

Third-Party/Vendor Risk Management Policy Guidelines

Based on the third-party risk management lifecycle



Table of Contents

Introduction	4
Upfront Policy Considerations	6
Getting Started	7
How to Use the Lifecycle-Based Third-Party/Vendor Risk Management Policy	8
Section 1: Best Practices for Third-Party or Vendor Risk Management Policy Content and Structure	9
Know your regulatory requirements	9
Understand how, or if, policies are enforced in your organization	9
Understand your organization’s policy writing requirements, format, and style	9
Keep it general	10
Don’t include processes or procedures	10
Less is often more	12
Watch your language	12
Use a language structure consistent with your organization’s culture	12
Use active and direct words	13
Define terms	13
Make it clear who does what	13
Follow the third-party/vendor risk management lifecycle	14
Refer to other policies	15
When it doubt, leave it out	15
Ask for stakeholder review and feedback	15
Looks count and so do spelling and grammar	16
Section 2: Understanding Policy Content	17
Policy Content and Flow	
1 Overview and Background	18
2 Statement of Purpose	18
3 Policy Statement	18
4 Terms	18
4.1 Third-Party/Vendor	
4.2 Third-Party Risk Management and Oversight	
5 Scope	19
5.1 Not in Scope	
5.2 Pre-Existing Third-Party Relationships	
6 Approach to Third-Party Risk Management	20
7 Third-Party Risk Governance	20
7.1 Oversight	
7.1.1 Policy Management and Approval	
7.1.2 Approval of Critical Third Parties	
7.1.3 Periodic Review of Critical Third Parties	
7.1.4 Staffing and Resources	
7.2 Accountability: Roles and Responsibilities	21
7.2.1 The Board of Directors	
7.2.2 Senior Management	
7.2.3 Third-Party/Vendor Risk Management	
7.2.4 Third-Party/Vendor Owners	
7.2.5 Independent Reviewers	
7.2.6 Legal Team or Counsel	22

7.3 Documentation	
7.4 Reporting	
7.5 Independent Review	23
8 Risk Management Overview	23
8.1 Onboarding Activities and Requirements	
8.1.1 Planning	
8.1.2 Risk Assessment	
8.1.3 Criticality	
8.1.3.1 Criteria for Determining Critical Third-Party Engagements	24
8.1.3.2 Non-Critical	
8.1.4 Risk Ratings	
8.1.4.1 Low	
8.1.4.2 Moderate	
8.1.4.3 High	
8.1.5 Residual Risk	
8.1.6 Due Diligence Overview	25
8.1.6.1 Completion of Risk-Based Due Diligence Before Contract Execution	
8.1.6.2 Scope	
8.1.6.3 Outsourced Due Diligence Collection and SME Review	26
8.1.7 Contracting	
8.1.7.1 Contract Terms and Provisions	
8.1.7.2 Analysis of Contract	
8.1.7.3 Contract Execution	
8.1.7.4 Completion of Due Diligence Before Contract Execution or Renewal	27
8.1.7.5 Contract Management	
8.1.7.6 Contract Noncompliance	
8.2 Ongoing Activities and Requirements	
8.2.1 Risk Re-Assessment	
8.2.1.1 Additional Risk Re-Assessment as Necessary	
8.2.2 Periodic Due Diligence	
8.2.3 Ongoing Risk Monitoring	28
8.2.3.1 Monitoring Activities	
8.2.3.2 Enhanced Monitoring	
8.2.3.3 Performance Monitoring and Management	
8.2.3.4 Corrective Action Documentation	
8.2.3.5 Third-Party Noncompliance	
8.2.4 Contract Renewal	29
8.2.4.1 Full Contract Review	
8.2.4.2 Completion of Risk Assessment and Due Diligence	
8.2.4.3 Contract Management	
8.3 Offboarding	
8.3.1 Termination	
8.3.1.1 Pre-Termination Contract Review	
8.3.2 Exit Plan Execution	
8.3.3 TPRM Closure	
9 Systems of Record	30
10 Related Policies	30
11 Revision History	30

Third-Party/Vendor Risk Management Policy Guidelines

Based on the third-party risk management lifecycle

You've been tasked with creating or updating your organization's third-party or vendor risk management policy. It's not unusual to feel confused or overwhelmed by what seems like such a monumental task. It's no secret that successful third party/vendor risk management relies on a solid policy. And that third-party/vendor risk management policies aren't only a best practice, they're also a regulatory requirement for many industries.

However, not everyone knows how to write a third-party/vendor risk management policy, or what type of content to include. If you're wondering how to start writing a third-party/vendor risk management policy, or need to update or review an existing policy, we're here to help.

Venminder has developed a comprehensive third-party risk management policy template that aligns with best practices and follows the third-party risk management lifecycle. This companion guide includes policy writing guidelines that meet most industry standards and best practices. Just remember that there is not a single "one-size-fits-all" approach to third-party risk management. Your organization will need to add to or change policy content, descriptions, processes, and so on, to ensure alignment with your third-party risk management framework. Your organization is solely responsible for its third-party or vendor risk management policy's structure, content, and regulatory compliance, so take great care when creating the policy.

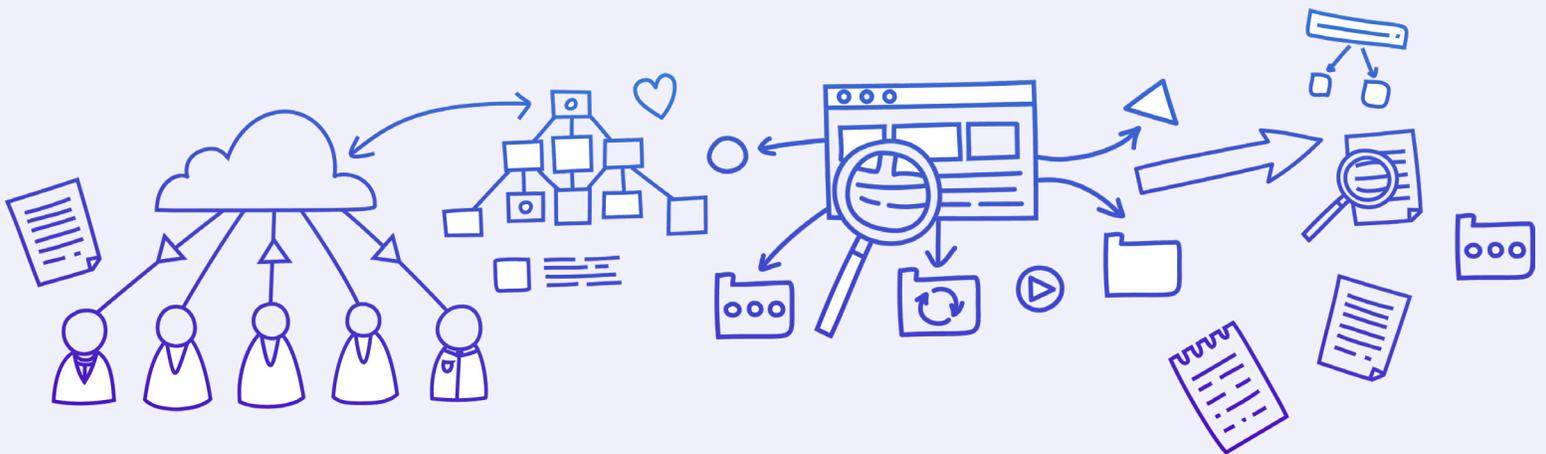
Effective third-party/vendor risk management policies are the foundation of any good third-party or vendor risk management program. Venminder is here to help you and your organization draft an excellent policy because we believe in making third-party/vendor risk management more accessible, less complex, and more effective for everyone.

Getting Started

We recommend taking some time to review the information provided in this guide first. We have purposely designed this document to assist you and your organization with the following:

1. Articulating the purpose of the third-party/vendor risk management policy
2. Identifying the users of the policy as well as process stakeholders
3. Determining the best tone and language to create your policy
4. Learning about the recommended content and information flow of a third-party/vendor risk management policy
5. Deciding on the specific content you'll need to create an effective policy for your organization
6. Aligning your policy with best practices and the third-party risk management lifecycle
7. Determining how you can leverage the third-party/vendor risk management policy template to get the best results

By reading this guide, you'll hopefully learn something new and get some answers to your most important questions. It will also enhance your confidence in the process and help you structure great policy content.



How to Use the Provided Third-Party/Vendor Risk Management Policy Template

We've provided you with a policy template that follows the third-party risk management lifecycle and illustrates the content, structure, and flow of a well-written third-party/vendor risk management policy. Remember, a template is merely a pattern you can follow to achieve a similar result.

Although you can use the template exactly as is, we strongly recommend you customize it to align with your organization's governance structure, needs, terminology, processes, etc.

The third-party risk management lifecycle-based policy template was created to include the most widely accepted best practices for third-party risk management and follow the requirements and activities of the third-party risk management lifecycle.

It's important to note that some of the specific language used in the template is directly taken from or highly influenced by the guidance documents issued by U.S. regulators. This is because regulatory guidance is the most significant influence on many third-party/vendor risk management best practices, even for non-regulated industries.

Additionally, the third-party risk management lifecycle was developed by financial regulators and illustrates the necessary activities required for fulsome third-party risk management throughout every third-party relationship. By incorporating the requirements and activities found in regulatory guidance, even non-regulated organizations using this template can create third-party risk management policies that meet the highest standards. It's important to remember that your organization's policy should be customized to fit its specific needs.

It's recommended to use the provided template as a guide to organize your policy structure, content, and flow.

You can even copy the template language. However, it's crucial to ensure your policy accurately reflects your organization's current practices and not what it "should" or plans to do in the future. When audited or reviewed, you will need to provide evidence that you follow the requirements and guidelines of your current policy. It's better to omit a policy requirement than to have one that isn't followed.

Note: *The terms "third-party risk management" and "vendor risk management" are used interchangeably in this document. Your organization may use a different term, which is perfectly acceptable. In this document, we will use "third party" or "vendor risk," and we'll also use the abbreviations of TRPM or VRM.*

Section 1:

Best Practices for Third-Party or Vendor Risk Management Policy Content and Structure

Know your regulatory requirements

If you're regulated, make sure to review the guidance provided by your respective regulator(s). Comprehensive guidance is available on regulator websites.

Read the guidance, any related information, and do the following:

1. Review the order of the information (how does it flow?)
2. Identify where your third-party/vendor risk management program or practices may have gaps compared to the regulatory guidance

Understand your organization's policy writing requirements, format, and style

If your organization has specific format requirements (e.g., font, layout, numbering conventions, etc.) for formal documents such as policies, be sure to follow them. Copy and paste the content into your organization's policy template rather than trying to reformat the template provided by Venminder. Take a look at some of your organization's existing policies to see how they are structured, written, and presented.

Understand how, or if, policies are enforced in your organization

Every organization has its own way of communicating and implementing its internal policies. Some organizations require their employees to read and sign a document stating that they understand and agree to follow the policy. Others simply create policies and store them somewhere, hoping that the employees will comply with them. However, it's crucial to communicate the policy effectively to all employees and ensure they're aware of it. If employees aren't aware of the policy, it's unfair to expect them to follow it and face consequences for noncompliance.

Auditors and regulators alike frown on policies that aren't enforceable or enforced. After all, what is the point of a policy other than to formally communicate a set of rules and requirements? If these rules and requirements aren't communicated, how or why should they be followed?

Talk to your management and Human Resources teams to discuss the following:

1. How are policies communicated, and to whom?
2. How are policies enforced?
3. What are the consequences of policy noncompliance?
4. How are policy exceptions typically handled and documented?



Keep it general

You can't anticipate every scenario in your policy. Writing policies that are broadly applicable while still being specific enough to apply to various situations is essential. Save your detailed instructions for your program documents and procedures.

Don't include processes or procedures

A policy is meant to convey rules and requirements. A policy isn't meant to instruct the reader on how to execute the specific requirements.

For example, suppose you have a requirement that a senior IT manager approves any vendor engagement providing technology products or services. You may have a specific form or routing process to make that happen. You want to include the requirement in the policy but omit the specific details regarding the process.

Here's a good example of how that requirement **SHOULD** be stated in the policy and how it **SHOULD NOT** be:



All vendor engagements providing technology products and services must be approved by the IT department manager (director or above) before the contract can be executed.



To get approval for vendor engagements for IT products and services, the vendor owner must get the approval of an IT manager (director or above).

1. Vendor managers complete form IT 1020 and submit it through the IT slack channel
2. Within 24 hours, the form is routed to the appropriate IT manager
3. The manager reviews the business case and validates budget availability
4. The manager accesses the vendor engagement record in the TPRM system and checks the approval box
5. Vendor owner and contract manager are notified of approval via email

It's not that process information isn't important. Yes, stakeholders need to know how to get approval for their engagements. **However, those specific details aren't appropriate for a policy for a few reasons:**

- Policies only convey the rules and requirements necessary to meet best practices, regulatory requirements, and stakeholder expectations
- Policies should be as brief as possible and practical
- Policies should convey only the information that is relevant to all stakeholders
- If your process changes (and they frequently do), you'll need to update your whole policy

Keep your process details but move them to a program or operating procedures document.

Less is often more

You don't always need a lengthy policy. In many instances, shorter is better. Still, you need to address all necessary elements and requirements. Don't get caught up on page count or document length. Focus on clearly communicating the requirements.

Watch your language

Be precise with your words, shorten your sentences, and use language that is easy to understand. Consistency is vital, so use the same terms throughout the document. For example, if you refer to your program as Vendor Risk Management, then refer to your policy as a Vendor Risk Management policy. And use the appropriate acronym, such as VRM. Ensure you don't refer to vendors in one part of the policy and as suppliers or third parties elsewhere.

Use a language structure consistent with your organization's culture

For example, a traditional organization like a bank may use more formal policy language. In contrast, a technology startup may use single sentences to describe policy requirements.

Here are some examples of formal vs more informal language:

- 1. Formal language:**
"These elements apply to all activities carried out by third parties. However, the extent and scope required of each third party depend on a variety of factors."
- 2. Less formal language:**
"The extent and scope of any third-party risk management activity depends on various factors."
- 3. Least formal language:**
"Requirements for third-party/vendor risk management activities vary."

The meaning of each of the statements above communicates the same concept. Still, when customizing content to reflect your organization's culture and policy style, be mindful of preserving the originally intended meanings and context.

Use active and direct words

Rather than “shall” when expressing requirements, use “must.” Use the following instead of “shall”:

- “Must” – if it’s a requirement
- “Must not” – if it’s prohibited
- “May” – for discretionary actions
- “Should” – as a recommendation

Define terms

Defining terminology and words with specialized meanings can make the policy more user-friendly. As a best practice, it’s recommended that you, at a minimum, define what the following terms mean for your organization:

- Vendor or Third Party
- Vendor Risk Management or Third-Party Risk Management
- Critical
- High, Moderate, and Low Risk
- Contract

Note: Defining key terms is not the same as adding a glossary, where all terms are defined. Including a full glossary can make the policy longer. Prioritize essential terms relevant to the policy’s scope. If you feel like a glossary would be valuable, consider adding it as part of a program document or operating standards guide.

Make it clear who does what

Identify and document stakeholder roles and responsibilities. When you think about third-party or vendor risk management at your organization, many different stakeholders likely contribute to that process. Those roles and responsibilities must be clearly identified in your policy. Why?

Establishing who is accountable for ensuring specific requirements are met is a key objective of any policy. This document’s “Understanding Policy Content” section, which starts on page 17, will share some example roles and responsibilities.

Follow the third-party/vendor risk management lifecycle

In most cases, the regulator’s content will align with the third-party/vendor risk management lifecycle. The third-party risk management lifecycle was designed by regulators and has been the primary influencer of accepted best practices for third-party/vendor risk management.



Looking at the lifecycle, you’ll see that oversight & accountability, documentation & reporting, and independent review create its foundation. Likewise, your policy should include those elements as core components of your program.

The third-party/vendor risk management lifecycle also identifies the specific risk identification, management practices, and activities that are necessary throughout the third-party relationship. The risk considerations and activities change slightly as the process progresses from Onboarding to Ongoing and Offboarding. Similar lifecycle activities may have different requirements depending on which phase of the lifecycle they’re in.

Example:

The requirements for an initial inherent risk assessment occurring during the onboarding stage may look slightly different than a risk re-assessment conducted in the ongoing stage. You’ll also find references to contracts in all three lifecycle stages, but each are distinctly different.

Following the structure and flow of the lifecycle is a great way to organize your policy content and address each risk activity during each lifecycle stage.

Pro Tip:

Before writing your policy, review your existing third-party risk management practices, activities, and requirements against the third-party/vendor risk management lifecycle. Does your organization currently have auditable processes that align with each stage of the lifecycle (Onboarding, Ongoing, and Offboarding)? If not, it’s good to record any current gaps and begin creating and documenting plans to develop and implement those requirements and practices as soon as possible and practical.

Refer to other policies

It's not unusual for a TPRM/VRM policy to reference other internal policies. As a best practice, you shouldn't quote or include specific language from another policy. Instead, reference the policy, create a hyperlink to its internal location, and include it in the related policies section. By using this approach, you can maintain complete control over the content of your policy without having to modify it when other policies are updated.

For example, you can state: "Additional contractual requirements can be found in the Company Contract Policy," as opposed to including specific language or requirements taken from the policy.

When in doubt, leave it out

The policy template reflects regulatory expectations and best practices, but that doesn't mean your organization follows these practices. Suppose, for example, you don't have an internal requirement to complete due diligence before the contract is signed or your senior management and board don't approve the policy. In that case, it's best to omit the content saying you do.

Your policy should only represent your current state and practices.

There is an expectation that your policy contains your actual practices and requirements. Having an auditor or examiner find gaps in your program is better than receiving an audit finding for noncompliance with an aspirational or unenforceable policy.

Ask for stakeholder review and feedback

Developing a policy is a process that should be done with transparency and collaboration. You should be comfortable allowing key stakeholders to weigh in, provide suggestions, and identify any inaccuracies. Taking these steps upfront ultimately creates a better and more effective policy. Having written your policy and prepared it for approval by senior management and the board, you wouldn't want that process derailed by a stakeholder claiming they didn't have the time or opportunity to provide input.

Gathering feedback is essential, but don't be surprised if not every stakeholder knows how to review the policy or provide that feedback.

Section 2:

Understanding Policy Content

This section will walk you through the content of the policy included in the lifecycle-based template to help you understand the purpose of each policy section and its objectives. We'll use the same section numbers as the template to make it easy to follow.

Taking time to understand the purpose of each section and the content provided in the policy template can assist you in determining the right content for your policy.

Policy Content and Flow

The general flow of the policy template is designed to convey the following information in a specific order:

- Why We Have TPRM/VRM
- What Is TPRM/VRM
- TPRM/VRM Scope
- The Approach to TPRM
- TPRM Governance
- Roles and Responsibilities
- Managing Third-Party Risks Throughout the Lifecycle
- Noncompliance/Escalation
- Systems of Record
- Associated Policies
- Policy Revisions History

The content included in the policy template has been designed to reflect the foundation and activities of the third-party risk management lifecycle and best practices. Your policy may need more or less information or a different content flow, which is fine. Most importantly, your policy should always spell out your organization's requirements and current practices.

We have provided descriptions of each policy section and subsection below to help you understand what is included in the policy template and why. The sections in this guide are numbered to match the sections and subsections found in the template, making it easier for you to locate the information. By understanding the reasoning behind the content and the requirements listed in the policy template, you'll be better able to adapt the template content to fit your organization's needs and requirements.

1 | Overview and Background

This section provides the reader with enough information to understand the background of the policy, why you need it, and the risks of not having it. Most formal policies should have this section; however, you may leave it out if your organization doesn't usually include this information.

2 | Statement of Purpose

This section details the policy's purpose, which usually boils down to managing the risks associated with third-party/vendor relationships and meeting regulatory expectations and best practices.

3 | Policy Statement

When people use the term "elevator speech," they typically refer to a short description of an idea, product, or company that explains the concept so that any listener can understand. Your Policy Statement is essentially your elevator speech for your organization's TPRM/VRM policy and practice. Short, specific, and to the point. Suppose you feel pressure to shorten or condense your policy. In that case, you can usually eliminate the Overview, Background, and Statement of Purpose sections and use the Policy Statement instead.

4 | Terms

The purpose of this section is to provide the reader with specific definitions of key terms used within your policy. This section shouldn't be confused with a glossary. Use this section to define the most important terms in the policy.

4.1 | Third Party/Vendor

Defines what a third party or vendor is to your organization.

4.2 | Third-Party Risk Management and Oversight

Defines both the purpose and the practice of third-party risk management or vendor risk management at your organization.

5 | Scope

Details which types of third-party or vendor relationships are in scope for the policy, program, and practice.

5.1 | Third Parties Not in Scope Under This Policy

Specifically, it details which types of third-party/vendor relationships are NOT in scope for your program. Common examples are:

- Customers
- Employees
- Investors
- Government entities
- Public utilities
- Sponsorships or donations
- Vendors covered under travel and expense policies (hotels, airlines, shuttle bus, etc.)
- Media subscriptions
- Professional membership dues and conference fees
- Payees (Board members, legal settlements, etc.)

Note: If your organization determines that specific relationships are out of scope for your third-party risk management practices, you must be prepared to articulate and defend that decision. For example, relationships with employees, investors, and customers are out of scope for most organizations. Why? Because even though those relationships would technically qualify as third-party relationships, they don't meet the criteria of providing goods or services to support the operation and its customers. Those relationships would be governed by other policies, requirements, and practices. Likewise, advertising in the spring musical program of a local high school would probably qualify as sponsorship rather than advertising. It wouldn't meet the criteria of providing goods and services.

5.2 | Pre-Existing Third-Party Relationships

This statement acknowledges that there may be engagements, contracts, or relationships that aren't totally compliant with the policy. And that when those gaps are identified, they're remediated at the first reasonable opportunity. Suppose you have inherited an old program or can't confirm that all your third-party or vendor relationships comply with the policy. In that case, a statement such as this is recommended. Be aware that when including a statement like this in your policy, your auditors or examiners will expect evidence that you're actively bringing your vendor relationships and contracts into compliance with the policy.

6 | Approach to Third-Party Risk Management

This section describes how the organization adheres to the principles of third-party risk management lifecycle, and the foundation of governance that supports those activities. And that all risk management activities are proportionate to the risks presented.

This section details third-party/vendor risk oversight accountability and briefly describes how that oversight is executed within the organization. Remember to structure this content to reflect how your organization assigns and executes these responsibilities.

7 | Third-Party Risk Governance

This section provides an overview of third-party risk governance at the organization and breaks out the components that are necessary to support effective governance.

7.1 | Oversight

This section will describe oversight of the TPRM program and list specific oversight activities and requirements. It will go on to detail the specific roles and responsibilities accountable for TPRM at the organization.

7.1.1 | Policy Management and Approval

Who is responsible and accountable for approving the policy? This section should detail how often the policy is reviewed (best practices and regulatory requirements expect the board to approve the policy; if there is no board, that responsibility falls to senior management).

7.1.2 | Approval of Critical Third Parties

Who is responsible for approving critical third parties? Best practices dictate this would be senior management or an approved committee. Considering the critical nature of these relationships, they should be considered and approved at the highest levels of the organization.

7.1.3 | Periodic Review of Critical Third Parties

Specifically, who is responsible for reviewing critical third-party status, risks, and performance to ensure everything is in good standing and that risks are within the organization's risk tolerance? Who is accountable for ensuring there are no unaddressed issues or new or emerging risks with critical third parties?

7.1.4 | Staffing and Resources

Who ensures sufficient and qualified resources to manage third-party risk across the organization? For example, if an auditor finds that a lack of resources prevents effective third-party risk management, who is responsible and accountable for correcting the issue?

7.2 | **Accountability: Roles and Responsibilities**

This section goes into more detail about specific vendor risk management roles and responsibilities. Having a lot of narrative detail is unnecessary. Short, bulleted lists can work well. Again, align roles, responsibilities, and titles to match your organization. We've included general roles and responsibility descriptions for each of the roles listed in the template. Remember that you can have more, fewer, or different roles represented in your policy.

7.2.1 | **The Board of Directors**

They're responsible and accountable for ensuring that TPRM/VRM is executed effectively at the organization and that TRPM/VRM is incorporated into business strategy and decisions. They approve the policy and hold senior management accountable for its implementation and execution.

7.2.2 | **Senior Management**

They're responsible for integrating TPRM/VRM into core business strategies and decisions. They're accountable for the design and effective execution of TPRM/VRM across the organization, including the structure and implementation of the TPRM/VRM program, establishing the TPRM/VRM risk appetite, and holding all stakeholders accountable for the proper and timely execution of their roles and responsibilities. They must ensure enough skilled resources to manage and execute the processes necessary for a safe and sound TPRM/VRM program. Another critical responsibility of Senior or Executive Management is setting the "tone-from-the-top" regarding the significance of TPRM/VRM in the organization.

Note: *Some organizations elect to refer to this as "Management," indicating a broader distribution of these responsibilities.*

While not included in the template, you may wish to include Business Unit Management to further refine the expectations for management at different levels of the organization.

Business Unit Management

Managers of departments, business units, and divisions ensure that TPRM/VRM practices are followed and implemented within their departments. And that appropriate planning for third-party/vendor relationships occurs before entering into business relationships. Additionally, they hold Third-Party Vendor Owners responsible for the performance of their third parties/vendors and identifying and managing risks associated with these relationships.

7.2.3 | **Third-Party/Vendor Risk Management**

This individual or team is responsible for creating the framework, requirements, rules, tools, and processes that enable effective third-party or vendor risk management at the organization. They oversee the processes across the third-party/vendor risk management lifecycle and review vendor owner deliverables to ensure quality and completeness.

7.2.4 | Third-Party/Vendor Owners

These individuals own the relationship with the third party/vendor. They are responsible for the effective and timely execution of all required TPRM/VRM lifecycle activities, including planning for the relationship, identifying appropriate third-party/vendor exit strategies, identifying the risks inherent to the product/service, ensuring the third party/vendor is responsive to all TPRM/VRM requests, managing the risk and performance of their third-party/vendor relationships, and the management and remediation of any third-party/vendor issues.

7.2.5 | Independent Reviewers

They're responsible for the objective review and assessment of the TPRM/VRM practices across the organization. They seek to confirm that the organization complies with all laws and regulations. Independent reviewers include internal and external auditors and regulatory examiners. When they identify gaps, material weaknesses, or other issues, they're responsible for reporting them to senior management and the board and tracking them until remediated.

7.2.6 | Legal Team or Counsel

Legal counsel or the legal team may be internal or external and is responsible for ensuring the legal validity and appropriateness of agreements between the organization and its third parties. They are also responsible for advising the organization on legal matters concerning third parties.

7.3 | Documentation

Documentation and reporting are essential for your TPRM/VRM program. In this section, you'll describe minimum documents to be maintained as records of your TPRM/VRM Program. Keep in mind that when listing documents here, you must be able to provide those documents to an auditor or regulatory examiner on request. Don't include any document that you do not or cannot preserve as records.

7.4 | Reporting

This section should briefly describe regular TPRM reporting and how often the program will be reported to the board and senior leadership. You don't need to include an inventory of every report generated or offered by TPRM/VRM. However, you should provide general information about reporting to the board, senior management, and other stakeholders with oversight responsibilities, such as risk committees.

Note: *Reports provided to your senior leadership and the board can serve as valuable evidence of oversight in an audit or exam.*

7.5 | Independent Review

This section describes how the organization audits and oversees the TPRM program. Typically, these audits are carried out by internal audit teams. If your organization doesn't have an audit team or doesn't audit the TPRM program, don't include this section in your policy.

8 | Risk Management Overview

This section provides an overview of how your organization follows the third-party risk management lifecycle and applies specific requirements to each stage of the lifecycle (Onboarding, Ongoing, and Offboarding). Subsections will further break down each of the lifecycle stages and the required activities during each.

8.1 | Onboarding Activities and Requirements

This section provides an overview of activities to take place during the onboarding stage.

8.1.1 | Planning

This section should describe the consideration and planning for vendor relationships requirements in your organization. Regulators, in particular, like to know that your organization is approaching each engagement carefully and with sufficient consideration of its risks. In addition, the organization should be clear about what it expects to gain from the engagement, how it will be managed, and what it will do if it needs to terminate the vendor.



IMPORTANT SECTION

8.1.2 | Risk Assessment

This section is perhaps one of the most important in any policy. Considering the whole point of the TPRM/VRM function and practices is to manage risk, identifying and assessing that risk is paramount. Spend extra time with this section to ensure all definitions and requirements related to criticality, risk levels, and rating methodologies are reviewed, approved, and endorsed by the necessary stakeholders. Once you include these definitions in your policy, they become the standard by which your auditors and examiners will test you. So, for example, ensure you're not defining critical or detailing risk levels in the policy that only apply to specific departments or haven't been approved. Your systems of record, tools, and processes should share a standard definition of criteria for critical vendors and have standardized risk-level definitions that match the policy.

8.1.3 | Criticality

This section documents how your organization identifies critical vendors. Critical is not a risk rating but a specific category representing a subset of your vendor inventory. Critical vendors are those that, should they fail or suffer a prolonged outage, there would be a material adverse impact on your operations or on your customers.

Every engagement should have a risk rating and be classified as critical or non-critical.

Note: *It's a standard regulatory requirement and best practice for organizations to identify critical vendors and manage them appropriately.*

8.1.3.1 | Criteria for Determining Critical Third-Party Engagements

Document the exact criteria you use to determine criticality in this section. It's essential to note that this applies only to the engagements that are critical for the entire organization. To clarify this, you could use terms such as “across the organization” or “enterprise-wide.” While the three criteria outlined in the template are the most common, some organizations might also want to consider some additional factors, such as:

- If replacing the vendor, or bringing the activity in-house, would require significant time, money, or other resources
- If the vendor failed to provide its products or services and your organization would be subject to regulatory scrutiny, fines, or enforcement actions
- If the vendor's failure would cause significant harm to the organization's brand or reputation
- If the vendor interacts directly with your customers

8.1.3.2 | Non-Critical

Likewise, it's recommended that you add content describing non-critical vendors. All engagements should be classified as either critical or non-critical.

8.1.4 | Risk Ratings

Use this section to detail the criteria for each risk level or rating. The criteria and ratings should be consistent throughout your TPRM/VRM framework, systems, etc. As a best practice, here are the risk level ratings we often see:

8.1.4.1 | Low

8.1.4.2 | Moderate

8.1.4.3 | High

8.1.5 | Residual Risk

This section isn't mandatory, but should be included in the policy if your organization calculates and considers residual risk. A brief description of residual risk and its application in your organization is sufficient. You don't need to include your methodology (i.e., criteria, formulas, or calculations) for determining residual risk within your policy. However, you must document that methodology and retain it elsewhere (as part of your program or procedures) as evidence for any audit or regulatory exam.

8.1.6 | Due Diligence Overview

Due diligence is an essential element of TPRM/VRM practices and processes. Your organization's policy should confirm its dedication to this practice. The policy should also specify that the level of due diligence required is proportional to the level of risk involved in the engagement.

8.1.6.1 | Completion of Risk-Based Due Diligence Before Contract Execution

Every organization should make completion of due diligence before contract execution a firm requirement. Executing a contract before due diligence is completed is risky because your organization loses valuable leverage to negotiate and legally obligate the vendor to remediate issues identified during due diligence. Worse still is discovering a "dealbreaker" after you've entered into the business relationship.

Here's an example of a worst-case scenario:

Suppose you rush to sign a contract, so you don't lose a time-sensitive discount. However, due diligence wraps up, and you discover that your new vendor has many customer complaints and lawsuits. Or, even worse, is on a sanctions list!

Due to its importance, you may emphasize this requirement within your policy by adding expanded language stating the requirements and prohibitions related to due diligence.

For example, you might say: "All vendor engagements require formal due diligence as determined by TPRM/VRM. An organization's employees or agents must not execute any contract or begin any work with a third party or vendor until due diligence has been completed. This requirement cannot be waived unless approved by TPRM and the Vendor Risk Management Committee."

IMPORTANT SECTION

8.1.6.2 | Scope

Please pay attention to this policy section as it defines when you will or won't conduct due diligence. At a minimum, this section should restate that due diligence activities are proportionate to the risk in the engagement.

Whatever you state here will be a review point in audits or exams. Listing your requirements here is recommended for all vendors identified as critical or rated as high risk. It may also be a good idea to add language stating the TPRM/VRM team has the discretion to request due diligence for any engagement, regardless of risk level, if a compelling reason exists.

It's essential to acknowledge that external factors play an important role in the due diligence process. For example, effective due diligence requires the participation of the third party or vendor providing information about and evidence of their risk management practices and controls.

8.1.6.3 | Outsourced Due Diligence Collection and SME Review

Adding this section isn't absolutely necessary, but it may be helpful if you're currently using external subject matter experts or hiring a firm to collect vendor documentation (or may need to in the future). The point you're making is that you do/will engage external resources to perform these processes when there is a compelling reason to do so. This disclosure statement provides transparency to your stakeholders, auditors, and examiners.

8.1.7 | Contracting

This section is frequently overlooked in TPRM/VRM policies as many organizations have their own separate contract policy covering contract review, signing authority, and other related aspects. However, these internal policies usually don't explicitly address regulatory requirements and best practices for third-party/vendor contracts. Therefore, TPRM/VRM policies should incorporate specific contractual standards to ensure all stakeholders can comprehend the contract requirements within the TPRM/VRM context.

8.1.7.1 | Contract Terms and Provisions

This section addresses specific contract terms and provisions reflecting regulatory requirements and best practices for TRPM/VRM. Before developing this policy section, work with your legal team to review your organization's existing contract templates. Taking time to review existing legal templates can help you avoid the inclusion of requirements that may not be fulfilled or that contradict stated terms and conditions used in your organization's contracts.

8.1.7.2 | Analysis of Contract

The contract terms listed below represent regulatory requirements for TPRM/VRM contracts. Your contracts, at minimum, should address the items listed in this Contracting section. Don't forget to include Audit or Right to Audit, as that single provision can legally obligate your vendor to provide data or information to you as you request. This contractual provision can be beneficial when working with vendors resistant to sharing due diligence information as requested.

Note: *As an essential consideration, you'll want to think about who is responsible for the analysis of the contract within your organization. While you don't have to specify precisely who in the policy, you should be able to identify the general requirement (i.e. review by a qualified legal professional) and what controls you have in place to ensure that contract analysis is occurring.*

8.1.7.3 | Contract Execution

This section should detail any specific requirements that must be met as part of contract execution.

8.1.7.4 | Completion of Due Diligence Before Contract Execution or Renewal

This section isn't necessary if the specific requirement has been listed elsewhere in the contracting section. However, reiterating it as a separate and distinct requirement is a preference for some organizations.

8.1.7.5 | Contract Management

Managing vendors to meet contract terms and maintaining administrative oversight to ensure timely renegotiation, renewal, or termination dates to maintain an organization's advantage is the essence of contract management. Provide a summary statement here that defines what contract management entails in your organization.

8.1.7.6 | Contract Noncompliance

This section describes the organization's right to terminate contracts when necessary. Because this isn't a specific requirement you may omit this section if desired.

8.2 | Onboarding Activities and Requirements

This section introduces the activities and requirements for the ongoing stage of the lifecycle. It provides a brief overview of the purpose for those activities. Each required activity should be detailed in its own subsection.

8.2.1 | Risk Re-Assessment

Third-party risks change and evolve all the time, so periodically re-assessing risk is necessary. This section should detail the purpose of risk re-assessment. List your requirements for formal periodic risk assessments that include a review of inherent risk and the validation of necessary controls through due diligence. This is a formal process and should be on an established schedule. Make sure to include the required intervals, by risk rating, for those reviews.

8.2.1.1 | Additional Risk Re-Assessment as Necessary

You may need to conduct risk reviews or due diligence more frequently than your schedule dictates, especially if there are specific triggers such as a change in ownership, data breach, etc. List the specific circumstances that might trigger an additional assessment or provide a generic statement giving TPRM/VRM the discretion to require periodic risk reviews when necessary.

8.2.2 | Periodic Due Diligence

Risk re-assessment and due diligence go hand in hand. As risks are re-assessed, the risk management practices and controls must also be considered and validated. As such, there must be a requirement to update and review due diligence documentation. Make sure you include the periodic due diligence intervals as part of the requirement.

8.2.3 | Ongoing Risk Monitoring

This section refers to vendor monitoring as a whole and describes the purpose of this required activity.

8.2.3.1 | Monitoring Activities

Not all of these activities will apply to every organization. List only the monitoring activities and practices currently performed at your organization.

8.2.3.2 | Enhanced Monitoring

This statement reiterates the additional monitoring activities and rigor is required based on risk rating, criticality or under other circumstances that warrant it. Provide details to ensure the requirement is understood.

8.2.3.3 | Performance Monitoring and Management

While the content in the policy isn't overly comprehensive, monitoring your third party's performance is an essential part of TPRM. Many organizations are still developing these processes. Include your organization's requirements for performance management in this section. At a minimum, it's important to require that performance issues are documented and monitored.

8.2.3.4 | Corrective Action Documentation

This section identifies the requirements to document and manage issues and escalating them when necessary and appropriate.

8.2.3.5 | Third-Party Noncompliance

This section describes the required action when efforts to identified problems and issues aren't managed or the corrective actions aren't effective.

8.2.4 | Contract Renewal

This section addresses the requirements for contract renewals vs their initial execution.

8.2.4.1 | Full Contract Review

This section outlines the necessity of reviewing all legal agreements before renewing contracts. The review is conducted to identify any potential changes to the contract that require negotiation and to ensure the contract complies with current contracting standards. This includes making sure all required terms and conditions are included. During the review, it's important to consider the risk profile and performance of the third party.

8.2.4.2 | Completion of Risk Assessment and Due Diligence

This section reiterates the requirement to ensure there's a completed risk assessment and due diligence before renewing any contract.

8.2.4.3 | Contract Management

This section reiterates the requirements to actively manage renewed contracts.

8.3 | Offboarding

As the final stage of the TPRM lifecycle, there are specific considerations when ending a third-party engagement to ensure a safe and sound termination. The decision to terminate may rest on various factors and considerations.

8.3.1 | Termination

This section acknowledges the risks of offboarding and lists the factors to be considered before the decision to terminate is made. This section requires the identification of specific controls to ensure negative impacts resulting from the termination are minimized. Describe the requirements your organization has for formally terminating a third-party engagement and any activities that must take place during that process. Keep in mind that the activities listed here are best practices, but if they aren't reflective of your actual practices, don't include them.

8.3.1.1 | Pre-Termination Contract Review

This section details the requirement to review contracts and agreements with legal counsel to ensure a legally compliant termination process.

8.3.2 | Exit Plan Execution

This section details a requirement for a documented exit plan for third parties that are high risk or critical. It lists the mandatory elements of such a plan. These plans help ensure all necessary risk mitigation controls are present and effective during the termination and it occurs safely and soundly and within the expected time frame.

8.3.3 | TPRM Closure

This section describes the requirements for managing administrative details related to the third-party termination and relationship. This should emphasize proper record keeping and organization.

9 | Systems of Record

This section informs the organization of the requirement to perform TPRM/VRM activities, derive data from, and retain documentation within specific systems of record. You may choose to list those systems or not.

Note: If your organization mainly relies on manual TPRM/VRM processes, such as spreadsheets, it's best to leave this section out.

10 | Related Policies

Many policies will refer to or are bound by other internal policies. Create an inventory with the official policy name, a brief description of the policy, and a hyperlink or other location information.

11 | Revision History

Your policy is a living document; you must practice version approval and control. Your revision history should document information regarding the versions, active dates, and approvals of your policies.

Note: Your organization may have a specific format or location for this information as part of an internal document standard. You may include this section where required for your organization.

Other Information

Perhaps you have other information or requirements that don't fit neatly into the sections detailed above. In that case, it's perfectly fine to add additional sections to the policy. Just remember that the policy is for listing requirements; don't include information on how to perform processes or procedures in your policy.

Developing or updating your third-party/vendor risk management policy represents a huge step forward in the development or maturation of your program.

Stay focused and be confident. You can do it!

