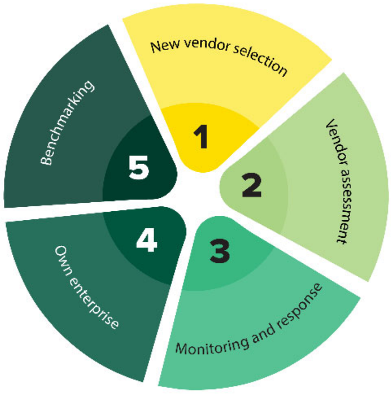
RiskRecon: Helping You Optimize Business Outcomes And Reduce Risk

While business partners are essential for any organization, the sharing of data poses a significant threat. Organizations must realize they are responsible for both their own and their partners' cyber security hygiene. Technology leaders are increasingly aware that the failure to properly assess third-party risks can expose their organizations to data breaches, supply chain attacks, and the reputational whiplash that follows.

RiskRecon, a Mastercard company, is a cybersecurity risk ratings solution that uses externally observable data about an enterprise's external internet presence to give a single, 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. With RiskRecon, organizations of all sizes can detect and correct cybersecurity risks that threaten their partners and their own organizations.

RiskRecon Supports Common TPRM Use Cases



To better understand the benefits, costs, and risks associated with RiskRecon, Forrester Consulting was commissioned to interview six customers and conduct a Total Economic Impact™ (TEI) study. The interviewees utilized RiskRecon's data to develop several use cases, which will be described in this spotlight.

NEW VENDOR SELECTION

Integrating a cybersecurity risk ratings tool into the procurement and contracting process for new-vendor evaluation was the most widely adopted use case for this type of tool. Historically, procurement departments relied on the security team to assess vendors through a routine security questionnaire. Third-party risk (TPR) analysts faced conflicting pressures to perform both timely *and* thorough assessments on increasing volumes of vendors.

When using RiskRecon during vendor selection, TPR analysts and/or the vendor risk management team can quickly pull a cybersecurity report card that rates the vendor's publicly facing risk posture. The information in the report enables the vendor management team to identify threats or noncompliance with security and IT requirements.

VENDOR ASSESSMENT

Attestation-based annual assessments are a time-intensive responsibility for third-party security and risk teams. The work involved with vendor assessments is notably manual, restricting analysts to only monitor a portion of vendors and to prioritize vendors without any data-driven insights. Analysts spent much of their time manually collecting and aggregating data, and insufficient time analyzing and acting on the assessment results.

With RiskRecon, TPR analysts armed with this information can 1) prioritize those vendors with the highest inherent risk and issues RiskRecon data identifies; 2) target questionnaires to the specific areas of known risk; and 3) proactively work with the vendors to improve their scores.

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

MONITORING AND RESPONSE

Without a continuous monitoring tool such as RiskRecon, interviewees relied on infrequent point-in-time snapshots into their organizations' third-party risk postures. If a breach were to occur, it might not be revealed until well after the incident, leaving large windows of vulnerability for the interviewees' organizations.

The investment in RiskRecon enables organizations to continuously monitor critical vendors. Interviewees noted that RiskRecon has helped their organizations proactively respond to breach incidences in their vendor ecosystem much sooner than previously possible. The VP of third-party risk for a financial services firm said: "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."

The interviewees shared that their organization uses the data within RiskRecon as a starting point for initiating conversations with those vendors with a lower than satisfactory risk score to remediate the open issues.

OWN ENTERPRISE

Another popular use case for interviewees was to use RiskRecon to evaluate their own organizations' domain, which identified web presence that IT was previously unaware of. By removing shadow IT instances, interviewees increased their organizations' own cybersecurity scores, improved IT's ability to maintain architecture standards, and minimized exposure to security breaches. Interviewees used their own score improvements to measurably justify the RiskRecon investment and demonstrate a tangible risk reduction.

BENCHMARKING

Customers compared their risk scores to industry standards and their closest competitors to understand how security is a competitive differentiation point. The director of information security for a healthcare organization shared, "We benchmark against other healthcare organizations, discuss our RiskRecon scores, and track each other's performance."

> **"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*

→ READ THE FULL STUDY HERE

KEY RESULTS

The interviews with RiskRecon customers revealed several quantified and unquantified benefits of their investment. The quantified benefits are as follows:

Benefit 1: Ongoing understanding, acting, and resolving of cybersecurity issues

- **Up to 150% higher productivity for analysts.** RiskRecon enabled analysts to identify, understand, and remediate open cybersecurity threats for their own organizations and to collaborate with third parties to improve their cybersecurity scores. Over three years and across a team of three analysts, the efficiency improvements are worth more than $1.1 million to the composite organization.

Benefit 2: Routine third-party assessment efficiencies

- **Targeted efforts and automation drive 56% 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.

Benefit 3: Avoided third-party audit savings

- **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.

Benefit 4: M&A savings

- **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.

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: “The Total Economic Impact^{TM} Of Mastercard RiskRecon,” a commissioned study conducted by Forrester Consulting on behalf of Mastercard, May 2021.

STUDY FINDINGS

Forrester interviewed six organizations with experience using RiskRecon and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Up to 150% higher productivity for analysts.
- Targeted efforts and automation drive 56% efficiency for routine assessments.
- Targeted audit efforts on critical vendors and eliminated 70% of external audits.
- M&A use case saves 80 hours of manual due diligence efforts per M&A event.

Return on investment (ROI)

147%

Net present value (NPV)

$1.4 million

DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Mastercard and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Mastercard RiskRecon.
- Mastercard reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester’s findings or obscure the meaning.
- Mastercard provided the customer names for the interviews but did not participate in the interviews.

ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.

FORRESTER®