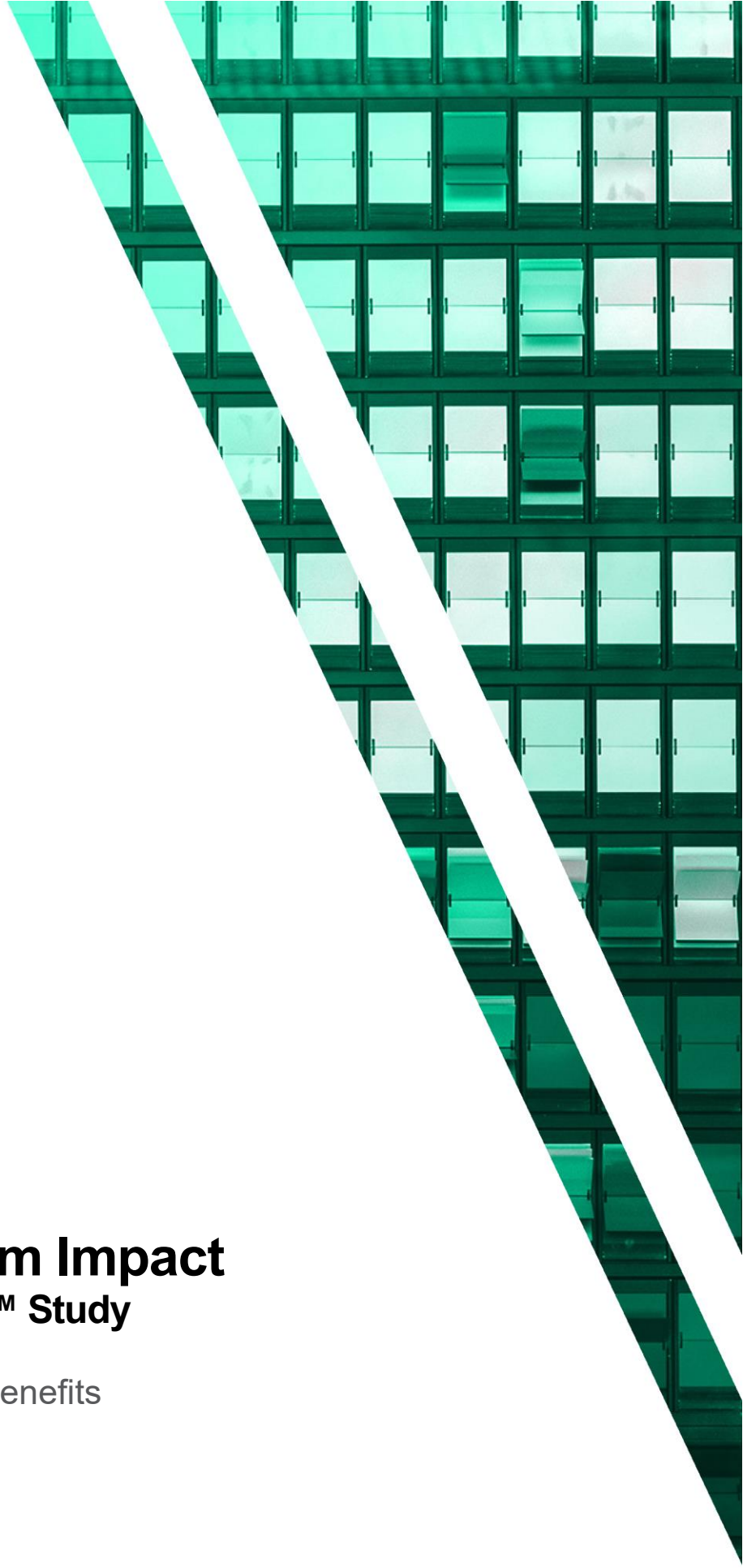
FORRESTER®



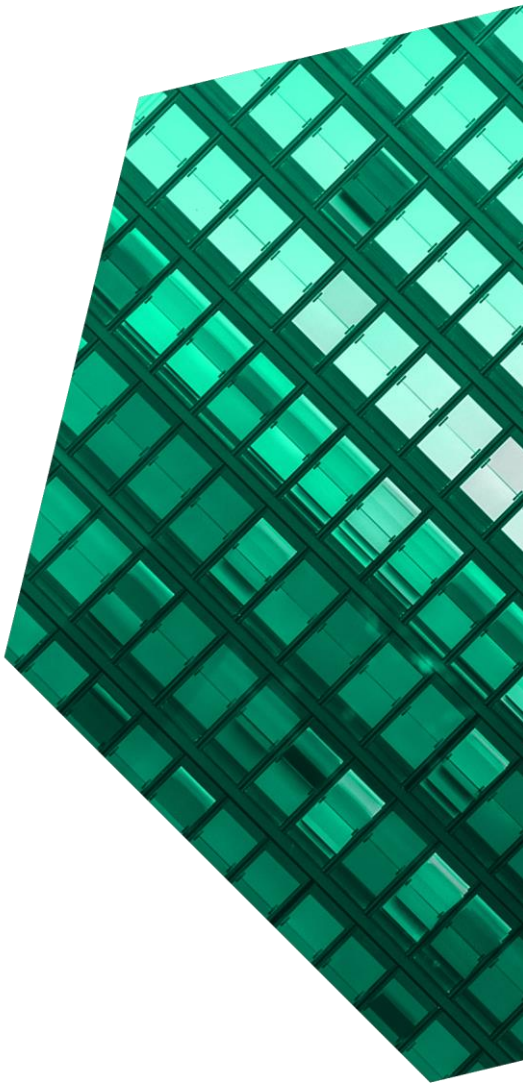
RiskRecon Program Impact
A Total Economic Impact™ Study

Cost Savings And Business Benefits
Enabled By RiskRecon

JUNE 2021

Table Of Contents

Consulting Team: Veronica Iles
Kara Luk



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

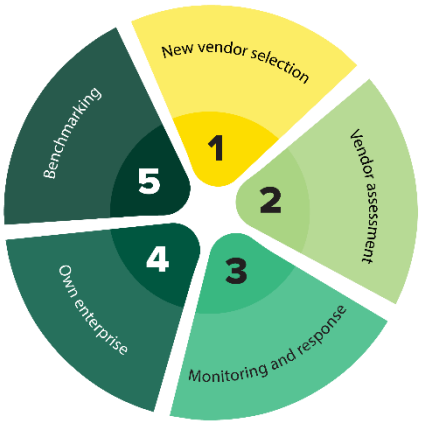
Executive Summary

RiskRecon's continuous monitoring solution detects and corrects cybersecurity risks that threaten organizations and their third-party vendors. The solution helps analysts measurably improve risk posture and hygiene, allowing them to focus assessment efforts where it matters most. With RiskRecon, customers have better visibility to proactively mitigate cyber risk exposure.

RiskRecon is a cybersecurity risk ratings solution and continuous monitoring tool. It uses an enterprise's externally observable data from its external internet presence to generate an aggregated rating of a firm's cybersecurity posture across several security risk factors. RiskRecon's data, customizable risk management policy, and issue prioritization allow customers to focus on the risks that matter most to their organization.

RiskRecon, a Mastercard company, commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying RiskRecon as part of a third-party cyber risk program. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of RiskRecon on their organizations.

RiskRecon Supports Common TPRM Use Cases



KEY STATISTICS

Return on investment (ROI)
147%

Net present value (NPV)
$1.4 Million

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six customers with experience using RiskRecon. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using RiskRecon, most interviewed customers did not have a cybersecurity risk ratings tool in place. Instead, they relied wholly on questionnaires and assessments to determine risk levels. One more mature interviewee's environment had several risk ratings tools. Customers struggled with running third-party risk management programs because of staffing constraints, a growing volume of third parties, and only subjective assessments to rely on. Key results from the study found that enterprises and smaller companies both saw automation and risk reduction benefits with RiskRecon, regardless of how many third parties the tool monitors.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Up to 150% higher productivity for analysts.** RiskRecon enabled analysts to not only identify, understand, and remediate open cybersecurity threats for their own organizations, but also collaborate with third parties and improve their cybersecurity scores. Over three years and across a team of three analysts, the composite organization sees more than $1.1 million in efficiency improvements.

Analyst efficiency improvements

Up to 150%

- **Targeted efforts and automation drive an increase of 56% in efficiency for routine assessments.** The ability to tailor scope and frequency of assessments based on third-party cybersecurity ratings and residual risk enabled analysts to focus on vendors with the highest risk. Instead of treating all vendors the same based on inherent risk, targeting assessments cut level of effort for assessments by 56%. Over three years and a cumulative total of 12,600 avoided assessment hours, the assessment efficiency is worth more than $591,000 to the composite organization.
- **Targeted audit efforts on critical vendors and eliminated 70% of external audits.** By leveraging RiskRecon data as part of the audit plan, analysts identified third parties with consistently healthy risk postures, alleviating the need for a formal commissioned audit on those vendors. The remaining vendors underwent a more targeted audit, increasing the value of the audit and reducing likelihood of significant risk that could create substantial harm to the business. Over three years, the more targeted audit efforts are worth more than $631,000 to the composite organization.
- **M&A use case saves 80 hours of manual due diligence efforts per M&A event.** For each M&A event, utilizing RiskRecon findings allowed analysts to avoid 80 hours of manual due diligence efforts. Over three years and a cumulative total of six M&A events, the process automation is worth nearly $23,000 to the composite organization.

> **"RiskRecon provides value to us for three reasons. First, it is a view into our own reporting, and it make us aware of shadow IT. Second, it shows progress of the program because it is quantifiable data. And third, it gives us the ability to put a risk factor on our third-party program. You would have to do a lot of labor to assign a risk to everyone you did business with."**
>
> *Director of information security, healthcare*

Unquantified benefits. Benefits that are not quantified for this study include:

- Senior leadership's ability to use RiskRecon scores in decision making.
- The ability for customers to proactively respond to incidences.
- A reduction of risk and increase in savings due to shadow IT consolidation.
- Increased savings from build vs buy analysis.

Costs. Risk-adjusted PV costs include:

- **RiskRecon licensing costs under $829,000.** RiskRecon has a subscription-based licensing model and offers four levels with varying feature options. The composite chooses the volume and type of seats according to the size of their vendor landscape and risk-monitoring requirements. Over three years, licensing costs total under $829,000.
- **Internal labor for implementation, training, and ongoing management cost of under $142,000.** A third-party risk (TPR) analyst dedicates 152 hours to initial implementation, optimization, and training. Ongoing management efforts require up to 30% of a TPR manager's efforts. Over three years, internal labor costs total $142,000.

Synopsis. The customer interviews and financial analysis found that a composite organization experiences benefits of nearly $2.4 million over three years versus costs of almost $970,000, adding up to a net present value (NPV) of over $1.4 and an ROI of 147%.

The bottom-line justification for RiskRecon is it improves your risk governance. It improves your cyber risk assessment and, therefore, improves your ability to do better risk governance."

— Partner, strategic risk, professional services

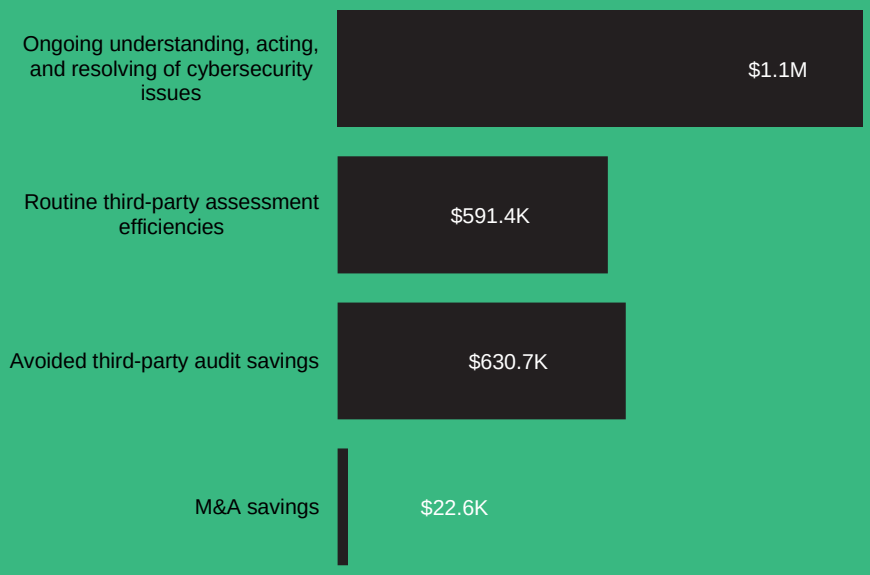
ROI
147%

BENEFITS PV
$2.4 million

NPV
$1.4 million

PAYBACK
<6 months

Benefits (Three-Year)



“Continuous monitoring is a lot easier to implement than you might think — it’s actually very simple to put in place. This program pays dividends and RiskRecon gives you access to the backend data for in-depth investigations, so you can double- and triple-check what you’ve seen in the tool and be able to really provide very targeted and detailed information related to a potential incident. Anybody can put a third-party continuous monitoring program in place very easily with minimum investment and pay off potentially huge returns.”

— VP, third-party cyber risk, financial services

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in RiskRecon.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that RiskRecon can have on an organization.

DUE DILIGENCE

Interviewed Mastercard stakeholders and Forrester analysts to gather data relative to the RiskRecon investment.

CUSTOMER INTERVIEWS

Interviewed six decision-makers at organizations using RiskRecon to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Mastercard RiskRecon Customer Journey

Drivers leading to RiskRecon investment

Interviewed Organizations

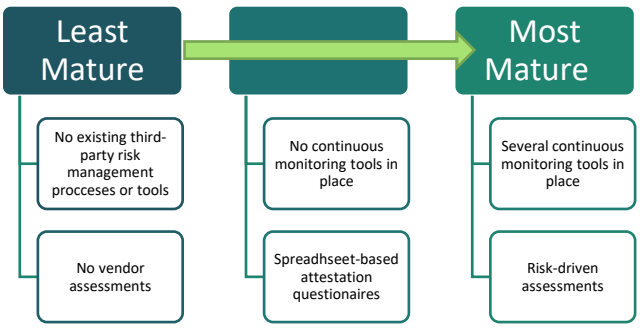
Industry	Region	Interviewee	Size
Healthcare	US HQ and operations	Director of information security	$10 billion in revenue 28,000 employees
Telecommunications	EMEA HQ, worldwide operations	Cyber security manager	$54 billion in revenue 92,000 employees
Professional services	US HQ, worldwide operations	Partner, strategic risk	$2 billion in revenue 8,500 employees
Financial services	US HQ, worldwide operations	VP, third-party cyber risk	$18 billion in revenue 50,000 employees
Information technology	US HQ, worldwide operations	VP, information security	$3 billion in revenue 9,000 employees
Pharmaceutical	US HQ, worldwide operations	Cyber risk management and governance manager	$42 billion in revenue 88,000 employees

PRIOR ENVIRONMENT

The interviewees described prior environments that ran the gamut of maturity from no awareness of third-party risk to well-established programs with multiple cybersecurity risk ratings tools and strategic assessment protocols. Most customers fell into the middle of this maturity spectrum with assessment-based approaches that provided point-in-time snapshots of their third parties' risk posture. Those organizations with developing maturity risk programs had the following characteristics:

- **A reliance on an assessment-based risk management approach.** The interviewee from the financial services organization had a mid-maturity third-party risk management approach before investment in RiskRecon. The program relied heavily on annual assessments, manual data aggregation, and limited issue resolution. This VP of third-party cyber risk shared: "We would email spreadsheet-based questionnaires asking cyber security questions, rate the answers, perhaps asking some follow-up questions, and then open observations or findings based on the answers to those questionnaires. But that was the only thing that we were doing back then."
- **A highly manual program built on home-grown assessment repositories.** The third-party risk management teams manually reviewed vendor assessments, consolidated findings, and stored information in home-grown file repositories. The cybersecurity manager of a telecommunications company shared: "Before RiskRecon, we built a homegrown repository for assessments. Before that, assessments were done mainly in spreadsheets and shared folders, so it was very manual."

Third-Party Risk Program Maturity Spectrum



KEY CHALLENGES

In their prior environments, the interviewees' organizations struggled with common challenges, including:

- **Risk assessment questionnaires were inherently flawed.** Relying on the security questionnaires was troublesome for the interviewees for two reasons: 1) risk assessment questionnaires provided only a point-in-time view into the risk posture of a third party and 2) a third-party representative answers these questionnaires and the answers could be incorrect, since the answers are not validated.
- **Limited frequency of assessments led to dated information.** Contract language and staff capacity limited interviewees' organizations to conducting these questionnaires annually, biannually, or every three years. This left huge gaps between assessments and left customers open to unseen third-party risk threats.
- **Staffing constraints created capacity bottlenecks**. The interviewees' organizations often managed thousands or tens of thousands of third parties with limited manpower. Without a data-driven solution, everything in the process was manual from the questionnaires to the onsite review. Capacity was a huge issue and customers had to choose between hiring several additional resources or face the realization that they could only evaluate a handful of suppliers.
- **Manual processes hindered program effectiveness.** The interviewees described environments with third parties that span the globe, dispersed risk management teams, and fragmented approaches to risk management. The cyber security manager of a telecommunications organization with 23 independently operating risk management teams shared, "The challenge internally was to keep and update documents in one place and then to actually mitigate risk because we were doing it manually."

"Suppliers mark themselves about how good they are in an assessment. We needed something independent that told us about their information security posture without infiltrating their network."

Cyber security manager, telecommunications

"We had an issue with the timeliness of our assessments. We would assess vendors on either one, two, or three-year cycles depending on their risk. So, the assessments wouldn't get refreshed for at least one year, which meant the information was very dated. A lot can happen in a year."

VP, third-party cyber risk, financial services

"There was a clear indication that we were not going to hire 20 people. We were going to have to make it work with some tools, a process, and a strategy."

Cyber risk management and governance manager, pharmaceutical

"One issue we had was the effectiveness of the whole program and process. It was very manual, prone to errors, and very slow."

VP, third-party cyber risk, financial services

- **Previous vendor data was not transparent.** The interviewee whose organization utilized a more mature program with an existing cybersecurity risk ratings tool found insufficient data from the legacy tool's reports, which led to the inability to engage with vendors to help them fix issues and a lack of understanding what issues were causing a drop in risk score.

> **"We have an established score threshold and, if a vendor drops below that score, then we ask them to remediate and get back up above the threshold. In [the legacy tool], we couldn't promise a vendor that this particular fix would get them the increase in score that was needed to meet the threshold."**
>
> *VP of information security, information technology*

WHY RISKRECON?

The interviewees' organizations conducted RFPs and comparative analysis to evaluate vendors. They selected RiskRecon for the following reasons:

- **The ability to tailor issue prioritization based on risk policy.** For the telecommunications customer, the ability to prioritize findings and define important vulnerabilities was a differentiating factor for RiskRecon. The cybersecurity manager shared: "RiskRecon had the capability for us to put a risk policy in place within the tool and, at the time, the other vulnerability scanning tools were a free-for-all. You'd do a perimeter scan and it would turn up thousands of vulnerabilities. With RiskRecon, we can define a risk policy to say we're interested in particular areas and prioritize them."
- **Stand out results for data transparency, issue attribution, and finding integrity.** Interviewees noted that data integrity was a key criterion when evaluating and selecting a cybersecurity risk ratings platform. They compared tool findings to each other and against known risk factors to determine the best fit tool. Interviewees recognized the need to have confidence in the data before approaching third parties with issues.

> **"RiskRecon is the only tool where I actually trust the data. Point blank, period."**
>
> *Cyber risk management and governance manager, pharmaceutical*

- **Cost and scalability of solution.** Potential platforms were also evaluated on future ability and cost effectiveness of scaling cybersecurity risk ratings tool to include critical third parties, fourth parties, and even customers. The interviewees found that RiskRecon's solution was more cost effective than alternatives.

- **The ability to integrate data downstream.** Interviewees evaluated integration capabilities of cybersecurity risk ratings providers including their ability to integrate with enterprise resource planning (ERP) platforms, incidence management systems, and risk assessment and questionnaire tools. RiskRecon delivered on this requirement.
- **An intuitive user interface.** Interviewees expected their cybersecurity risk ratings solution to be easy to understand and have a user-friendly interface. They looked for a solution that was intuitive and simple enough for rapid adoption.
- **RiskRecon culture and service team responsiveness.** The solution provider would also be an ongoing partner and a source of expertise. The VP, third-party cyber risk of a financial services company said: "RiskRecon continues to take our feedback to make the tool better. So, they're really good at listening to the voice of the customer. RiskRecon creates a great experience for us and that was a huge positive."

"First, we chose RiskRecon because of the quality of the data. They do not source data from third parties, they crawl and compile their own data and they provide easy access to the backend data. Second was how intuitive the tool is to use; how easy it was for anyone to just go and get access to it and be productive quickly. And finally was how responsive the whole customer service is and the interaction with them. RiskRecon was just very, very different compared to the other big providers."

VP, third-party cyber risk, financial services

INVESTMENT OBJECTIVES

The interviewees shared several goals they hoped to achieve with the investment in RiskRecon. These goals included:

- **Lower operational risk across the business.** Interviewees shared the importance using the insights provided from RiskRecon to help mitigate cybersecurity risk to the business, reducing the risk of breach and resulting poor cybersecurity consequences. RiskRecon was tapped to help lower operational risk in several key areas: contract management, supply chain logistics, firewall-to-firewall connectivity, compliance, and regulatory requirements.
- **Improved visibility into third-party risk hygiene between assessment cycles.** Using a continuous monitoring tool would allow interviewees' organizations to stay on top of the ever-changing risk landscape and monitor their third parties more frequently than once a year.
- **Comparable scores to industry averages and competitors.** Not only can RiskRecon monitor external third parties' cyber risk hygiene, but it is also a valuable tool for organizations to monitor their own externally visible cyber risk profile. As the cybersecurity risk ratings technology matures, cyber risk hygiene may become a more prominent brand differentiator. The interviewees noted that one goal of their organizations' investment was to monitor their own organizational hygiene compared to industry averages and competitors.
- **Visualization of cybersecurity risk for executives to inform data-driven decisions.** Interviewees hoped RiskRecon would help raise awareness of third-party risk across the organization, especially to non-technical business stakeholders.
- **Monitoring KPIs to prove out program efforts.** Risk is a tricky metric to report on, and interviewees identified RiskRecon as a tool that would help measure KPIs around their organizations' risk program, helping determine impact and prove risk-mitigation efforts were creating value for the organization.

> **"The goal for any cybersecurity program is to reduce risk. The goal for us was to mitigate risk ourselves and, if not, then to raise awareness of the risk internally to our business owners. We are not in control of who they deal with, we can only advise. But now we can give them factual evidence so the business owners can make their own decisions."**
>
> *Cyber security manager, telecommunications*

> **"The main goal was to stay on top of our critical vendors more than just once every year when we went to do an assessment. We need to understand changes that could impact us in between assessment cycles."**
>
> *VP, third-party risk, financial services*

> **"Our goal was to get visibility based on risk, find the risk components that are really driving our operating risk, and then put it up in front of the business in a way that they can make good decisions."**
>
> *Cyber risk management and governance manager, pharmaceutical*

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas a RiskRecon investment financially affects. The composite organization is representative of the six companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The multibillion-dollar organization is headquartered in the US and employs more than 2,000 employees. The third-party risk management team is comprised of three resources. The organization has about 7,000 third parties. 1,200 of these third parties are considered inherently high risk based on the nature of the business relationship. Before the investment in RiskRecon, the composite organization did not have a cybersecurity risk ratings tool in place, used a homegrown tool for spreadsheet-based assessments, and assessed third parties on annual or biannual schedules based on the inherent risk of the third party.

Deployment characteristics. The use cases for RiskRecon include supply chain security, monitoring the Composite's own external cybersecurity presence, benchmarking, M&A due diligence, and executive or board-level communication.

Key assumptions

- **$2 to $10 billion revenue**
- **Use cases: new vendor selection, vendor assessment, monitoring and response, and own enterprise assessment and benchmarking.**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Ongoing understanding, acting, and resolving of cybersecurity issues	$351,000	$526,500	$526,500	$1,404,000	$1,149,782
Btr	Routine third-party assessment efficiencies	$231,790	$238,310	$244,490	$714,590	$591,358
Ctr	Avoided third-party audit savings	$243,000	$256,500	$263,250	$762,750	$630,676
Dtr	M&A savings	$9,072	$9,072	$9,072	$27,216	$22,561
	Total benefits (risk-adjusted)	$834,862	$1,030,382	$1,043,312	$2,908,556	$2,394,377

ONGOING UNDERSTANDING, ACTING, AND RESOLVING OF CYBERSECURITY ISSUES

Before investing in RiskRecon, interviewees' organizations had limited visibility into the cyber risk postures of their third parties via questionnaire results. After the investment, the solution objectively quantified and prioritized vendor cyber risk according to customer preferences, the severity of the issue, and the potential impact if the risk was exploited. Using this information, interviewees' organizations could have open, data-based dialogues with their third parties and constructively collaborate with the vendor to remediate the risk or shore up the defect in their own environment.

The interviewees shared several ways they measured the impact of the RiskRecon investment on their own and third-party security postures:

- **Organizations' own self score increased by an average of 62%.** When utilizing RiskRecon findings to evaluate their organizations' own score, interviewees cited significant improvements to their organizations' own security posture and the ability to identify and consolidate shadow IT events. Customers also compared their risk posture to industry standards and their closest competitors to understand how security can become a competitive differentiation point. Customers used their own score improvements to measurably justify the RiskRecon investment and demonstrate a tangible risk reduction. The director of information security of a healthcare organization shared, "We benchmark against other healthcare organizations and we discuss our RiskRecon scores and track each other's performance."
- **Third-party ecosystem scores improved by an average of 30%.** Interviewees used RiskRecon reports and identified areas of improvement to focus on improving their third-party eco-systems' scores. Interviewees shared that, in the absence of RiskRecon, achieving these improvements would have required them to add between five and 20 new headcounts.

> **"When we started with RiskRecon, our score was in the mid-fives. We worked hard to improve that and now we're around mid-nines. It has given us a good track record of what to improve."**
>
> *Director of information security, healthcare*

- **Customers resolved 70% of security weaknesses within one year.** Armed with trusted objective data, interviewees' organizations could approach third parties about open cybersecurity weaknesses and collaborate with them to remediate the issue. For the interviewee whose organization had a previously established continuous monitoring tool, attribution failure and a lack of visibility into supporting data undermined the organization's ability to approach vendors with identified risk.

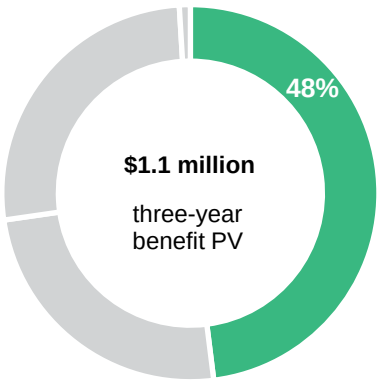
> **"We are now able to have a conversation with a supplier about their end-to-end cybersecurity. The assessment and vulnerability scanning enables us to be clearer with our suppliers about what we expect from them. It also enables us to interact with them monthly rather than once a year."**
>
> *Cyber security manager, telecommunications*

Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes for the composite organization:

- The third-party risk management team is comprised of three full-time resources. In the prior environment, these resources were at full capacity with reviewing security questionnaires, identifying gaps or areas requiring clarification, and providing recommended remediation steps.
- With the investment in RiskRecon, the composite organization avoids hiring additional resources to manage growing demand, effectively increasing the capacity of the three resources by 100% in Year 1 and 150% in Years 2 and 3. These resources now engage directly with third parties to discuss uncovered threats and work on improving both third parties and the enterprise's own score.
- The burdened annual cost of a third-party risk analyst is $130,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and the benefit will vary depending on the size of the third-party cyber risk management team, existing capacity in the prior environment, and the effective utilization of RiskRecon findings.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.1 million.



Ongoing Understanding, Acting, And Resolving Of Cybersecurity Issues					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Risk management FTEs handling security threats and vendor corrective action plans	Composite	3	3	3
A2	Issue prioritization, automated action plan, process automation, and data transparency efficiencies	Interviews	100%	150%	150%
A3	Additional headcount required to support TPR efforts without RiskRecon	A1*A2	3	4.5	4.5
A4	Burdened cost of TPR analyst	Composite	$130,000	$130,000	$130,000
At	Ongoing understanding, acting, and resolving of cybersecurity issues	A3*A4	$390,000	$585,000	$585,000
	Risk adjustment	↓10%			
Atr	Ongoing understanding, acting, and resolving of cybersecurity issues (risk-adjusted)		$351,000	$526,500	$526,500
	Three-year total: $1,404,000			**Three-year present value: $1,149,782**	

ROUTINE THIRD-PARTY ASSESSMENT EFFICIENCIES

Although RiskRecon is not a tool to replace the vendor questionnaire process, it provides visibility into the risk hygiene of third parties. Because of this, organizations can target their efforts on the vendors with the highest need, choosing to pass on companies that have consistently high scores and reprioritizing based on known risk versus just following methodology to save time.

RiskRecon provides the opportunity for organizations to send assessments less frequently and to deprioritize lower risk companies to focus on those that are higher risk. Organizations can also tailor assessments to target areas and issues that they are aware of, providing deeper insights to the cyber security areas that matter most.

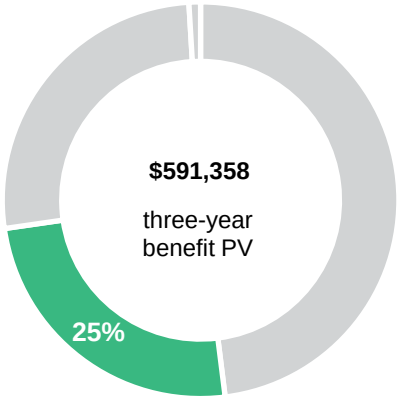
> **"The risk prioritization enables us to narrow down into the highest risk suppliers based on the vulnerability of their perimeters."**
>
> *Cyber security manager, telecommunications*

Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes for the composite organization:

- The composite's third-party risk team evaluates approximately 100 new vendors annually as part of the normal procurement process. In addition to new vendors, it also assesses 10% of its key vendors. It has 1,200 key vendors in Year 1, 1,250 in Year 2, and 1,300 in Year 3.
- In the prior environment, procurement vendors and key vendor assessments took 25 hours on average.
- Approximately 15% of inherently risky vendors are considered medium risk and receive an annual evaluation that each take 10 hours on average.
- After the investment in RiskRecon, the composite focuses its efforts, streamlines its questionnaire, and improves the efficiency of its assessments by 56%.
- The burdened annual cost of a third-party risk analyst is $130,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and the benefit will vary depending on how many assessments are conducted on existing third parties, the number of new third parties procured annually, the extent to which assessment were conducted manually, and how well a customer utilizes RiskRecon in determining who and how often to assess.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of more than $591,000.



Routine Third-Party Assessment Efficiencies

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of vendor assessments conducted for new and key vendors (annual)	New vendors +10% of high-risk vendors	220	225	230
B2	Number of vendor assessments conducted for medium-risk vendors (annual)	15% of vendors	180	188	195
B3	Average hours per assessment in legacy environment for new and key vendors	Composite	25	25	25
B4	Average hours per assessment in legacy environment for medium-risk vendors	Composite	10	10	10
B5	Subtotal: Assessment hours on new, key, and medium-risk vendors in the legacy environment (annual)	(B1*B3) + (B2*B4)	7,300	7,505	7,700
B6	Increase in assessment efficiency using RiskRecon	Interviews	56%	56%	56%
B7	Hours of manual work avoided using RiskRecon (annual)	B5*B6	4,088	4,203	4,312
B8	Hourly burdened cost of TPR analyst	$130,000/2,080 hours	$63	$63	$63
Bt	Routine third-party assessment efficiencies	B7*B8	$257,544	$264,789	$271,656
	Risk adjustment	↓10%			
Btr	Routine third-party assessment efficiencies (risk-adjusted)		$231,790	$238,310	$244,490
	Three-year total: $714,590		**Three-year present value: $591,358**		

AVOIDED THIRD-PARTY AUDIT SAVINGS

RiskRecon is a valuable addition to the third-party risk management toolbelt, but it is not a substitute for multidimensional risk assessments and robust audits. Interviewees' organizations engaged specialist consulting services to help supplement internal security expertise and perform cybersecurity risk audits for the most critical tier of third parties.

With the RiskRecon investment, interviewees' organizations leveraged RiskRecon data as part of the audit plan to determine which vendors to evaluate based on the risk scoring mechanism. As a result, they identified third parties with consistently healthy risk postures, alleviating the need for a formal audit on those vendors. The remaining vendors undergo a more targeted audit, increasing the value of the audit and reducing likelihood of significant risk that could create substantial harm to the business.

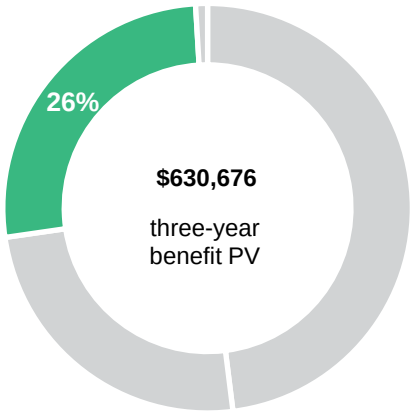
Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes for the composite organization:

- The composite organization has between 1,200 and 1,300 high-risk vendors. Risk is based on the type of information shared and the type of relationship with the vendor.
- Of those inherently high-risk vendors, 10% were considered critical risk in the prior environment and underwent formal audits.
- The audits cost approximately $7,500 per assessed vendor.
- After investing in RiskRecon, the composite audits vendors with the lowest scores, fluctuating scores, and pose the most risk. The composite reduces the percentage of vendors who receive an audit from 10% to 3%.

Risks. Forrester recognizes that these results may not be representative of all experiences and the benefit will vary depending on how an organization uses RiskRecon, the legacy state of professional audits, and the ability to use targeted findings to reduce the number of audits conducted. Other risks to consider are as follows:

- Audit prices vary widely depending on firm choice, engagement terms, and auxiliary expenses like travel and entertainment, lodging, and transportation costs.
- Beyond the value of reducing audit expenses, there is a significant risk reduction and subsequent potential savings from using RiskRecon data to focus on where the risk is highest and identify exposure that the supply chain team missed.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $631,000.



Avoided Third-Party Audit Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Number of inherently high-risk vendors	Composite	1,200	1,250	1,300
C2	Number of critical-risk vendors receiving security audit before RiskRecon	10%*C1	120	125	130
C3	Cost per external audit assessment	Interviews	$7,500	$7,500	$7,500
C4	Number of audits avoided because vendor fell below audit risk threshold	3%*C1	36	38	39
Ct	Avoided third-party audit savings	C3*C4	$270,000	$285,000	$292,500
	Risk adjustment	↓10%			
Ctr	Avoided third-party audit savings (risk-adjusted)		$243,000	$256,500	$263,250
	Three-year total: $762,750			**Three-year present value: $630,676**	

M&A SAVINGS

RiskRecon mitigated risk during the M&A process for interviewees' organizations. By using the tool to gather information about a target's security program, the organizations quickly identified major cybersecurity problems like obsolete infrastructure or poor patch management. With this information, interviewees raised concerns of potential liabilities for decision-makers to consider as part of the deal. Interviewees were able to quantify that RiskRecon helped reduce manual efforts for cybersecurity team while conducting due diligence. Other benefits identified, but not quantified included:

- Avoided capital spending to resolve infrastructure technology problems post acquisition.
- The ability to identify problems to demand tail coverage to protect against cyber liabilities post acquisition.
- Negotiation power for more favorable contractual terms.

Faster due diligence efforts

Saved 80 hours per M&A evaluation

Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes for the composite organization:

- The composite organization conducts due diligence on two M&A targets each year.
- By using RiskRecon to identify issues, the risk team evaluates the target more quickly, saving 80 hours of effort for each target evaluated.
- The hourly burdened cost of a third-party risk analyst is $63.

Risks. Forrester recognizes that these results may not be representative of all experiences and the benefit will vary depending on whether an organization conducts M&A activities, how many M&A targets are evaluated each year, and the burdened cost of resources performing due diligence. Although not quantified here, further savings may be realized, including:

- Reduced purchasing price as a result of using identified concerns as a negotiation lever.
- Avoided capital expenses as a result of requiring tail coverage to protect against post acquisition liabilities.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $23,000.

M&A Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of M&A targets evaluated annually	Interviews	2	2	2
D2	Risk team hours saved per M&A transaction	Interviews	80	80	80
D3	Hourly burdened cost of TPR analyst	$130,000/2,080 hours	$63	$63	$63
Dt	M&A savings	C1*C2*C3	$10,080	$10,080	$10,080
	Risk adjustment	↓10%			
Dtr	M&A savings (risk-adjusted)		$9,072	$9,072	$9,072
	Three-year total: $27,216		**Three-year present value: $22,561**		

UNQUANTIFIED BENEFITS

In addition to the benefits noted above, there were several benefits that customers experienced but were not quantified for this study.

- **Senior leadership used RiskRecon scores to inform decision making.** Communicating with non-IT business roles and senior leaders about technical cybersecurity concepts was a challenge in the prior environment. With a simple scoring methodology, interviewees found it much easier to inform decision-makers properly and objectively about vendor cybersecurity risk concepts.

> **"The scorecard is simple and easy to grasp for people outside of the security industry. Now, it's really easy for our senior leadership to comprehend the scoring mechanisms."**
>
> *Director of information security, healthcare*

- **RiskRecon enabled customers to proactively respond to incidences.** According to Forrester Consulting's Q4 2020 "Cost Of A Security Breach" survey, organizations were likely to see multiple breaches per year with damages in the seven figures for larger enterprises.[1] Interviewees noted that RiskRecon helped them reduce the chances of a breach, but also responded rapidly to incidences before they could become full-blown disasters. The cybersecurity manager of a telecommunications organization shared, "When we hear of an incident then we get a RiskRecon report on that company … so with RiskRecon we can be proactive."

> **"If there is a specific vulnerability out there that we're concerned with, we can look at our portfolio of critical vendors and identify those that could potentially be affected based on what RiskRecon has gathered."**
>
> *VP, third-party risk, financial services*

- **Shadow IT consolidation reduced risk and drove savings.** Shadow IT is more frequently plaguing organizations as solutions are moved to cloud. The migration reduces IT's visibility and its ability to maintain architecture standards and minimize exposure to security breaches. IT can also lead to costly redundancies and tech sprawl. Interviewees used RiskRecon to evaluate their organizations' own domain, which identified web presence of which IT was unaware. Consolidating and removing the shadow IT instances helped reduce risk and provided some minor savings.

> **"We did a [proof of concept] on our domain and were surprised by the depth of the crawl. We found things that our IT department was not aware of like the marketing teams had stood up hundreds of websites. While they weren't necessarily tied to [personally identifiable information], they could still be defaced. So, RiskRecon really gave us a lot of insight into housekeeping in the organization as well."**
>
> *Director of information security, healthcare*

- **Buy-versus-build analysis revealed savings.** The VP of third-party cyber risk of a financial services firm noted that any effort to build a solution similar to RiskRecon would have been extremely costly and time consuming. He shared: "If we were to build this in-house, we estimated the cost was a factor of 10 to 1 compared to a [software as a service] tool that is inexpensive, has zero upfront costs, zero implementation cost, and is very easy to use."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement RiskRecon and later realize additional uses and business opportunities, including:

- **Continuously improve risk policy to prevent data breaches.** Trusting RiskRecon's model accuracy was an important factor for interviewees when choosing a continuous monitoring tool. With RiskRecon, they can evaluate policies to ensure their organizations' efforts reduce data breaches. The cybersecurity manager of a telecommunications company shared: "I'm currently looking at the RiskRecon policy and working internally with our cyberdefense team to see whether what we are actually prioritizing in the tool reflects what we are seeing in the threat landscape. We are talking to our cyber defense team to see the kinds of incidents that are happening through our suppliers. We will then look at the risk policy and decide whether we need to make adjustments."
- **Extended integrations across risk management tools.** To amplify the value of RiskRecon, the platform can integrate with other tools in the risk management stack and organizations can create their own APIs to drive further value. For example, they can take alerts from RiskRecon and generate alerts within their incidence management system, helping to measure the number of tickets and how many have been resolved.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

"We plan to be more proactive and do more continuous monitoring of vendors. We're moving away from doing the questionnaires more and more. Tools like RiskRecon will be part of our strategy for the foreseeable future. We want to do more with the tool rather than less."

VP, third-party cyber risk, financial services

RISKRECON DATA FEEDS CONSULTING USE CASE

One interviewee shared how her organization uses RiskRecon in an out-of-the-box way — leveraging the risk data to inform risk assessment consulting efforts.

The partner of strategic risk at a professional services firm shared: "We've built [our consulting product] using risk intelligence. We could do it without RiskRecon data, but it's just not going to be as accurate. Our use case is to get a very specific risk assessment of an organization and to then apply that risk assessment within the context of a quantitative model. In the absence of having the data, we used other statistical approaches to figure out answers and there were certainly more blind spots and points of inaccuracy that can arise in that approach. Having reliable data that helps us formulate predictions about the future gives us an advantage over having no data."

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	RiskRecon licensing	$0	$316,863	$342,735	$342,735	$1,002,332	$828,810
Ftr	Internal labor	$10,534	$52,800	$52,800	$52,800	$168,934	$141,839
	Total costs (risk-adjusted)	$10,534	$369,663	$395,535	$395,535	$1,171,266	$970,649

RISKRECON LICENSING

RiskRecon has a subscription-based licensing model that consists of four licensing levels with varying feature sets. These levels include Discover, Advisor Snapshot, Advisor, and Own Enterprise.

Interviewees selected licensing types based on the priorities of their organizations' third-party risk monitoring program, the size of their vendor landscape, and number of high-risk vendors in their environment. All interviewees held at least one Own Enterprise seat dedicated to monitoring their own company's risk profile. They noted that their organizations grew the number of vendors monitored with additional licenses after Year 1 of the investment. One interviewee's organization purchased an unlimited license, allowing the organization to monitor its entire third-party ecosystem as well as select customers and fourth parties.

Regardless of the number of third parties monitored with RiskRecon, customers found that their third-party risk management teams gained value from RiskRecon data and ratings. The larger, more mature organizations utilized platform customizations, while smaller organizations relied on the preconfigured out-of-the-box functionalities to reduce manual efforts and provide visibility into third-party risk postures.

Modeling and assumptions. Based on the costs incurred and license seats the interviewees' organizations hold, Forrester assumes the following:

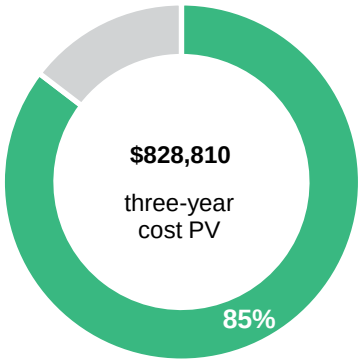
- The composite organization's licensing fees for RiskRecon are $288,000 in Year 1 and grow to $312,000 in Years 2 and 3. This increase occurs as it purchases additional licenses based on the growth of the composite's vendor ecosystem, successful use of the tool in Year 1, and growing demand to better monitor third-party security posture.

Risks. Forrester understands that licensing costs may vary by organization and the best way to determine licensing costs is to speak directly with a RiskRecon sales representative. Factors to consider when estimating licensing costs include:

- The size of the third-party ecosystem, inherent risk of third parties, and the number of information-sharing parties that will be monitored with RiskRecon. The ROI will scale with the number of vendors an organization licenses and there may be licensing efficiencies when licensing additional seats.
- The number of new vendors added each year through organic growth or M&A activity that will be evaluated through RiskRecon.

- The possibility of monitoring stakeholders beyond third-party vendors, including fourth parties and customers.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $828,810.



RiskRecon Licensing

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	RiskRecon licensing	Composite	$0	$288,057	$311,577	$311,577
Et	RiskRecon licensing	E1	$0	$288,057	$311,577	$311,577
	Risk adjustment	↑10%				
Etr	RiskRecon licensing (risk-adjusted)		$0	$316,863	$342,735	$342,735
	Three-year total: $1,002,332			**Three-year present value: $828,810**		

INTERNAL LABOR

Customers incurred internal labor costs related to the implementation and ongoing management of RiskRecon:

- **Implementation costs.** The interviewees described implementation timelines ranging from two weeks to two months, involving the effort of one member of the interviewees' third-party risk teams. A portion of this work involved collecting and inputting the names and domains of to-be-monitored companies. The bulk of the time was spent on initial configuration work with dedicated RiskRecon customer success representatives who helped to optimize the platform according to customer risk policies and thresholds. Interviewees shared that they found RiskRecon to be very receptive and collaborative during this process.
- **Training.** Customers cited minimal training requirements due to RiskRecon's ease of use and intuitive user interface. Each new third-party risk resource typically took one to two hours of training on the platform and its functionalities.
- **Ongoing management.** Interviewees noted that RiskRecon requires minimal management, estimating that no more than 30% of an employee's time is assigned to platform maintenance. Ongoing management activities included onboarding vendors, resolving issues with third parties, analyzing data, and reporting. Customers also spent time on monthly check-in calls with RiskRecon's customer success team.

> **"The tool is pretty intuitive. When we add a new vendor to the portfolio, all we do is provide a name and a domain, so implementation is minimal."**
>
> *VP of third-party cyber risk, financial services*

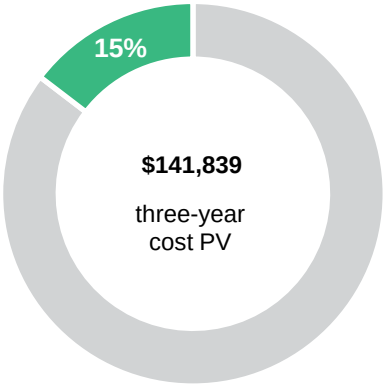
Modeling and assumptions. To capture the findings of the customer interviews, Forrester assumes the following for the composite organization:

- 152 hours of a third-party risk analyst's time is allocated to inputting domains, optimizing, and undergoing training in Year 1. The annual burdened cost of a TPR analyst is $130,000.
- A third-party risk manager is tasked with ongoing management. Only 30% of the manager's time is spent maintaining RiskRecon.
- The annual burdened salary of a third-party risk manager is $160,000.

Risks. Internal labor costs can vary due to uncertainty related to:

- The total volume of vendors entered during implementation and how frequently new third parties are added or moved on/off the platform.
- The availability of an organization's vendor domain list during implementation.
- The market rate and burdened salaries associated with third-party risk managers and analysts.
- The length of issue remediation conversations with third parties.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $142,000.



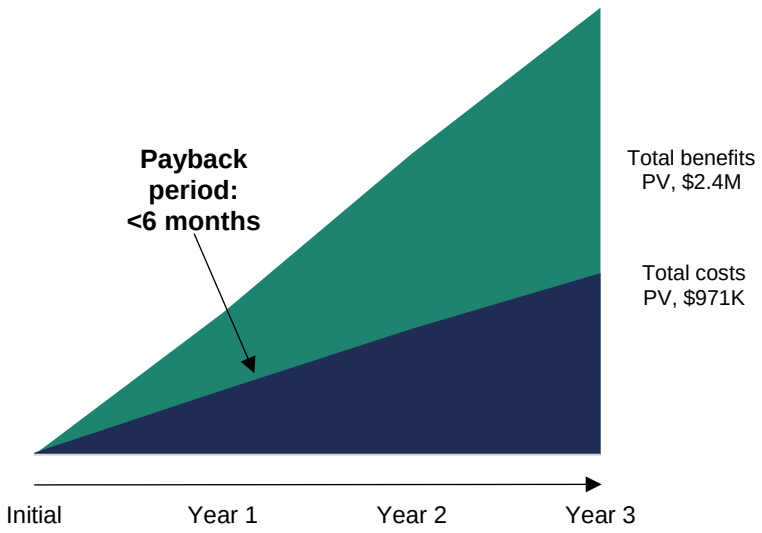
Internal Labor

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Hours dedicated to product evaluation, implementation, and training	Interviews	152			
F2	Hourly burdened cost of TPR analyst	$130,000/2,080 hours	$63			
F3	Number of FTEs tasked with ongoing management	Interviews		0.30	0.30	0.30
F4	Burdened cost of TPR manager	Composite		$160,000	$160,000	$160,000
Ft	Internal labor	F1*F2 + F3*F4	$9,576	$48,000	$48,000	$48,000
	Risk adjustment	↑10%				
Ftr	Internal labor (risk-adjusted)		$10,534	$52,800	$52,800	$52,800
	Three-year total: $168,934			**Three-year present value: $141,839**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Financial Summary



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($10,534)	($369,663)	($395,535)	($395,535)	($1,171,266)	($970,649)
Total benefits	$0	$834,862	$1,030,382	$1,043,312	$2,908,556	$2,394,377
Net benefits	($10,534)	$465,199	$634,847	$647,778	$1,737,290	$1,423,728
ROI						147%
Payback period (months)						<6

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Survey data represented is based on a data subset base of 84 manager level or higher security professionals at organizations within the 2,000 to 4,999 employee segment, taken from Forrester Consulting's Q4 2020 Cost of a Cybersecurity Survey.


FORRESTER®