VENDOR & THIRD PARTY RISK MANAGEMENT

VRM Program Development and Outsourced Services

LYNX TECHNOLOGY PARTNERS

IT RISK, COMPLIANCE, & CYBERSECURITY EXPERTS

PROGRAM DEVELOPMENT

- Benchmarking & Maturity
- Risk Identification/Classification – Inherent Risk
- Vendor Assessments
- Workflow Design & Implementation
- Policy & Procedure Development

OUTSOURCED SERVICES

- Complete VRM Life-cycle Services
- Remediation Management

WE SOLVE PROBLEMS.

63% A recent survey by Soha Systems places the percentage of all data breaches linked directly or indirectly to third-party access at 63 percent.

CONTACT US

309 Smithfield St. 3rd Floor
Pittsburgh, PA 15222
New York | Washington D.C. | San Francisco

+1 (800) 314-0455

Sales@LynxTP.com
www.LynxRiskSolutions.com

Vendor and Third Party Risk Management is more than simply checking the compliance boxes. It is a combination of truly analyzing the inherent risks organizations pose to your environment as well as continuously monitoring those organizations.

OUR PHILOSOPHY

Strong cybersecurity monitoring solutions and compliance programs are based on sound risk management strategies and visibility. Lynx Technology Partners' Vendor and IT Risk Management Services, as well as our Compliance Solutions, provide holistic capabilities that combine security and risk professional services with the ability to perform thorough third party and IT risk assessments. These services and solutions also enable the ability for us to facilitate remediation efforts to assist organizations in combating their compliance challenges.

THE CHALLENGE

With third parties being the leading documented pathway for data breaches, the return on investment from developing and implementing robust VRM programs has become clearer. Repercussions include reputational consequences, legal costs and regulatory fines, customer notification costs, as well as high profile Board and C-level accountability. Due to these possible repercussions it is very important for companies to ensure they are taking into account and assessing the potential inherent and residual risk associated with the utilization of third parties. Therefore, it is becoming more and more important for companies to develop and maintain a robust VRM program.

THE SOLUTION

The Lynx Vendor Risk Management Consulting Team (VRMCT) works with organizations to assist them in the creation and implementation of a holistic Vendor/Third Party Risk Management (VRM) program and/or to improve a customer's existing program and practices. The main objectives that the VRMCT strives to meet are:

- Determine the maturity of a company's program as well as assistat in establishing a benchmark baseline for the company's vendor risk management program.
- Identify areas for program and process improvement.
- Provide an action plan for the organization.
- Create policies, processes, and procedure documentation that supports the move to a more robust program customized to align with the organization's compliance needs and risk posture.

> "No organization is an island, entire of itself; every organization is a piece of the continent, a part of the main."
> - John Donne

VENDOR & THIRD PARTY RISK MANAGEMENT

VRM Program Development and Outsourced Services

LYNX TECHNOLOGY PARTNERS

IT RISK, COMPLIANCE, & CYBERSECURITY EXPERTS

SUPPLY-CHAIN RISKS

- Third-party service providers
- Poor information security practices by lower-tier suppliers
- Compromised software or hardware purchased from suppliers
- Software security vulnerabilities in supply chain management
- Software security vulnerabilities in supplier systems
- Counterfeit hardware or hardware with embedded malware
- Third-party data storage or data aggregators
- Unauthorized sharing of data by third-party providers
- Overreliance on non-specific, "boiler plate" contracts
- Failure to have a cyber-focused insurance policy

Lynx Technology Partners is a Member of The Shared Assessments Program. The Shared Assessments Program is the trusted source in third-party risk assurance.

SCHEDULE YOUR CONSULTATION

InsideSales@LynxTP.com
www.LynxRiskSolutions.com

THE METHODOLOGY

The Lynx team utilizes a proven methodology in association with an extensive array of industry subject matter experts to assess the areas of opportunity that exist within an organization's VRM program. Once we have identified the areas of opportunity, an action plan will be provided that specifies deltas in the areas identified, and the Lynx VRMCT can assist the organization in the creation and/or refinement as well as the implementation of a completely customized VRM program that is aligned with the organization's specific compliance needs and risk posture.

The Lynx VRMCT has expertise in the utilization of The Shared Assessments Program Vendor Risk Management Maturity Model (VRMMM) to perform the internal Vendor/Third Party Risk Management (VRM) program assessment.

The VRMMM is a holistic tool for evaluating maturity of third party risk programs including cybersecurity, IT, privacy, data security and business resiliency controls. The VRMMM examines all areas of program governance and identifies elements critical to a successful and mature TPRM program. The VRMMM's focused content allows organizations to:

- Evaluate their own program against a comprehensive set of best practices.
- Identify specific areas for improvement to guide well-informed decisions that drive efficient resource allocation and use and help manage vendor-related risks effectively.

High-level categories are broken down into components in a manner that makes the model adaptable across a wide spectrum of industry groups.

VRM METHODOLOGY

1. PRESCREEN

Understand and assess the inherent operational and jurisdictional risk to the organization prior to performing due diligence.

2. SCAN

Determine the processes and methodology to be used for the execution of vendor assessments.

3. ASSESS

Best in-class Screening process that provides a comprehensive view into complete enterprise risk – financial, regulatory, reputational, and governance.

4. MITIGATE

Dictates mitigation activities that must be taken by both the third party and you.

5. MONITOR

Periodic re-screening process that identifies change in enterprise risk, ensures information is kept current, and continue compliance to client policies.