TEVORA™

Third Party Risk Management Maturity Assessment

2022 Tevora White Paper

Jeremiah Sahlberg
Riley Webber

June 2, 2022

Table of Contents

Introduction

The modern organization's success lies in collaboration. By cultivating a complex array of third-party relationships, businesses have been able to expand market reach, achieve dynamic operational models in the wake of pandemic restrictions, and bolster underdeveloped business functions through outsourced expertise. Although these benefits can significantly improve an organization's bottom line, flaws within a third party's security practices can also directly impact the organization. To reap the benefits that third parties offer while minimizing the attached security risks is a trait mature Third-Party Risk Management (TPRM) programs enjoy.

With the frequency and severity of ransomware and other cyberattacks on the rise, it is not enough to simply shore up your organization's defenses. You need to ensure that the security of your third parties is equally strong because your defenses are only as good as your weakest link.

You may have a TPRM program in place today, but how do you know if it is mature enough to effectively manage and report on your third-party risks? Is your organization confident in not only its security controls but those of its third parties? How far does your third-party ecosystem reach – and how much does it expose your organization?

In this white paper, we'll describe how Tevora's TPRM maturity assessment service can help you measure the maturity of your TPRM program and identify areas where your program can be improved to better secure your third-party ecosystem.

Tevora's TPRM Maturity Assessment Process

The object of the TPRM maturity is to summarize the current state of an organization's TPRM program for assessing and managing third-party risks. Once the areas of improvement are identified, Tevora then provides actionable improvements to elevate the program and alleviate any inefficiencies or oversight.

Process Overview

To ensure alignment and project success, Tevora begins efforts with a kickoff meeting to introduce our team and meet key project stakeholders. During this session, the assessment approach is discussed, the project scope is determined, and personnel is identified for interviews to lend their insight on current organizational TPRM procedures, documentation, and technologies.

Following the kickoff meeting, our team begins interviews with those key staff members. In conjunction with a detailed review of existing TPRM documentation, Tevora assessors observe the execution of TPRM processes and procedures to identify inefficiencies, pain points, and areas that may introduce risk to the organization.

After completing our review of the environment, we will prepare and present our assessment findings, including detailed recommendations for improvements needed to transform your TPRM program into a mature, effective, and efficient program.

Divide and Conquer

Tevora breaks down the TPRM program into six key operational phases and then uses an adaptation of the Capability Maturity Model (CMM), initially developed by Carnegie Mellon and the Department of Defense, to assess the maturity level of each phase.

Six Phases of the TPRM Program

The six TPRM phases are defined as follows:

- **Vendor Identification**—The stage of identifying vendors with certain criteria, status, and the services provided by the vendor.
- **Vendor Tiering**—The stage of classifying vendors into a certain category based on the criticality of data being handled or access provided to certain networks and environments.
- **Vendor Contracting**—The stage of engaging with third parties, forming a contractual agreement on services being provided, and aligning expectations for quality, liability, and security.
- **Vendor Assessment and Reassessment—**The stage of assessing vendors based on their responses to the Vendor Risk Questionnaire, conducting continuous monitoring, and reassessing third parties at as appropriate for any change in data handling or services being provided.
- **Program Documentation**—The maintenance of all program-related documentation, ensuring processes are formalized, management-approved, and reviewed at least annually. This also includes an efficient inventory of all third-party documentation to serve as evidence for required security controls.
- **Program Metrics**—The ability to provide key measurements and trends on the operational effectiveness of the program to keep leadership and stakeholders informed of the organization’s extended enterprise.

TPRM Maturity Levels

The CMM defines five levels of organizational maturity, which consider both optimizations of processes and formally supported documentation. Ideally, organizations should strive to achieve and maintain the highest level of maturity: “Maturity Level 5 – Optimizing.” Organizations of this level are characterized by a focus on continuously evolving, adapting, and growing to meet the ever-changing needs of their environment and stakeholders.

The following table describes the different maturity levels and the description of each as it applies to the TPRM program:

Maturity Level	Expectation of Policy Maturity Level	Expectation of TPRM Process Maturity Level

Level 1: **Initial**	Processes are viewed as unpredictable and reactive. At this stage, “work gets completed, but it’s often delayed and over budget.” This is the worst stage a business can find itself in—an unpredictable environment that increases risk and inefficiency.	A standard process does not exist.
Level 2: **Managed**	There’s a level of project management achieved. Projects are “planned, performed, measured, and controlled” at this level, but there are still a lot of issues to address.	An ad hoc process exists and is done informally.
Level 3: **Defined**	At this stage, organizations are more proactive than reactive. There’s a set of “organization-wide standards” to “provide guidance across projects, programs, and portfolios.” Businesses understand their shortcomings, how to address them, and what the goal is for improvement.	A formal process exists and is documented. Evidence can be provided for most activities. Less than 10% exceptions.
Level 4: **Quantitatively Managed**	This stage is more measured and controlled. The organization is working off quantitative data to determine predictable processes that align with stakeholder needs. The business is ahead of risks, with more data-driven insight into process deficiencies.	A formal process exists and is documented. Evidence can be provided for all activities, and detailed metrics of the process are captured and reported. A minimal target for metrics has been established. Less than 5% of process exceptions occur with minimal reoccurring exceptions.
Level 5: **Optimizing**	Here, an organization’s processes are stable and flexible. At this final stage, an organization will be in a constant state of improving and responding to changes or other opportunities. The organization is stable, which allows for more “agility and innovation” in a predictable environment.	A formal process exists and is documented. Evidence can be provided for all activities, and detailed metrics of the process are captured and reported. A minimal target for metrics has been established and continually improved. Less than 1% of process exceptions occur.

TPRM Maturity Assessment Findings

With the environment reviewed and maturity levels assessed, Tevora provides actionable recommendations to each identified risk that, when implemented, will help elevate your TPRM program. Our assessors construct a detailed report to outline the project methodology, scope, and findings. Additionally, our team will present to the key stakeholders on project’s success and noteworthy findings.

Executive Summary

The first section of the report will include a high-level overview that outlines:

- What Tevora was engaged to do (i.e., perform a TPRM assessment).
- How the assessment was conducted.
- Summary of client's current TPRM process.
- Summary of assessment findings and recommendations.

Objective and Process Summary

This section of the report will describe all background aspects of the project including the objective, methodology, scope definition, a summary statement of the client's business, and an overview of the client's IT infrastructure, composed of the specific software and applications used to manage contracts and third-party assessments.

Maturity Assessment Summary

Before diving into the specific deficiencies, this section will include a general assessment of the organization's TPRM maturity level for each of the six key phases. Here's an example of what this might look like:

TPRM Maturity Summary

Phase	Maturity Level				
Vendor Identification	☒ **Initial**	☐ **Managed**	☐ **Defined**	☐**Quantitatively Managed**	☐ **Optimized**
Vendor Tiering	☐ **Initial**	☐ **Managed**	☐ **Defined**	☒**Quantitatively Managed**	☐ **Optimized**
Vendor Contracting	☐ **Initial**	☒ **Managed**	☐ **Defined**	☐**Quantitatively Managed**	☐ **Optimized**
Vendor Assessment and Reassessment	☐ **Initial**	☒ **Managed**	☐ **Defined**	☐**Quantitatively Managed**	☐ **Optimized**
Program Documentation	☐ **Initial**	☐ **Managed**	☒ **Defined**	☐**Quantitatively Managed**	☐ **Optimized**
Program Metrics	☒ **Initial**	☐ **Managed**	☐ **Defined**	☐**Quantitatively Managed**	☐ **Optimized**

Detailed Findings and Recommendations

This section will include the detailed assessment findings, categorized by each TPRM phase the deficiency resides within. For each finding, Tevora provides practical recommendations tailored to the organization's business to promote ease of implementation.

Below is an example of detailed findings for a fictitious company named ABC Global. This example includes findings specific to the Program Documentation phase; however, Tevora will provide details for all findings identified within the six phases of the TPRM process.

Maturity Assessment Findings: Program Documentation Phase

Finding ID	Finding Description	Recommended Remediation
2022.VM.P4.01	ABC Global's Vendor Management Program does not have a formalized list of alternative evidence for assessing larger organizations that will not complete the questionnaire. Additionally, Tevora identified that the Vendor Manager may assist with completing questionnaires for a larger organization when the questionnaires are initially filled out by the vendors themselves.	Tevora recommends that ABC Global formalize a document or add a section into the current vendor documentation to address larger organizations such as Microsoft, who are unable to complete the Vendor Risk Questionnaire. In this document or section, a list of alternative evidence should be created for the ABC Global assessor to assist with acquiring the necessary documentation and information needed to complete the Vendor Risk Questionnaire. For Example: • Download publicly-available documentation and resources from the organization's web pages (data security and compliance certifications, encryption methodologies, third-party assessments and audits, data center security, etc.) • Refer to the organization's FAQ or Q&A page for specific questions. • If faced with outstanding questions, contact the organization's representative or customer support service. • Other applicable methods of evidence collection. Furthermore, any notes or entries made on the questionnaire by ABC Global should clearly indicate what information was completed by ABC Global versus the vendor for audit purposes.
2022.VM.P4.02	After reviewing the Vendor Risk Questionnaire, Tevora identified the following questions that should be reviewed and possibly updated: **Question 25** and **26**: does not ask for the encryption methodology used to	Update the Vendor Risk Questionnaire and consider making the following changes to ensure concise information gathering for vendor assessment: **Question 25**: *"Is sensitive data encrypted in transit? If yes, please describe the encryption methodology used to encrypt ABC Global data in transit (i.e., TLS version)."*

	encrypt ABC Global's data in transit or at rest. **Question 37**: the incident notification time for the vendor to alert ABC Global of any security or data breach is set to one week.	**Question 26**: *"Is sensitive data encrypted at rest? If yes, please describe the encryption methodology used to encrypt ABC Global data at rest (i.e., AES bit size)."* **Question 37**: *"Do you have a process in place to notify ABC Global within 48 hours of discovering a breach?"* The BAA template should also be updated to reflect Question 37 in the Questionnaire.
2022.VM.P4.03	Tevora identified that there were informal and limited processes and documentation regarding the vendor assessment process in current vendor management processes. Datacenter evaluations were also not formalized.	Tevora recommends that ABC Global formalize processes regarding data center evaluations and create appropriate policies and standards as necessary to document those processes. Furthermore, the checklist in ServiceNow regarding Vendor assessments should be documented as a formal procedural process. Additional personnel assisting the Vendor Manager will be able to reference the documentation and go through the process of assessing a vendor from beginning to end and monitoring them thereafter. ABC Global should also create a formal process flow diagram outlining the vendor assessment process. An example is included in Appendix A—Figure 2: Vendor Assessment Process Flow Chart.
2022.VM.P4.04	The Vendor Security Policy document was last reviewed and approved in April of 2019.	Tevora recommends that appropriate ABC Global personnel and management teams conduct at least an annual review of their policies and standards to ensure all documentation is kept up to date with the latest procedures within ABC Global. If there are significant changes to defined policies and processes, the supporting documentation should be updated accordingly.

Common Findings

While no two organizations are the same, some findings turn up in many of our clients' assessments, preventing them from reaching a high level of TPRM maturity. In this section, we'll describe some of the most common findings and present potential solutions.

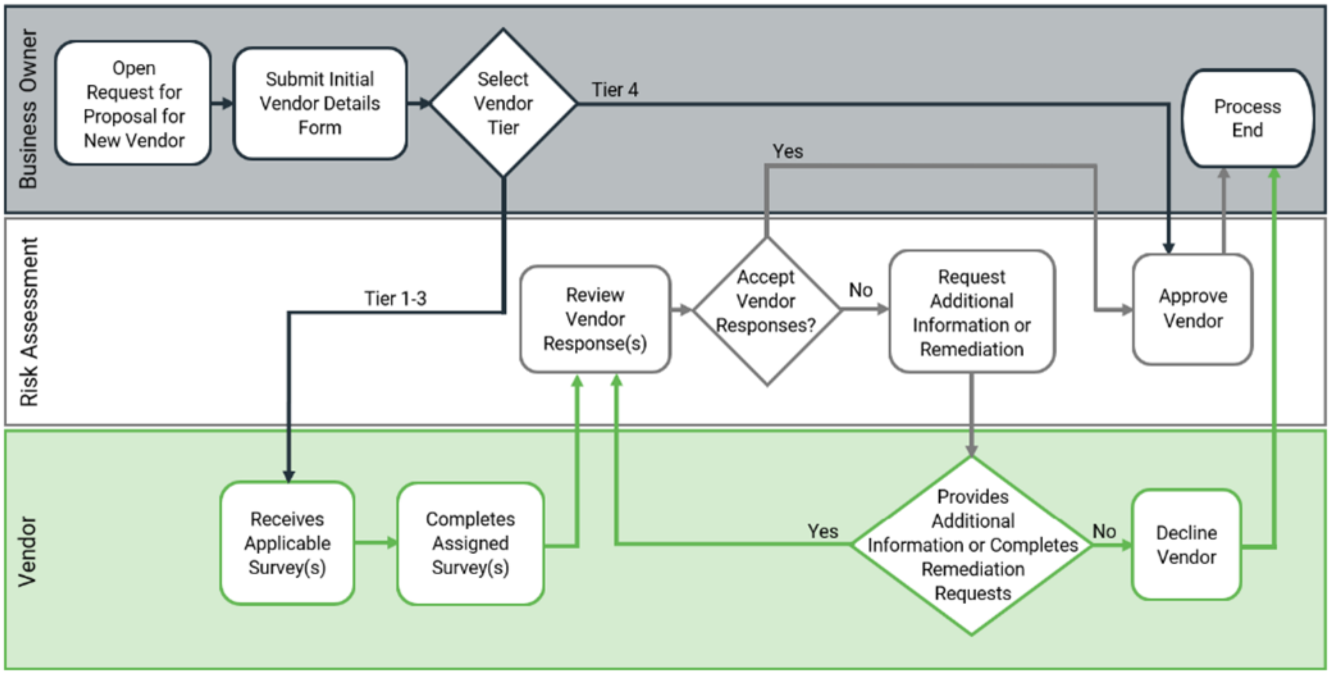
Inadequate or Incomplete Process Documentation

Whether due to the ad-hoc nature of how organizations manage third parties or resource allocation constraints present within an organization's TPRM capabilities, many clients maintain poor documentation of the processes they use to interact with third parties. Without strong process documentation, procedure steps are often missed, potentially allowing risks to amass and persist undetected.

As with all operational processes, Tevora recommends organizations formally define third-party process documentation to establish a consistent workflow, delineate responsibilities, identify decision points, and determine approximate timelines. Building an operational foundation for TPRM processes provides a visual baseline to promote continuity in process execution and expedite onboarding for individuals who will be responsible for TPRM. Additionally, the creation of process documentation serves as an excellent opportunity to streamline identified inefficiencies and mitigate risks that arise from either compliance regulations or missing security controls.

Here's an example of what documentation of a third-party process may look like:

Vendor Assessment Process Documentation Example



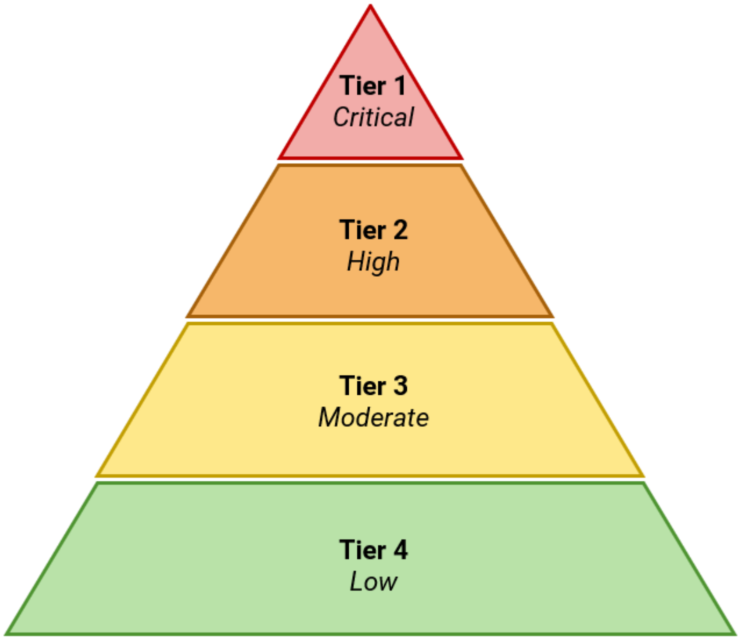
Business Owner
Open Request for Proposal for New Vendor
Submit Initial Vendor Details Form
Select Vendor Tier
Tier 4
Process End
Yes
Risk Assessment
Tier 1-3
Review Vendor Response(s)
Accept Vendor Responses?
No
Request Additional Information or Remediation
Approve Vendor
Vendor
Receives Applicable Survey(s)
Completes Assigned Survey(s)
Yes
Provides Additional Information or Completes Remediation Requests
No
Decline Vendor

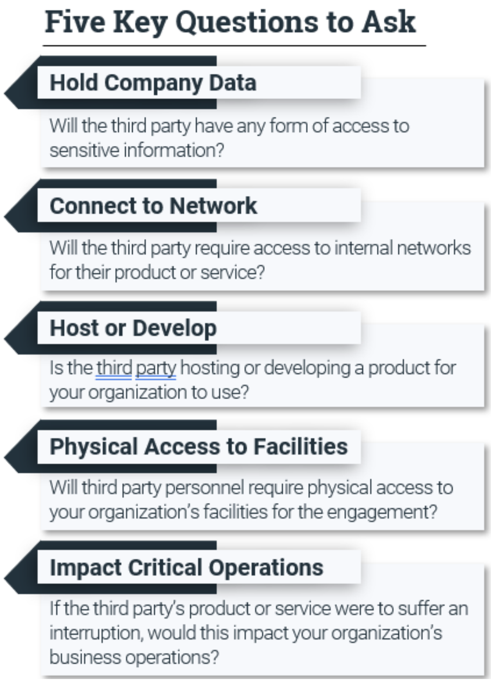
Failure to Categorize Third-Parties by Risk Tier

Clients often struggle with an extensive and sometimes daunting backlog of third parties to assess. One main contributing factor to this backlog is organizations failing to effectively categorize third parties according to risk tier.

Tevora recommends defining multiple tiers based on the level of risk a third party's product or service presents. This allows organizations to prioritize resources on the highest-risk third parties and ensure the proper security controls are in place. Here's an example of what your tier structure may resemble, along with five suggested questions to consider when categorizing a third party:

Third Party Tiering





Five Key Questions to Ask

Hold Company Data

Will the third party have any form of access to sensitive information?

Connect to Network

Will the third party require access to internal networks for their product or service?

Host or Develop

Is the third party hosting or developing a product for your organization to use?

Physical Access to Facilities

Will third party personnel require physical access to your organization's facilities for the engagement?

Impact Critical Operations

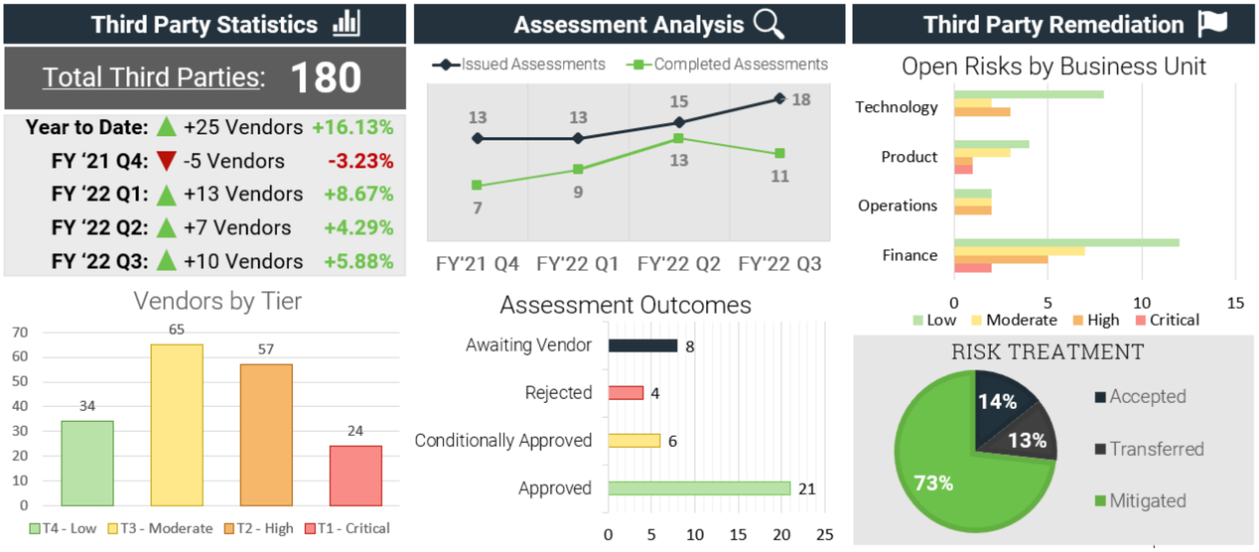
If the third party's product or service were to suffer an interruption, would this impact your organization's business operations?

Although the examples provided display a four-tiered structure, your organization should not be bound to this model. Organizations should employ a number of tiers that is both helpful to the organization and does not introduce excessive complexity or administrative overhead.

Poor Metrics

Many TPRM programs used by organizations today either do not support sufficient metrics to facilitate communication with supporting parties or lack any form of data gathering altogether. Key metrics allow for optimized resource allocation and planning while also giving leadership the insight necessary to make informed decisions regarding company relationships. Without a robust collection of metrics, it can be difficult to know if the TPRM program an organization fosters is succeeding or not. Here are some examples of the kind of metrics we'd expect to see in a mature TPRM program.

Third Party Review Metrics Example

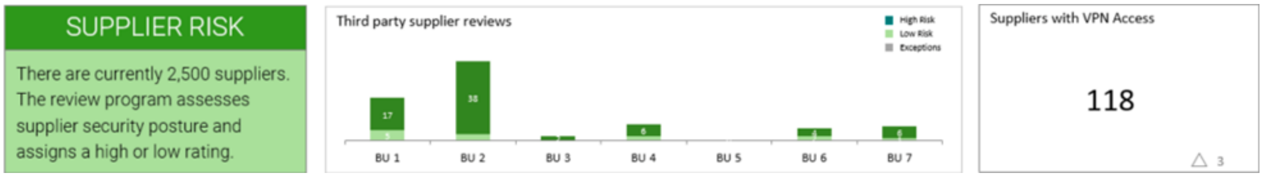


Third Party Statistics

Total Third Parties: 180

Year to Date:	▲ +25 Vendors	+16.13%
FY '21 Q4:	▼ -5 Vendors	-3.23%
FY '22 Q1:	▲ +13 Vendors	+8.67%
FY '22 Q2:	▲ +7 Vendors	+4.29%
FY '22 Q3:	▲ +10 Vendors	+5.88%

Supplier Risk Metrics Example



SUPPLIER RISK

There are currently 2,500 suppliers. The review program assesses supplier security posture and assigns a high or low rating.

We Can Help

If you have questions about Tevora's Third-Party Risk Management Maturity Assessment process or would like Tevora to conduct an assessment of your program, just give us a call at (833) 292-1609 or email us at sales@tevora.com.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora’s leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that can fully implement whatever it recommends, Tevora works with all of the industry’s top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients’ needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as “obsessive.” We consider this a fair assessment.

Our hard work and dedication have established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information, please visit www.tevora.com.

Our team is ready to discuss your specific challenges and identify the best solutions.

TEVORA™

Go forward. We’ve got your back.

Email us: sales@tevora.com

Call us: 833.292.1609