Venture Lynk
CAPITAL & ADVISORY

Experts at Vendor Risk Management Services

*Always **Trust but Verify** your vendor provided questionnaires and documents.*

Services

- **Information Security Risk Reviews**
  Determine the deficiencies of a vendors info sec policy
- **Constant Daily Cyber Risk Monitoring**
  Discover vendor vulnerabilities that could endanger your security or service delivery
- **Financial and Business Health Risk Monitoring**
  Proactively identify vendor financial risk before it's too late
- **Financial and Business Risk Evaluation**
  Evaluate existing and applicant vendors to prevent surprises later
- **Remote Access Cyber Security Service (RACCS)**
  Constantly monitor the cyber risk of remote workers

About **Us**

Our team of subject matter experts at **Venture Lynk** are here to intensify and expand the risk evaluation and identification capabilities of your vendor management team. We know that managing the risk associated with numerous existing and applicant vendors can overwhelm your team and create the possibility of inadequate risk evaluations. Our role is to go far beyond what the vendor provided questionnaire(s) and policy documents say and help you protect your company.

Today's Challenge for Vendor Managers

- Vendors answer questionnaires and provide policy documents in a way that gets them approved
- Vendor management has the obligation to ***Trust but Verify*** that information
- VM platforms do not fully evaluate vendor related risk
- Vendor management has limited time and resources to evaluate and manage risk

**"Data Risk in the Third-Party Ecosystem", Ponemon Institute, 2018.*

Why **Venture Lynk**

- Venture Lynk provides risk evaluation, identification, and remediation functions
- We are not a VM platform provider. We are a service provider
- Venture Lynk can replace or support your cyber, information security, and financial health risk analysis
- Little to no implementation cost or staff training is required
- We can immediately start work within your existing VM platform
- This means we can start directly monitoring risks constantly and daily on Day 1.

Vendor Risk **Management Services**

Information Security Risk Reviews

- Identify vulnerabilities in vendor Info Sec policies for a data breach or impact to supply chain delivery
- Remediation and policy change recommendations

Constant Daily Cyber Risk Monitoring

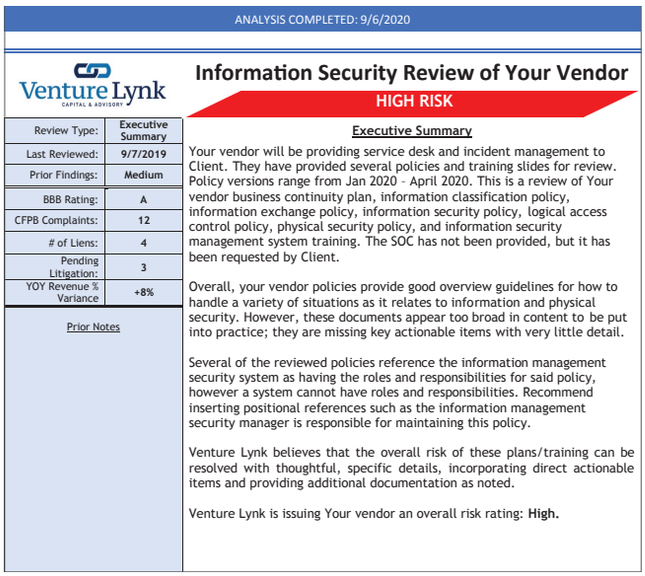
- Monitor and ping each vendor's public and remote staff IP addresses
- Use Open FAIR model to identify cyber risk exposure in financial terms
- Recommendations on how vendor to remediate and then verify cure

Financial and Business Vendor Risk Monitoring

- Daily financial, business, and market risk monitoring
- Provide scores related to client's financial stack, business model, executive team movements, payment history, public records

Financial and Business Risk Reviews

- Quarterly or semi-annual review of vendor financials
- Suggest financial, business, and market risk evaluation questions to ask vendor



ANALYSIS COMPLETED: 9/6/2020

Venture Lynk
CAPITAL & ADVISORY

Information Security Review of Your Vendor

HIGH RISK

Review Type:	Executive Summary
Last Reviewed:	9/7/2019
Prior Findings:	Medium
BBB Rating:	A
CFPB Complaints:	12
# of Liens:	4
Pending Litigation:	3
YOY Revenue % Variance	+8%

Prior Notes

Executive Summary

Your vendor will be providing service desk and incident management to Client. They have provided several policies and training slides for review. Policy versions range from Jan 2020 - April 2020. This is a review of Your vendor business continuity plan, information classification policy, information exchange policy, information security policy, logical access control policy, physical security policy, and information security management system training. The SOC has not been provided, but it has been requested by Client.

Overall, your vendor policies provide good overview guidelines for how to handle a variety of situations as it relates to information and physical security. However, these documents appear too broad in content to be put into practice; they are missing key actionable items with very little detail.

Several of the reviewed policies reference the information management security system as having the roles and responsibilities for said policy, however a system cannot have roles and responsibilities. Recommend inserting positional references such as the information management security manager is responsible for maintaining this policy.

Venture Lynk believes that the overall risk of these plans/training can be resolved with thoughtful, specific details, incorporating direct actionable items and providing additional documentation as noted.

Venture Lynk is issuing Your vendor an overall risk rating: **High.**

Remote Access Cyber Security Service (RACSS)

- **Scan Remote Users** - identify if a remote worker's machine is infected with malware, has botnet activity, or has out-of-date system patches
- **Prevent Unauthorized Entry** - detect if there any exploitable vulnerabilities on the remote workers machine and identify any repeated attempts by an adversary to gain access to your application
- **Non-Invasive and Permissible** - the application sits within your proprietary network and tracks incoming users along with the network they are using
- **Full Coverage** – monitor enterprise and vendor remote workers that access your network

Contact **Information**

P: (213) 421-3050
E: admin@venturelynkfinancial.com
www.venturelynkfinancial.com