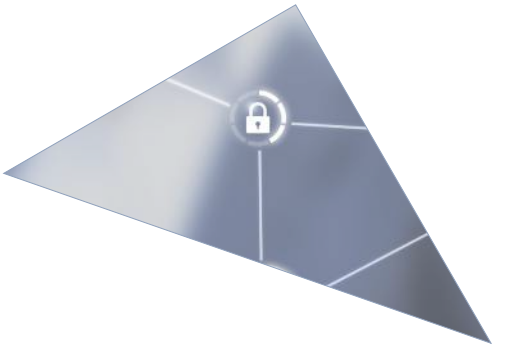
BITSIGHT
The Standard in SECURITY RATINGS

EBOOK

4 Ways To Optimize Your Vendor Onboarding Process

With BitSight Security Ratings

Onboarding New Vendors Quickly And Securely Requires A Delicate Balance



Third parties are essential to helping businesses grow and stay competitive, but if you are not careful, your trusted partnerships can introduce unwanted cyber risk and overhead into your organization.

Worse: The cybersecurity threat posed by third parties grows commensurate with the number of businesses your company is working with. If your organization is like most, that can be a big number.

According to Gartner,[1] 60% of organizations now work with more than 1,000 third-party vendors – including partners, subcontractors, and suppliers. These third-party vendors and suppliers can help you become leaner, more agile, flexible, and efficient, which makes them desirable business partners.

But before they become partners, you need to ensure they are vetted properly. That can be difficult to do if you do not have all the information you need to evaluate their cyber risk posture effectively.

It is even harder when you are getting pressure from executives to accelerate your vendor onboarding processes and make quick decisions about vendor risk so that your organization can continue to grow and stay competitive. Hence, you may feel compelled to complete cybersecurity risk assessments too quickly, which could lead to unknown risks entering your organization.

How can you ensure you are performing the necessary security assessments and evaluations while keeping your onboarding process as flexible and agile as possible?

With BitSight for Third-Party Risk Management (TPRM), you can gain immediate visibility into cyber risks within a potential vendor's ecosystem – enabling you to reduce your onboarding time and costs, and scale your processes to assess and monitor all of your vendors with your current resources.

Ultimately, this makes it easier than ever for you to balance your need for speed with security.

1 https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk/

Making Vendor Onboarding More Efficient

Many security managers turn to a “one-size-fits-all” approach to onboarding new vendors, where each third party is assessed in the same manner.

But every vendor is different, and cookie-cutter assessment practices are not scalable to suit each third party. After all, you don’t want to spend unnecessary time and resources doing extended, full-blown assessments on non-critical vendors. You will end up undermining your efforts to onboard more quickly, as well as your business’ goals to go to market faster and gain a competitive edge.

Let’s look at how you can streamline your assessments and yield better results.

TIP #1

Group Vendors By Criticality

Prioritize your efforts by grouping or tiering potential vendors based on how critical they are to your organization. A “critical” vendor is one that has access to your sensitive data or provides an important service.

For example, a payroll provider working with confidential employee and company information represents a much higher level of inherent risk than a food service provider that does not have direct access to your network.

Tiering helps determine whether a vendor needs a more in-depth assessment or requires fewer touchpoints. Perhaps a non-critical vendor does not need to fill out a lengthy questionnaire assessment after all, whereas a more critical vendor may require that questionnaire – and an on-site visit.

You can scale the assessment process accordingly, allocating your resources to areas which require more due diligence – empowering you to achieve greater efficiencies while still managing third-party risk effectively.

THINGS TO CONSIDER

- The type of data the vendor will hold
- What services the vendor is being used for
- Whether the vendor will have persistent access across your network

TIP #2

Evaluate Third-Party Cyber Risk

Once you have tiered your vendors, it is time to take a closer look at their security postures.

At this stage, it is important to have a common, standard set of cyber risk KPIs that allow you to measure and communicate the effectiveness of a potential vendor's security program. Calculated using externally observable and verifiable data, BitSight Security Ratings provide an instantaneous snapshot of each potential partner's overall security posture.

These ratings, which range from 250 to 900, empower you to compare vendors' security profiles side-by-side and prioritize them according to risk – with a higher score suggesting a stronger security posture.

In addition to receiving a numerical representation of a vendor's security profile, you also can view detailed information about the number and severity of security issues that led to that rating and need to be acted upon.

With this data in hand, you can go beyond your initial tiering and further prioritize which vendors need the most attention. You may decide, for example, that the assessment process for vendors with high security ratings may not need to be as rigorous, while the process for vendors with lower ratings could be more thorough.

BITSIGHT SECURITY RATINGS ARE GENERATED BASED ON FOUR CLASSES OF DATA

- Compromised Systems
- Diligence
- User Behavior
- Data Breaches

TIP #3

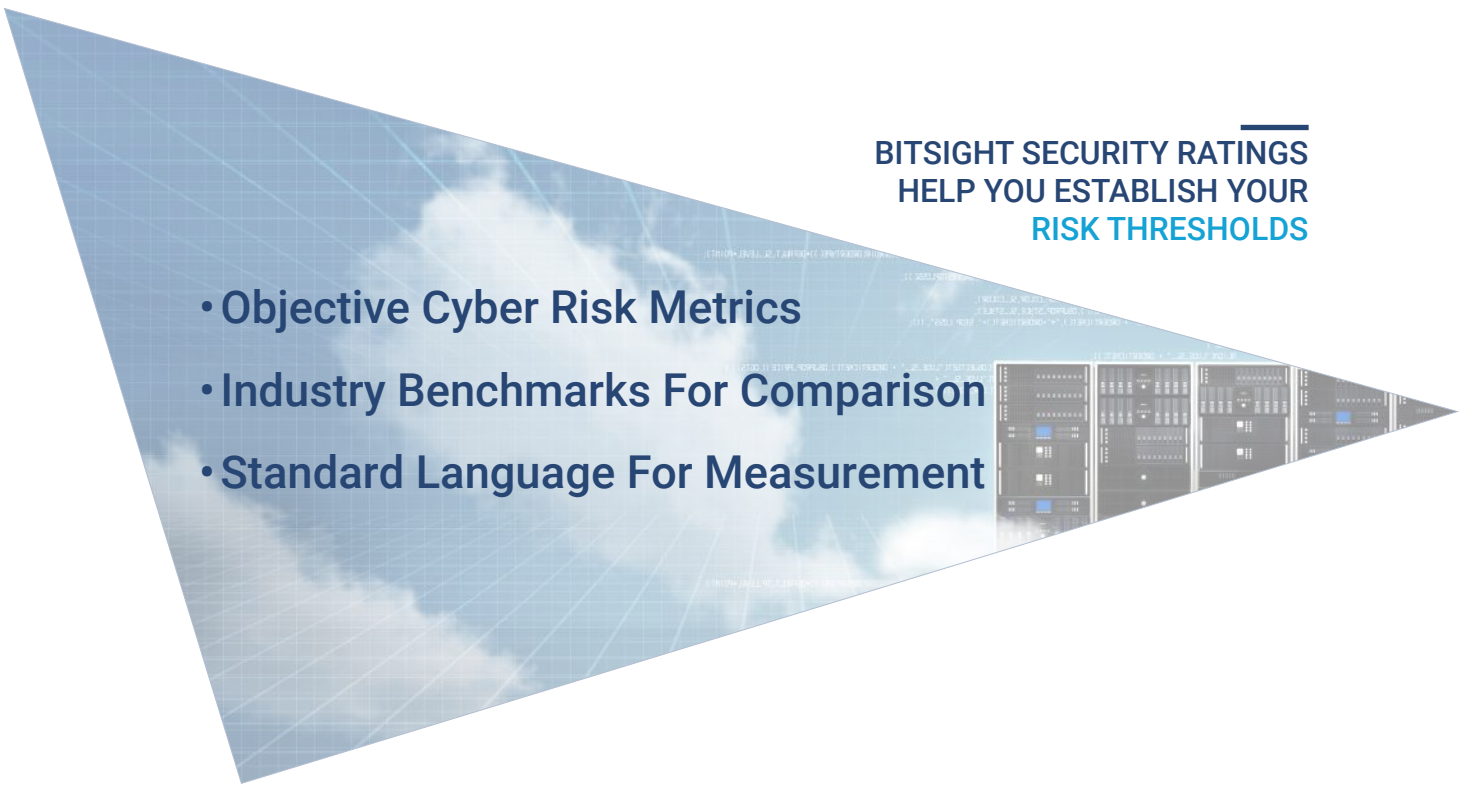
Establish Acceptable Risk Thresholds

You also can use BitSight Security Ratings to establish acceptable risk thresholds and develop language to ensure that your entire third-party network meets these thresholds.

For example, you might consult with your legal and finance teams to put extra contractual controls in place based on the rating of a particular vendor. Those with lower ratings may require more stringent controls to ensure that they meet your acceptable risk threshold.

Once you have established this threshold, continue to collaborate with legal to devise policies and enforceable contract language to ensure compliance throughout the life of your contracts.

Work with the team to develop a remediation plan in case a vendor dips below the established threshold, and then engage in ongoing monitoring to ensure that the third parties in your vendor network continue to hold up their ends of the security bargain.



TIP #4

Monitor Your Vendors Continuously

Once the contract is signed, it is critical that you keep tabs on the security postures of your vendors throughout the remainder of your partnerships. By implementing a continuous monitoring program, you can stay aware of the changing risk profiles of your vendors and make data-driven decisions about when a specific third party needs a security reassessment.

This is more efficient than maintaining spreadsheets, calendar reminders, and other manual processes, and allows you to develop a more agile and streamlined risk management program.

Unlike traditional point-in-time security snapshots, BitSight Security Ratings are updated daily, so you easily can track how your vendor's security performance is changing over time.

Setting up monitoring alert filters for different groups (e.g., critical and non-critical) can help you sort through the noise and focus on vendors that require immediate attention.

For example, you may choose to receive notifications when a critical third party's security rating experiences a drop of any kind. For vendors that are less critical, it might make more sense to create alerts for significant performance drops or for the specific risk vectors that are of the greatest concern to your organization.

These alerts empower you to make data-driven decisions about when to perform a reassessment. Instead of going through this process on a specified incremental basis, you can create rules that define when a vendor reassessment is required – helping you save time and resources. For instance, you may determine that a critical vendor that has gone below a specific BitSight Security Rating always needs to be reassessed.

Turn TPRM Into A Business Enabler, Not A Roadblock

With BitSight Security Ratings data, you can define enforceable policies and procedures that help you manage risk based on your organization's unique security thresholds and concerns. Save time, reduce costs, and scale your onboarding process with ease by leveraging an adaptive, tiered approach that takes each prospective vendor's relationship and security posture into account when determining the appropriate level of assessment.

BitSight Security Ratings
Deliver Better Data for Better Decisions
About Your Organization's Security

Learn how.
www.BitSight.com/security-ratings

BITSIGHT®
The Standard in SECURITY RATINGS

BitSight
111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable, and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to analyze vast amounts of data on security issues continuously. Seven of the top 10 largest cyber insurers, 25 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog, or follow @BitSight on Twitter.