LTIMindtree

Point of View

Third Party Risk Management: **Service Providers**

Why Third Party Engagement?

In a rapidly changing business environment, every organization intends to increase its focus on its core business and engages third party services for all other support activities. The business drivers behind engaging third parties include business process outsourcing, cost optimization, hiring specialized expertise, exploring new ideas and increasing footprints of the business in new territories. The third party services cover wide number of areas like technology development and implementation, hosting of infrastructure, providing cloud services, providing manpower and logistical support, conducting operational activities and high end consulting or niche consulting requirements. The third parties operate from multiple countries, use different technological platforms, use diverse types of skill sets. Their services, products, and networks are closely interlinked with the operational processes of the organization. Today, the third parties can be considered as an extended organization.

Awareness & alertness is the key

Engaging third party services keep organizations dynamic and vibrant. At the same time, such an arrangement also brings in new risks that could be strategic, financial, operationaland legal in nature and can also impact compliance. The key to manage these risks lies in the ability to detect these at an early stage and control their impact.

Risks arising due to any activity or non-activity of third parties service providers are normally dormant, and often considered as "outside the organizational control". These risks however

directly impact the organization's operations, profitability, reputation and in extreme cases can lead to cyber-attacks, data breach and penalties.

Every organization today needs a strong Third Party Risk Management (TPRM) program that identifies, tracks and mitigates such risks throughout the life cycle of the engagement. Such program unearths hidden risks in a timely manner for mitigation. A good TPRM gives 360 degree, as well as granular view of all risks, thus helping organizations to take necessary actions in timely manner

Early detection, early action

Given the complex nature of third party risks and their potential impact on the organization, the key success factor of the program is to detect any risk at early stages.

All third party assessments should be conducted:

- **Prior to on-boarding process that identifies critical risks**
- **As a part of on-going assessments that identify risks having material impact**
- **When critical changes take place**
- **Post incidence – when an incident is detected and is a triggered-based monitoring**

An effective risk detection program should have an intelligent mechanism that keeps track of emerging threats in the global market.

Current programs and their limitations

Current Third Party Risk Management programs of most organizations have limited coverage in terms of the number of vendors and frequency of conducting audits Organizations also have limited visibility about the changes that take place at the vendors end, new threat vectors, changed compliance requirements, and the impact of these on the vendor-organization relationship. Also, the vendor's assessment cycle time is typically quite high, and history of prior assessment is not linked. Organizations strive hard to compare vendor performance, or benchmark them against industry standards. Third parties have begun to occupy more space in the organization as operations, monitoring, mitigation and controlling risks becomes tedious and difficult. Organizations also lack a collaborative platform that allows vendors and assessors to interact with each other in a regular and transparent manner.

Organizations need a single repository of all vendors, question banks, prior and scheduled assessments, evidences with trails. They need to conduct risks assessments in a user-friendly, efficient manner and churn out all the data available to have a complete view of third party security posture. Organizations would need to integrate any third party risk management platform with their existing technical environment to increase productivity of assessments.

Stakeholders have their own perspectives for Third Party Risk Management programs.

Affordable yet highly effective

In most organizations today, the costs associated with third party risks remain an unknown factor. Tracking such risk manually on a continuous basis for all vendors is a costly proposition. Success of any organization greatly depends on the ability of the third parties to render services in a timely, effective and secure manner. Sometimes, third party systems become launchpads for malicious attacks on the organizational infrastructure. Such incidences create significant disruption to the day-to-day functioning of the organization, and in extreme cases, lead to data breaches – the consequences of which could be far-reaching. Therefore, the top management is interested in Third Party Risk Management program that is cost-effective and can prevent potential impact of any security vulnerability.

TPRM also helps to filter out vendors that pose risks to the organization and prioritizes vendors whose ratings are consistently on high. This helps organization to build reliable network of vendors and gives a competitive advantage.

Drilling down to provide granular views

A good TPRM program needs to be comprehensive, should cover activities and risks of all vendors on a continuous basis, be based on international standards and frameworks and keep the organization secure. The TPRM should also reduce subjectivity during assessments and allow rating systems that can be used for comparative and trend analysis using various parameters. TPRM models should help organizations quantify risks and track them at granular levels. The quantification should include weightages to the questions and rating the quality of the response. This gives complete visibility of risks to the organization with a drill down capability and pin point the areas that need attention.

Act as a central repository

TPRM programs also need to be collaborative by maintaining history of all communication and prior assessments, in order to be useful and effective. Such risk assessment data should be accessible to all concerned parties with appropriate security controls. This builds a good transparency in the system. The platform should be able to build repositories such as question banks, vendor profiling, vendor interactions, vendor risk mitigation plans and actions taken, vendor compliance status, etc. A good TPRM program should address common concerns of all the stakeholders including the third party.

Adhere to multiple compliance rules

An SIG (Standardized Information Gathering) questionnaire is a repository of third party information security and privacy questions that refers to multiple regulations and control frameworks. TPRM programs should leverage SIG as well as all control frameworks such as ISO, CMMI, PCI DSS, SOX and apply the same to the context of the business and the purpose of the audit objective.

Conclusion

Today, organizations tend to be highly dependent on third party service providers, and any deficiency in services can make them vulnerable to various risks. Service providers need to visualize, monitor and control these risks and their potential impact on the organization. Third Party risk is very much an organizational concern, not just a third party concern. While TRPM solutions help organizations protect themselves from risks, services need to be comprehensive, scalable, flexible and ensure compliance monitoring, in order to be truly valuable and effective.

Madhav Kulkarni

Sr Project Manager, LTIMindtree

Madhav is an IT industry professional with more than 30 years of overall experience in diverse number of industries and platforms and specializes in the area of IT Risks and Controls. He is a platinum member of ISACA, member of (ISC)2, with several other Credentials and certifications and is a speaker at industry forums & platforms. IT control automation, continuous monitoring, service continuity plans are the areas of his great interest.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit **https://www.ltimindtree.com/.**