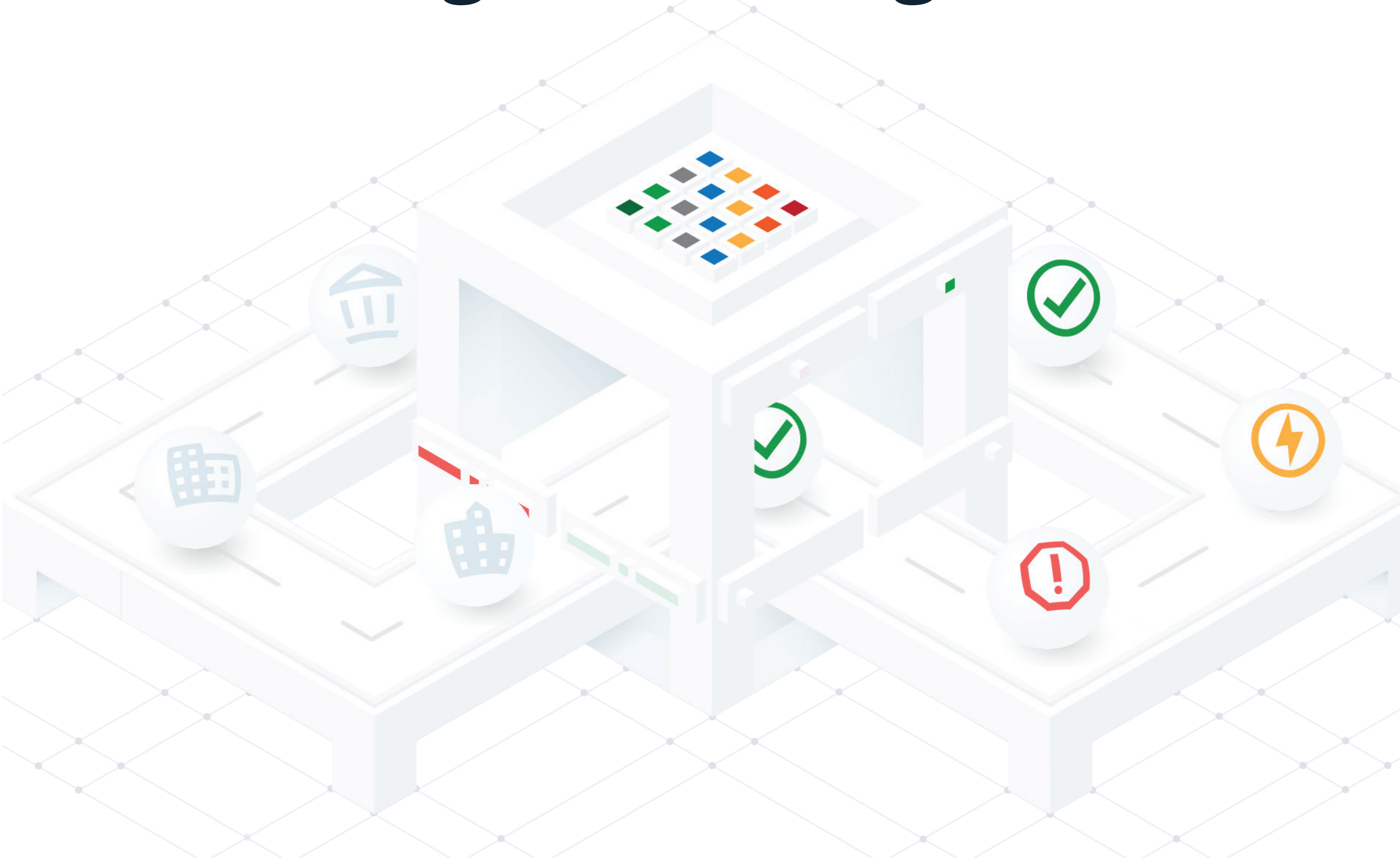
riskrecon
mastercard

10 Steps to Incorporating Continuous Monitoring into Your Third-Party Risk Management Program



RiskRecon.com
sales@riskrecon.com

Salt Lake City, UT
Boston, MA
(801) 758 - 0560

Introduction

Continuous monitoring is a valuable tool for organizations seeking to improve their cyber third-party risk management programs. Adding an ongoing view of the biggest vulnerabilities that vendors expose to the internet can help enterprises regularly validate the answers they've historically taken on faith from annual security questionnaires. More importantly, enterprises can start to institute proactive governance practices based on empirical, continuous evidence of risk.

As a result, it's possible to move from a manual, one-size-fits-all vendor risk process to one that is scalable and risk-adjusted.

If your organization seeks to gain more risk visibility than questionnaires offer but struggles to scale up coverage through on-site reviews, continuous monitoring can offer a clear path to better results. But moving from a questionnaire-based approach to a program backed by continuous monitoring will take planning and finesse to successfully pull off. Here's what it will take to elegantly incorporate continuous monitoring into the mix.

STEP 1. SET YOUR POLICIES

Before your organization sets up its continuous monitoring mechanisms, it needs to first start by thinking critically about the third-party risks it most wants to quantify. Identifying the risk levers that will expose the business to the biggest or most-likely losses will provide a guided framework for instrumenting the monitoring.

As your team examines the most relevant areas of risk, it should start carving them out into buckets based on both vulnerability levels and associated threats to the business. These categories can then feed the governance policies that monitoring will support. These policies will determine which steps should be taken for remediation based on the type of vendor or supplier, the system in question, and the kind of security finding uncovered.

For example, critical vulnerabilities found in connected systems run by a financial services vendor will most definitely require a different set of remediation actions than medium vulnerabilities in a random web server run by a parts supplier. Establishing clear policies ensures that monitoring can be tuned to alert and route mitigation work accordingly.

Every organization will be different, but the people your organization will want at the table during these policy discussions should include stakeholders like the chief security officer, chief risk officer, legal, cyber third-party risk managers, and vendor risk management personnel. As they set policies, this team should keep in mind the regulatory requirements the business will be dealing with in order to ensure that policies align with those.

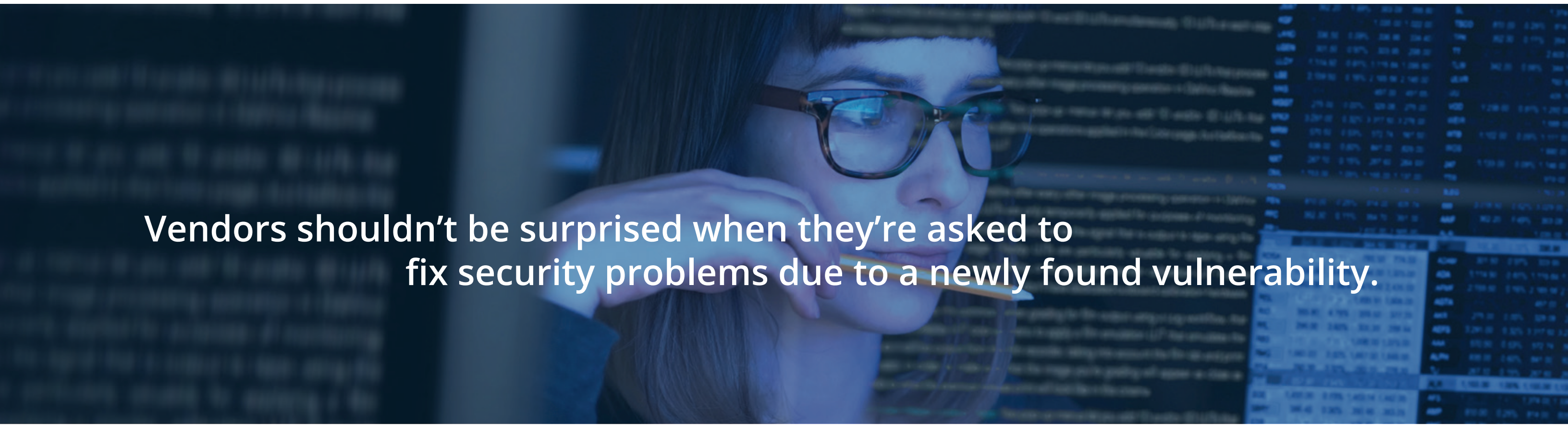
STEP 2. MAP INTERNAL STANDARDS AGAINST OBJECTIVE DATA

Once you set the stage with policy goals, it's time to start surveying the governance mechanisms already in place for relevant vendors and figuring out where the organization can bolster that with objective data.

A lot of organizations already have security questionnaires they use to assess vendors. They should now take the opportunity to look at the questions that already exist, the standards developed by policies, and map that against the empirical information that can be collected by continuous monitoring to gain a fuller, more timely understanding of the risk posed by each vendor.

The mapping process should determine:

- which vendors and suppliers should be covered by monitoring,
- what data should be collected,
- how the data triggers further investigation,
- what the remediation actions look like, and
- the cadence with which data should be analyzed (daily, weekly, monthly).



Vendors shouldn't be surprised when they're asked to fix security problems due to a newly found vulnerability.

STEP 3. DO A PILOT

Take baby steps first. Rather than rolling out continuous monitoring across all vendors at once, consider starting with a pilot. Start observing a select group of vendors for one or two business quarters. The pilot group could be chosen by the business function they support or simply by expedience—sometimes the easiest bet is to choose a set of vendors already scheduled for their annual assessment during the pilot period.

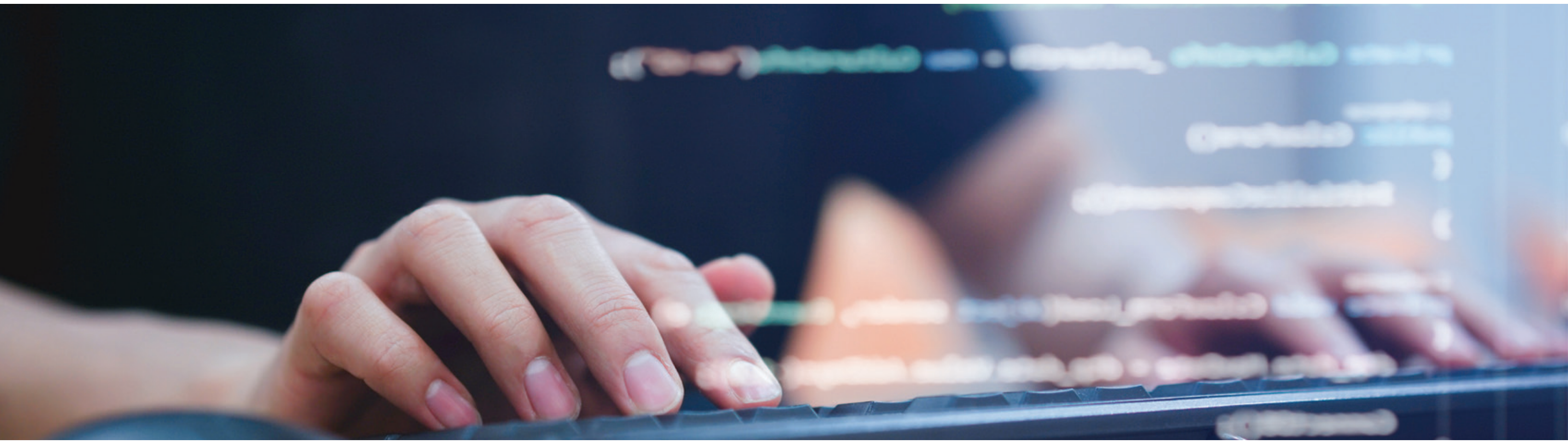
The pilot provides a good opportunity to train up risk management analysts on how risk scoring data works and gives them a chance to figure out how to best develop new workflows in how they engage with vendors. Management can track things like analyst productivity, remediation effectiveness, and feedback from third parties to pragmatically tweak policies and monitoring coverage to match the realities of the business.

In addition to learning through trial and error, the pilot stage should be a time for building up evangelism for continuous monitoring—both internally and among vendors. Monitoring champions should be clearly communicating how the approach is improving the program.

STEP 4. SETTING EXPECTATIONS

Before you begin rolling out continuous monitoring across the wider portfolio of third-party vendors, start having conversations with them to set expectations. Be upfront about what the improved governance model looks like and what it means for them as a supplier. Explain clearly how continuous monitoring tools collect data, and what certain findings will require them to remediate in order to maintain good standing as a supplier.

The key here is that vendors shouldn't be surprised when they're asked to fix security problems due to a newly found vulnerability. Ideally, communication should be done in the spirit of partnership. Your organization can help them improve their security posture with alerts to serious problems they may have overlooked, and that's good for everyone involved. Part of the process may be in explaining that continuous monitoring is not an invasive look into their systems—it is simply identifying the broken windows observable from outside of their metaphorical building.



STEP 5. EMBED POLICES IN CONTRACT LANGUAGE AND RFPS

Not only should your organization set expectations informally through training and evangelism, but it should also formalize policies through contract language. Contracts and RFPs should be developed to set enforcement policies and procedures that layout remediation actions and timeframes. As with any contract, there will obviously be a collaboration with vendors to customize based on the relationship, but at a high level, you should be inserting prevailing policies into standard contracts.

STEP 6. USE AUTOMATION AND TOOLS TO OPERATIONALIZE RISK DATA

The additional visibility afforded by continuous monitoring of third-party cyber risk can potentially add a heavy burden on those in charge of engaging vendors to toe the line. This is why automation and tooling on the remediation end of the process should be a crucial component to include within a continuous monitoring platform.

Consider the following back-and-forth process that continuous monitoring findings could potentially elicit:

- Monitoring finds a list of problems at a vendor
- You need to prioritize risk and identify remediation actions
- You must inform the vendor to make certain fixes based on risk levels
- The vendor thinks they fixed the relevant issues and informs you of their response
- Monitoring finds only part of the issues were remediated
- You must go back to the vendor to let them know that further action is warranted
- The vendor makes further fixes but also finds a false positive
- You've got to verify their additional fixes
- You also must verify their false positive
- You close this round of validation

That is a lot of work for a team to handle if human intervention is required at each of these steps. Ideally, your organization should seek an automated tool that can remove manual work from each stage in this operational process. Not only will that put internal operations on rails, but it will also make remediation less onerous for vendors as well.

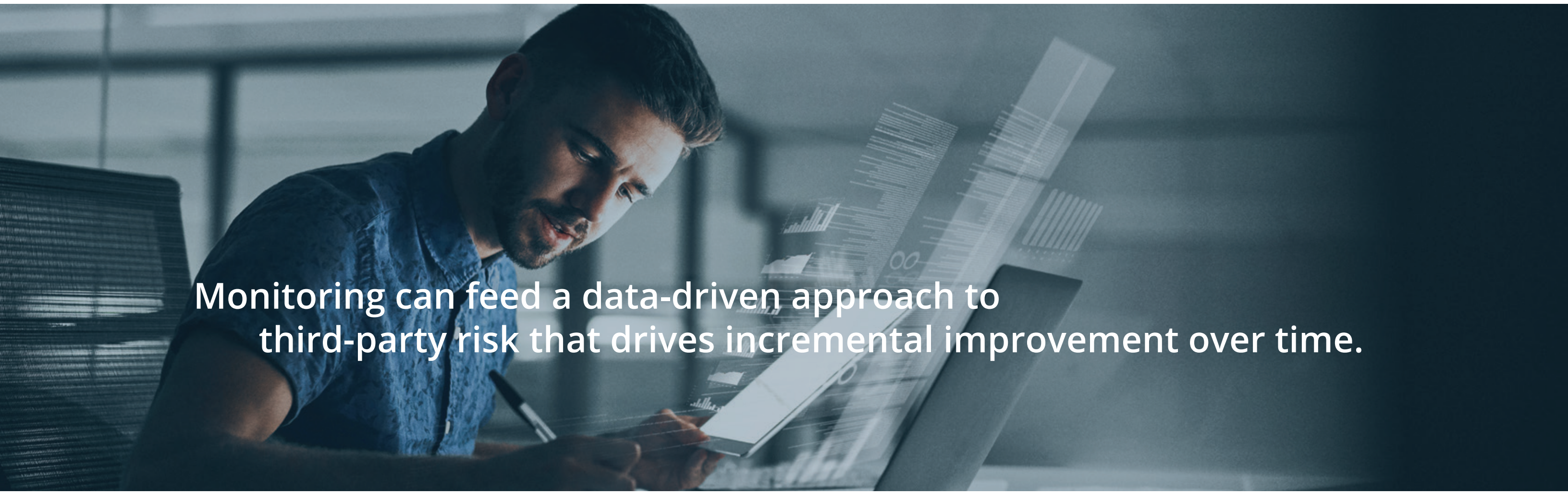
STEP 7. SHIFT INTERNAL RESOURCES TO SUPPORT VENDORS

Even with the best remediation automation, continuous monitoring will still require additional support from your third-party cyber risk management teams. There simply will need to be people available to evaluate what's going on with vendors. It's important to be realistic about the requirements here. If your current resources are limited, you either need to work with the powers that be to build a bigger team or repurpose people from elsewhere.

One way to do this is to start looking at staff dedicated to running questionnaire programs and rethinking how they work. With continuous monitoring in place, it may be possible to cut back on how often questionnaires are run and use people who validate those to instead run the continuous monitoring function. This way engagement roles spend more targeted time on the vendors you've got demonstrable problems with.

STEP 8. INTEGRATE THIRD-PARTY CONTINUOUS MONITORING INTO CYBER INCIDENT RESPONSE

As your organization gets further along into the use of continuous monitoring of third-party vendors, consider integrating this risk data into your internal organization's cyber incident response process. This makes it easier for your security analysts to pick up on big changes in third-party environments that occur between regular assessments that could warrant emergency remediation. It also smooths the way for the organization to respond to "celebrity vulnerabilities" tracked by the SOC that would be worth immediate follow-up with third-party vendors to ensure their systems aren't exposed to these newly found threats.



Monitoring can feed a data-driven approach to third-party risk that drives incremental improvement over time.

STEP 9. MAKE INCREMENTAL IMPROVEMENTS ALONG THE WAY

As your organization starts to accumulate historical data on all of its vendors it can start using that store of monitoring information to make continuous improvements on how it manages third-party cyber risk. Using historical risk and objective data it can be possible to expand visibility into unmanaged vendors and fourth parties. A broader base of experience can also help your team streamline assessment processes, extend coverage, and quickly pinpoint where they need to focus their efforts to get the most risk reduction from their efforts.

The point is that monitoring can feed a data-driven approach to third-party risk that drives incremental improvement over time.

STEP 10. FEED CYBER DATA INTO BROADER VENDOR RISK MANAGEMENT PROGRAM REPORTING

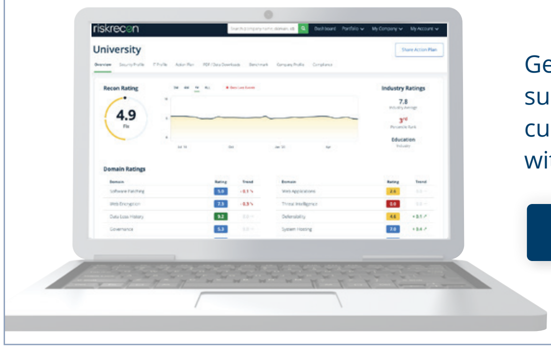
Throughout the process of incorporating continuous monitoring into your third-party cyber risk management program, it's crucial to remember that the results from this monitoring should also be feed into broader vendor risk management program. Cyber risk should be reported alongside other types of risk, like financial and operational risk. These third-party cyber metrics will obviously be reported up through the executive chain by the CSO when explaining the company's complete cyber risk posture. But it should also be included in regular documentation of broad business risk categories.

REAPING THE BENEFITS OF CONTINUOUS MONITORING

Folding continuous monitoring into a third-party cyber risk management program will take a decent runway for successful takeoff. Based on experience, full implementation of the steps we've described here typically takes a year or more.

However, the results will have long-lasting benefits. Once you've implemented continuous monitoring, your firm will be able to use verifiable and objective risk assessment information to fuel a risk-adjusted program that can have a laser focus on quickly fixing the problems that expose it to the most cyber risk.

Get Your Risk Report



University

Recon Rating

4.9

Industry Ratings

7.8

3rd

Education

Domain Ratings

Domain	Rating	Trend	Domain	Rating	Trend
Software Patching	5.0	-0.1 ↘	Web Applications	2.6	[illegible]
Web Encryption	7.3	-0.3 ↘	Threat Intelligence	0.0	[illegible]
Data Loss History	9.2	[illegible]	Defensibility	4.6	+ 0.1 ↗
Governance	5.3	[illegible]	System Hosting	7.0	+ 0.4 ↗

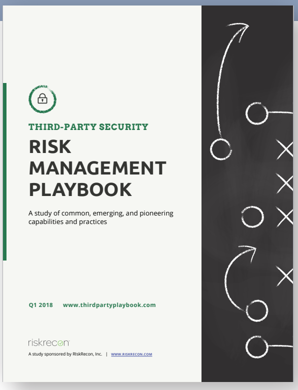
Get a free risk report with a summary of your organization's current cybersecurity posture with influencing risk factors

Get Your Risk Report

Third-Party Risk Management Playbook

The Playbook is built directly from the third-party security practices observed in 30 leading enterprises around the world. Compare your own program with the Playbook data and identify the capabilities and practices that make sense for your organization.

Get the Playbook



THIRD-PARTY SECURITY

RISK MANAGEMENT PLAYBOOK

A study of common, emerging, and pioneering capabilities and practices

Q1 2018 www.thirdpartyplaybook.com

riskrecon

A study sponsored by RiskRecon, Inc. | WWW.RISKRECON.COM