Today, enterprises are increasingly integrating third-party vendors in an attempt to facilitate the streamlining of business processes. Nonetheless, such vendors also boost the IT environment, increasing the threats that their data security controls face. The data sharing and link between enterprises and their partners call for the creation of a strong program for vendor risk management. Nonetheless, participating in vendor risk management needs the creation of a workflow that is well-organized in a bid to respond to the risks affecting the data environment.

**Tips for Enhancing your Vendor Risk**

**Assessment Process**

**Who are the Third-Party Vendors?**

Looking at the business world today, it is irrefutable that its future resides in the cloud. In fact, Cisco’s Global Cloud Index projection showed that 59% of every cloud workflow would be provided through software-as-a-service ([SaaS](https://en.wikipedia.org/wiki/Software_as_a_service)) providers by the close of 2018.  In the meantime, the report claims that both platform-as-a-service and infrastructure-as-a-service would drop. The emergence of remote employees propelled by the cloud translates to enterprises that can minimize physical capital expenses.   The only problem is that such third-party vendors are accompanied by more risks.

**What risks do SaaS Vendors pose to your Environment?**

Based on information from Dark Reading, the costliest data breaches are caused by third-party providers.  For instance, out of the five leading expensive data breach cases, the third-party cloud services and third-party hosted infrastructure vendors account for two of the incidents.

Often, suppliers have virtually unlimited access to your data. For instance, the web apps that your workers utilize in accessing your databases require the use of your most vital information. What’s more, enterprises regularly have inadequate visibility, primarily into their cloud provider security. In case you are utilizing a vendor, keep in mind that the same vendor could be in business with a third-party provider.

**What are the Requirements for Regulatory Compliance?**

Industry standards such as the International Standards Organization (ISO) offer guidance over creating ideal practices. Nonetheless, many industries often find themselves being threatened by penalties.

* Risk management, particularly in the financial services industry is controlled by both state and federal laws.  The Federal Financial Institutions Examination Council or FFIEC IT exam handbook  calls  for    banking institutions  to:
* Evaluate potential third-party providers not only on the basis of scope but also the importance of the services they offer.
* Determine whether a given third-party relationship supports the entire strategic and objective plans of the institution.

Customize the institution’s third-party management program on the basis of an ongoing and initial risk assessment of the organization’s third parties as well as the services they offer. In the meantime, the Department of Health and Human Services ([HHS](https://en.wikipedia.org/wiki/United_States_Department_of_Health_and_Human_Services)), which is tasked with the role  of overseeing  the 1996 Health Insurance Portability and Accountability Act ([HIPAA](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act)) states that  as  a section  of the National Institute of Standards and Technology  security  risk evaluation, medical care  providers  ought  to ask:

* What is e-PHI’s external sources?  For instance, do consultants or vendors build, receive, retain or convey e-PHI?

While several organizations look for compliance certifications create customer and client trust, the financial services, and healthcare industries have to comply since noncompliance often results in penalties and fines.

**How to Start a Third-Party Risk Assessment**

Information security experts regularly help in reminding you to “trust but verify.” Nonetheless, verification is regularly difficult since you do not only work for your vendors but also lack insight into their business processes. The inadequate visibility results in most of the risks that your organization faces.

Vendor risk evaluations have a similar workflow to the risk evaluation that you utilize for your business activities.

* What vendors are important to your business operations?
* What types of information do your vendors gather, convey and store?
* What vendors have access to your servers, systems or networks?
* What level of uses access does your vendor have to such servers, networks, and systems?

**How to Participate in Proper Due Diligence**

Identifying risks serves as the initial step to carrying out due diligence for third-party risk management.  The second step is to confirm that your vendors follow the protocols that are stipulated in the documentation. In the past, vendor risk management depended on audit reports and questionnaires.

Unluckily, questionnaires require you to trust a vendor, and conventionally, audits offer point-in-time insights only. Although vendor questionnaires provide insights into the strategies that companies plan to use, the communication lines sometimes break down.

**How to Build a Security-First Vendor Management Program**

Vendor management may seem overwhelming since you have numerous vendors spread out across your ecosystem.  Nonetheless, it serves as another compliance branch. As such, when you are dealing with a [security-first compliance tool](https://reciprocitylabs.com/industries/hospitality/), then you must best ahead of other companies by far. Through real-time risk monitoring, you can evaluate the prospective threats posed by your vendors and assist them in securing their data.

**Author Bio**

Ken Lynch is an enterprise software startup veteran, who has always been fascinated about what drives workers to work and how to make work more engaging. Ken founded Reciprocity to pursue just that. He has propelled Reciprocity's success with this mission-based goal of engaging employees with the governance, risk, and compliance goals of their company in order to create more socially minded corporate citizens. Ken earned his BS in Computer Science and Electrical Engineering from MIT.