



BUYER'S GUIDE

Buyer's Guide to a Third Party Risk Management Solution



CENTRL is a leading risk and compliance technology company that provides a software platform for managing privacy, compliance, and third party risk. CENTRL offers solutions for automating modern slavery act compliance, vendor risk, privacy management, and operational due diligence. CENTRL's platform is used by leading companies in all sectors across the globe.

US/Global +1-415-780-9667 | UK/Europe +44 (0) 20 3389 8429 | Australia: +61 1800 531 802

And, for more information, please visit: oncentrl.com/vendor360



 [@oncentrl](https://twitter.com/oncentrl) |  [/company/centrl/](https://company/centrl/)

Rev. 2021.7

TABLE OF CONTENTS

I. Introduction

II. Third-Party Risk Lifecycle

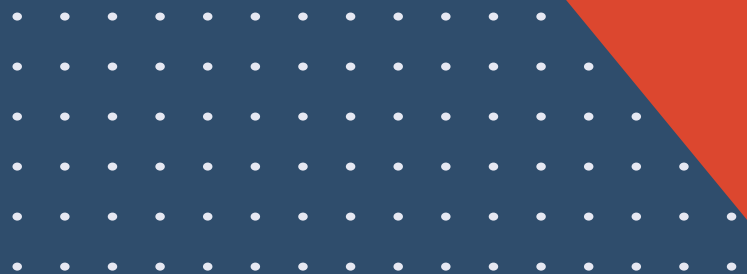
III. What to Look For in a TPRM Platform

- A Vendor Directory
 - New Vendor Selection & Onboarding Management Capabilities
 - Automation for Ongoing Risk Assessments, Audits and Monitoring
 - Third Party Access & Responses
 - Streamlined Evaluation of Third-Party Responses
 - Issues and Track to Remediation
 - Analytics to Gain Insights and Monitor Risk Trends
-

IV. Pricing

V. Your Perfect Solution

- From the Experts
- Vendor360 for Third Party Risk Management



INTRODUCTION

Vendor risk is increasing

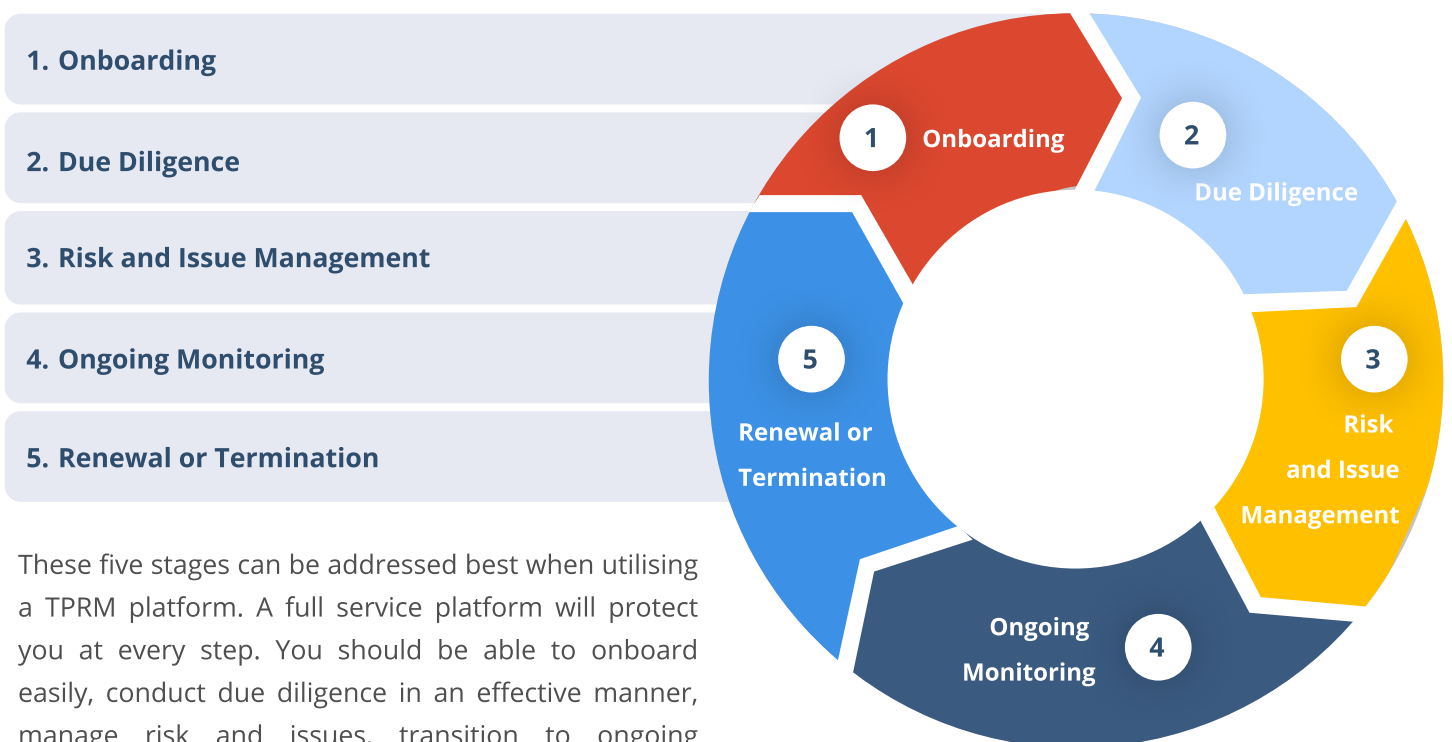
Recent shifts towards global sourcing have created countless business advantages for procurement and supply chain management teams. But the global marketplace has created additional challenges for third-party risk management programs due to the wider range of international regulations and geo-political considerations. In fact, a full 81% of organizations increased the number of third-parties in their supply chain over the past two years, with an average 181 vendors granted access to the institution's internal network [1].

This digitization of vendor access coupled with globalization have intensified the risk management challenges for enterprise security and compliance teams. It has become increasingly more difficult to identify the specific points of vulnerability within complex networks of suppliers, service providers, agents, consultants, and independent contractors. Lack of oversight can cause serious security issues leading to costly fines, litigations and risk to a company's reputation.

Are your third parties vulnerable to attacks. If you're looking to make a decision on selecting a platform you've come to the right place. The perfect Third Party Risk Management (TPRM) platform is different for every organization. This buyer's guide will provide you with the context to make an informed decision about platform options.

THIRD PARTY RISK LIFECYCLE

The third-party risk lifecycle consists of five stages.



These five stages can be addressed best when utilising a TPRM platform. A full service platform will protect you at every step. You should be able to onboard easily, conduct due diligence in an effective manner, manage risk and issues, transition to ongoing monitoring, and renew or terminate as needed.

WHAT TO LOOK FOR IN A TPRM PLATFORM

No matter your unique situation, there are some fundamental features a TPRM platform needs to include. The following section will address necessary features, the needs they meet, and what to look for.

A Vendor Directory

A typical vendor management team, lacking a dedicated solution, often finds itself in a mishmash of spreadsheets -- with disorganized and disconnected pieces of information about their vendors. This results in inefficiencies and frustrations, not to mention occasional loss of critical information and lack of standardized process for oversight. The first area a dedicated solution should provide to overcome this is a centralized vendor directory.

A centralized, comprehensive vendor directory should be able to:

- **Manage all vendor information**-- from documents, to policies, to risk profiles--in a single, centralized, cloud-based platform.
- **Leverage attributes like criticality and inherent risk levels** to segment vendors into multiple risk tiers.
- **Manage risk, spend, contract information, and other attributes** for each vendor at the product, service and engagement levels.
- **Display a comprehensive view** of all vendor data in one place

New Vendor Selection & Onboarding Management Capabilities

Onboarding is the first stage in the TPRM lifecycle and can set you up for success in the long term when carried out efficiently. Onboarding capabilities should:

- **Streamline pre-contract inherent risk analysis for new vendors** - either initiated by business requests or by sending surveys to internal teams.
- **Assess and understand inherent risk for each vendor** at the engagement, product, and service levels. Risk should be assessed at an aggregate level and also for specific risk domains
- **Segment vendors into multiple tiers** based on attributes such as criticality and inherent risk.
- **Use inherent risk analysis to conduct detailed pre contract due diligence and assess appropriate vendor controls.** This due diligence process should assess areas where inherent risk is high.



TIP: A strategic vendor on-boarding and due diligence process can identify third-party risk during the initial vetting process. TPRM tools and technologies have emerged as a popular deployment model to streamline this process through a centralized platform to communicate, store large volumes of documentation, and deliver vendor risk assessment questionnaires designed to identify third-party risk.

Automation for Ongoing Risk Assessments, Audits and Monitoring

The screenshot displays a software interface for a risk assessment tool. The main window is titled "SIG Lite - 2019" and has tabs for "Answer", "Review", and "Overview". It shows a section titled "C. Privacy" with a question: "Is there collection of, access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information?". Below the question are radio buttons for "Yes" (selected) and "No", and a text area for "Additional Comment". A green "Submit Answers" button is at the bottom. A modal window is open in the foreground, titled "Assign Question(s) To:", with a dropdown menu showing "Susan Baker". The "Message:" field contains the text: "Hi Susan, Please answer these questions! Let me know if you have any questions!". There are "Assign" and "Cancel" buttons at the bottom of the modal.

Automation is required to scale and be efficient. Without a streamlined process you're still relying on a manual system, costing you time and money. A good TPRM solution provides the following capabilities:

- **Conduct third-party assessments**, onsite audits, and surveys to monitor risk.
- **Leverage integrated industry standard templates** like SIG or upload your own existing, proprietary questionnaires
- **Map controls questions or sections** to regulatory frameworks
- **Publish one-time or create a recurring schedule** to automatically send out appropriate questionnaires.
- **Prepopulate questionnaires** with previously submitted answers from vendors to focus on only what has changed.
- **Track assessment progress, manage due dates and review status** of questionnaires across the third party portfolio.
- **Auto score responses** to understand overall risk



TIP: Traditionally, organizations have relied on spreadsheets to prepare, collect, and review surveys for vendor risk audits, an exceedingly time-consuming and labor-intensive process. The good news is that you can automate this process by using TPRM software. TPRM tools are equipped to automate the survey process. With an automated and streamlined survey process, you can multiply your capacity and perform vendor due diligence on a scale that simply isn't possible with the manual and spreadsheet methods.

Third Party Access & Responses

Third-party access to your platform that is truly user friendly is a very important element to ensure you are getting the most from your solution provider. A TPRM solution should provide third parties the necessary features to respond to multiple assessments efficiently without the need to go to multiple channels for exchanging information. Features like collaboration, assignments workflows, and a common file library make the process of responding to assessments more efficient.



TIP: Enterprises entering new markets will likely need to develop new local distribution networks for their goods and services. As a result, enterprise risk management teams need a process to properly assess vendor risk in often-unfamiliar marketplaces. These third-party risks continue to be intensified by regulators and new legislation holding enterprises liable for the behavior of their suppliers, coming from jurisdictions across the globe [2].

Streamlined Evaluation of Third-Party Responses



Saving time and avoiding manual entry is the main driver for adopting a TPRM platform. As such, it's incredibly important that the platform be streamlined and capable of cutting down on any unnecessary documents, steps, and resources. A true streamlined evaluation process should:

- **Evaluate responses on multiple dimensions and auto-score** via a flexible scoring engine.
- **Assign sections or questions** to other subject matter experts for evaluation.
- **Leverage a platform's auto-scoring** to evaluate answers and flag deviations.
- **Clarify questions, resolve issues and collaborate** in one application.

Issues and Track to Remediation

Once you've guided vendors through onboarding and have performed due diligence you're able to enter a new stage of the life cycle, risk and issue management. At this stage a TPRM platform should:

- **Identify and raise the visibility of issues** at a question or section level.
- **Collaborate with third parties and request updates** on issues within the common application.
- **Capture important details** about specific issue severity, resolutions recommendations and issue status.
- **Capture all communications and in context**, in case of an audit or future questions.
- **Create action plans and manage progress** from start to completion.

A TPRM program should address your unique needs as a company with vendors. When selecting the right program for you you'll want to ensure the capabilities covered in this section are addressed.



Analytics to Gain Insights and Monitor Risk Trends

Utilizing available analytics can provide insights to direct your future business and help you monitor risk trends. A good TPRM platform will let you:

- **Gain comprehensive visibility** into trends, risk, and status of third parties.
- **Compare performance, score, and risk of third parties** and run cross-vendor comparisons.
- **Leverage deep search capabilities** to quickly and easily find relevant items.
- **Analyze aggregate third-party data** or drill down to partner/product/service or engagement details to understand source of risk.

PRICING

Vendor risk is not something to take lightly or neglect resources for. According to the Ponemon Institute's "Cost of a Data Breach Report", the global average cost of a data breach was \$3.86 million in the year 2020 [3]. A separate Ponemon survey from 2019 also identified that a data breach caused by a third-party was almost twice as high with an average cost of \$7.5 million to remediate [4]. A recent study by the Institute of Internal Auditors, showed that more than 65% of organizations "rely heavily" on third parties, yet most allocate less than 20% of their internal resources for assessing third party risk [5].

So when deciding on needed value, the best benchmark to measure the cost of a TPRM program is the "Total Cost of Ownership (TCO)". This is the sum of all direct and indirect costs required to develop, implement, and administrate the program. The direct costs are much easier to quantify. These are mostly the software licenses and capital expenditures (CAPEX) required to conduct vendor due diligence and risk assessments.

The indirect costs, also known as "hidden costs", are far more subjective and harder to quantify. According to a 2019 survey of 554 IT and security professionals, the yearly hidden cost of managing vendor risk is \$3.8 million [6].

The variables below are the most common hidden costs driving up TCOs of third-party risk management programs:



As with any enterprise solution, pricing will always be a contributing factor in the decision making process. However, in this instance pricing is not determined by dollar amount, but by value. A platform with the most value will be one that is scalable and has all necessary features available.



TIP: The introduction of automation into the third-party risk management marketplace has emerged as a popular deployment model to mitigate these hidden costs through a purpose-built cloud service provider (CSP) environment.

YOUR PERFECT SOLUTION

Not all third-party risk management solutions are created equal. Use the checklist below to find a good software.

With this TPRM software I can:

- Create a centralized, comprehensive directory of all my vendors**
- Assist with vendor onboarding, including the conducting of pre contract due diligence, and setting appropriate vendor controls**
- Continuously monitor vendor risk, through scheduling recurring assessments for critical vendors, and tracking of progress and updates**
- Streamline the evaluation of third party responses to questionnaires and assessments, through collaboration, customizable and automatic scoring**
- Intelligently identify critical issues, and track their resolution through completion**
- Gain comprehensive visibility over my TPRM program, with insightful analytics of trends across my entire portfolio, and the causal factors behind them**

Your ideal solution may be different from another company's, but by using the guidelines above you'll be able to find your perfect TPRM technology partner.

FROM THE EXPERTS

CENTRL may be the solution you need to protect your company from third party risk. But don't just take our word for it. Our trusted customers, the experts, display our value the best.



“ We are passionate about helping our clients maximize the value they derive from their third-party relationships. Leveraging CENTRL’s leading-edge technology to identify, mitigate and control risks typically associated with these relationships allows us to bring additional value and safeguards to our clients. ”

- **Lois Coatney**, *partner and global leader, ISG Managed Services*

“ We appreciate the speed and responsiveness of the CENTRL support and development team. Our relationship with CENTRL has evolved to more of a partnership than a typical vendor-client connection. ”

- *NYCB's First Senior Vice President, IT Senior Director of Applications, Sharon Michitsch*



New York
Community Bank
Member FDIC



“ Especially in today's world where we are all connected, the ability to pull up the tool directly with the client in the meeting, document live with them in the tool the answers and corresponding scores and reasoning for them, rather than needing to come back with notes tabulated later, has been a game changer. Now, with CENTRL, it's just go fill in the information, risk rank the answers, score them, and you get an output that you can pull from to design your presentation based the output's visuals to tell the story. The tool really gets everything into a single place, all the clients we are managing throughout the year, and facilitates that whole process. ”

- **Kevin Brady**, *Sr. Associate in EisnerAmper's PRTS Practice*

“The tool just helps us document and follow up so much more efficiently, which in turn is bringing in more profit for the firm as we are able to serve more clients.”

- **Tyler Dwyer**, *Sr. Associate in EisnerAmper's PRTS Practice*





Vendor360 for Third Party Risk Management

Vendor 360 is a simple solution to automate the process of ongoing vendor risk analysis while maintaining control of third party risk and oversight. The Vendor 360 platform leverages intuitive workflows to automate third party information gathering, evaluation assessments, risk scoring, issue management, and collaboration with third parties' extended ecosystem of partners.

This functionality enables companies to identify, manage, assess and mitigate third party risks across all stages of the vendor lifecycle. The solution provides easy to use workflows for vendor onboarding, ongoing due diligence, and onsite audits to streamline risk identification. It also provides integrated flows to manage and mitigate issues identified during this process.

For more information, we invite you to schedule a demo or download our datasheet through the contact information listed on the front and back cover.

WORKS CITED

- [1] <https://www.esecurityplanet.com/networks/181-third-party-vendors-access-the-average-companys-network-each-week/>
- [2] <https://www2.deloitte.com/lk/en/pages/risk/articles/on-boards-agenda-april-2016.html>
- [3] <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>
- [4] <https://securityboulevard.com/2020/06/automation-in-compliance-why-its-a-business-imperative-and-where-to-start/>
- [5] https://cfo.cdn.ncms.io/content/uploads/2013/12/Crow_IAA_Study.pdf
- [6] <https://www.businesswire.com/news/home/20190710005065/en/Ponemon-Institute-and-Censinet-Find-Third-Party-Risk-Costs-the-Healthcare-Industry-23.7-Billion-a-Year>

LEGAL DISCLAIMER

This document and the information provided therein were prepared by CENTRL, Inc. for informational purposes only and not for the purpose of providing legal advice. You should obtain independent advice regarding any of the information covered in this document and its applicability to your business.



CENTRL

VENDOR RISK MANAGEMENT



Learn More: oncentrl.com/vendor360

Get a 1:1 Demo: oncentrl.com/demo-request/



US/Global +1-415-780-9667

UK/Europe +44 (0) 20 3389 8429

Australia: +61 1800 531 802



info@oncentrl.com



company/centrl/



[@oncentrl](https://twitter.com/oncentrl)

More Third-Party Risk Management Resources

Enjoy this guide?

Visit www.oncentrl.com/resources

for more best practice guides, videos and ebooks on third-party risk management.

CENTRL

VENDOR RISK MANAGEMENT

CENTRL is a leading risk and compliance technology company that provides a software platform for managing privacy, compliance, and third party risk. CENTRL offers solutions for automating modern slavery act compliance, vendor risk, privacy management, and operational due diligence. CENTRL's platform is used by leading companies in all sectors across the globe.

US/Global +1-415-780-9667

UK/Europe +44 (0) 20 3389 8429

Australia: +61 1800 531 802

And, for more information, please visit: oncentrl.com/vendor360



[@oncentrl](https://twitter.com/oncentrl)



[/company/centrl/](https://company/centrl/)

Rev. 2021.7