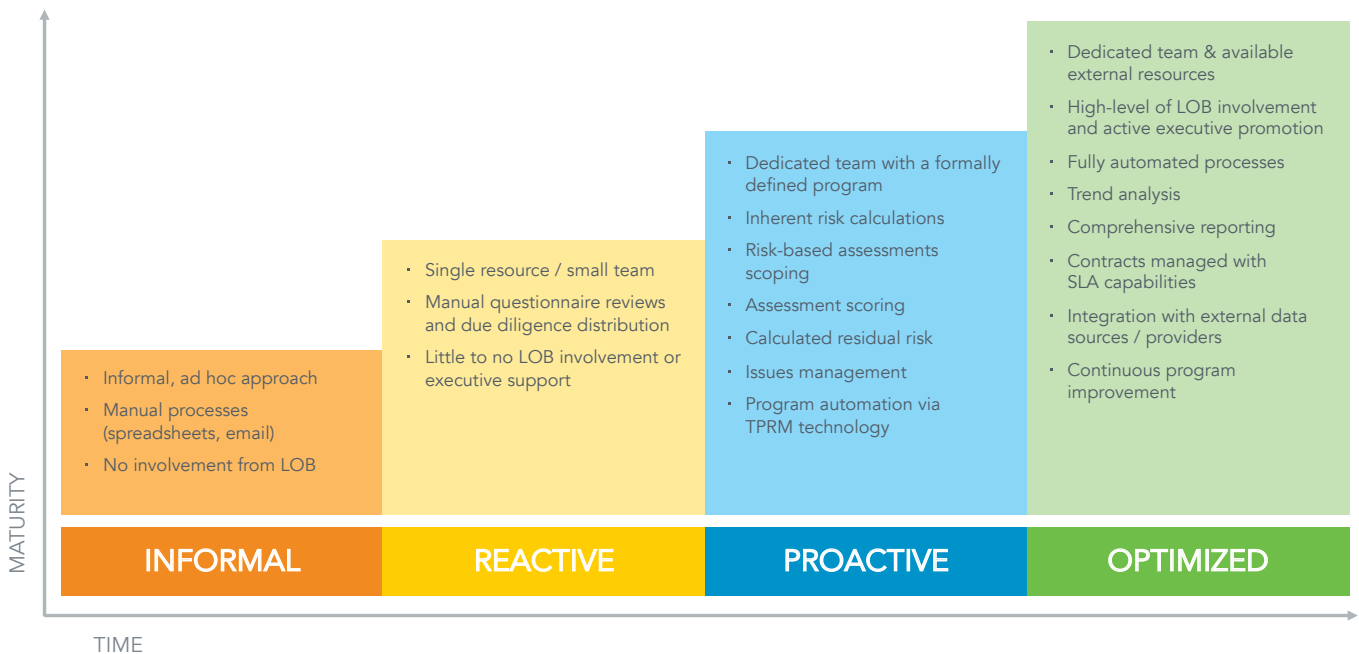


Figure 6.1 – The Third-Party Risk Management Maturity Model

## Take steps to advance your program (and your career)

Here are the steps you can take to move your program to the next level:

**Informal to Reactive program:** The key advantage in moving from informal to reactive is a blank slate. Find peers in the industry that are “better” than you are; ask how they are running their programs and find out what mistakes they made so you can avoid them. Formalize your program. Document your workflows and inherent risk scoring system. Surface results (and issues) to the executive team.

**Reactive to Proactive program:** Get rid of spreadsheets and email. Establish a third-party risk management system to manage data and automate manual tasks. Define inherent risk and residual risk. The key advantage here is your experiential knowledge regarding what is and what is not working. Push aside what is not working and focus on what is.

**Proactive to Optimized program:** When your organization reaches the proactive level, seek to increase LOB involvement (use LOB involvement to help with inherent riskscores early in the process and with performance reviews after contracts have been signed). Begin looking beyond early phases of vendor risk management lifecycle to focus on ROI generating opportunities and incorporate contract management and SLA tracking. The advantage here, especially for highly-regulated organizations, is that at this stage your organization should have consistency with your regulators and audits should be more routine and less challenging, which will lead to regulators having confidence in your organization.

**Optimized to Better Optimized:** When your organization reaches the top of the mountain, it has all of the data it needs to make better business decisions around contracts and negotiations and put KPIs, SLAs and other performance metrics in place. Continue to transform a cost-of-doing-business into an ROI center for the organization.

INFORMAL	REACTIVE	PROACTIVE	OPTIMIZED
<ul style="list-style-type: none"> <li>Formalize your program</li> <li>Document, document, document</li> <li>Socialize program's charter with executives</li> <li><b>Advantage: Blank slate</b></li> </ul>	<ul style="list-style-type: none"> <li>Nix the one-size-fits all questionnaire</li> <li>Implement a repository for TPRM data</li> <li>Calculate inherent and residual risk</li> <li>Look to automation</li> <li><b>Advantage: Leverage your recent experience to determine what's working...and what's not working</b></li> </ul>	<ul style="list-style-type: none"> <li>Increase LOB involvement and executive promotion</li> <li>Extend beyond onboarding and due diligence</li> <li>Improve contract management and SLA tracking</li> <li>Incorporate external data into onboarding and continuous monitoring</li> <li><b>Advantage: Consistency builds confidence with regulators</b></li> </ul>	<ul style="list-style-type: none"> <li>Focus on cost reduction and vendor service quality</li> <li><b>Advantage: Improved negotiation power based on accurate, actionable data on vendors' ability to meet KPIs, SLAs and other performance metrics</b></li> </ul>

Figure 6.2 – Keys to maturing your TPRM program

These are truly achievable goals. No matter where you are in your vendor risk maturity there is always an opportunity for growth and improvement: you will find that your program is one that will mature over time, increasing in value as you gain experience.

## Conclusion

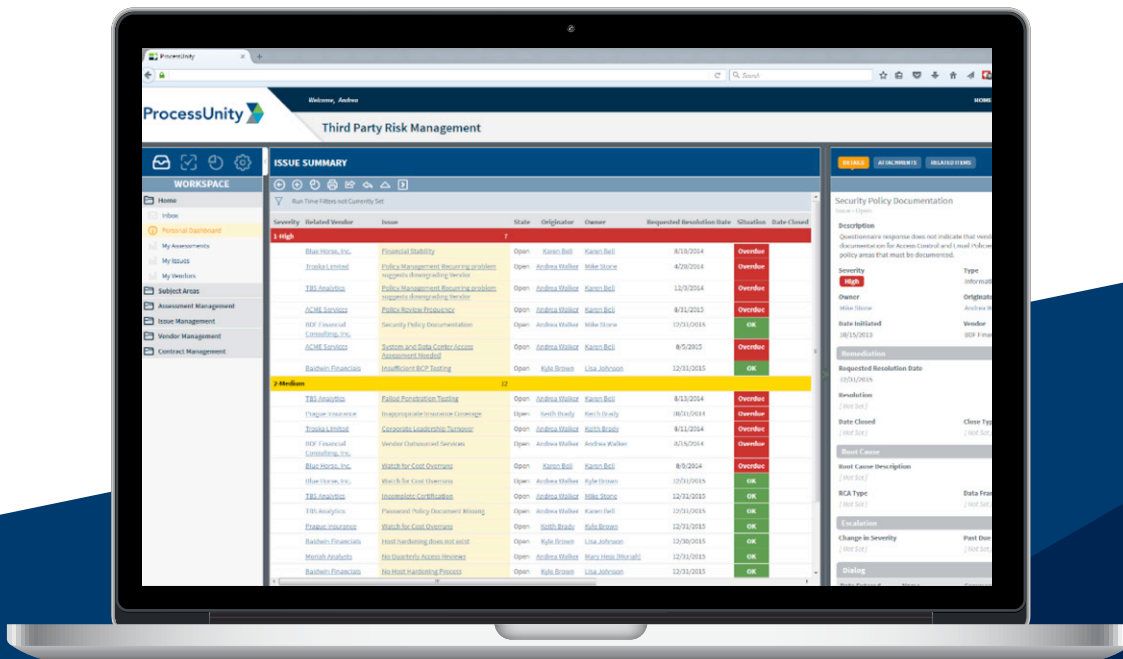
By implementing these best practices, you will be well on your way to a successful TPRM program and ProcessUnity is here to help you along the way. While there is no silver bullet to eliminate risk in its entirety, you will find by working together with our experts, we can prepare your organization to meet any future changes and challenges to your vendor landscape with confidence. We are a leading provider of Third-Party Risk Management software tools that organizations use to automate and streamline their programs. We work with organizations of all sizes, with different levels of maturity, helping them advance their programs to realize greater value and reduce more risk. To learn more about ProcessUnity Vendor Risk Management visit us at [www.processunity.com/automate](http://www.processunity.com/automate).


## About ProcessUnity

ProcessUnity is the leader in third-party risk management automation. ProcessUnity Vendor Risk Management provides:

- Programs for organizations of all sizes and maturity
- Built-in best practices
- Unparalleled subject matter expertise
- Short deployment times
- A documented history of successful client partnerships with hundreds of successful implementations

Learn more about ProcessUnity Vendor Risk Management at [www.processunity.com/automate](http://www.processunity.com/automate).





## More Third-Party Risk Management Guides

Enjoy this guide? Visit [www.processunity.com/resources](http://www.processunity.com/resources) for more best-practice guides, videos and ebooks on third-party risk management.



[www.processunity.com](http://www.processunity.com)



[info@processunity.com](mailto:info@processunity.com)



978.451.7655



Twitter: @processunity  
LinkedIn: ProcessUnity



ProcessUnity  
33 Bradford Street  
Concord, MA 01742  
United States