ASA

Risk Consultants

Research Note

Managing Third Party Risks

By Divya Yadav

Applicable Sectors: Information Technology, Banking and Finance, Public Healthcare

Keywords: Vendor Management, Third Party Risk, Compliance and Governance

Abstract: Third Party contracts have become the norm in today's competitive business environment which essentially means handling of an organization's business processes by an external service provider. This form of operational arrangement can sometimes result in loss of accountability and ownership, non-compliance to regulations, and data breaches that can cause financial and reputational risks. This research note highlights some key points that can help organizations manage their third party vendors and contractors and mitigate potential risks.

Introduction

Third Party vendors and contractors exist across all vertical markets, be it manufacturing, finance, retail, IT or healthcare. The term Third Party essentially means that organizations hand over some of their operational functions or products and services to an external party. A term that became synonymous with third party vendors a decade ago was "outsourcing," where companies contract their functions or line of business to third parties that can otherwise be performed in house[1]. Third party contracts and Vendor Management is a complex issue that needs to be dealt with care as organizations are not only trusting external parties with their sensitive data but are also relying on them to deliver on time, hence making it a complex equation of fulfillment of each criteria. Growing competition has compelled companies to give control of their core processes to external providers, which has potential risks and therefore a need for risk framework that protects proprietary data and intellectual property cannot be emphasized enough. An important question that arises is how do organizations go about selecting contractors and what strategy do they have in place to hire contractors on which they can rely completely to effectively perform their tasks and protect the company data. The aim of this research note is to learn more about the potential risks across industry verticals, and how these risks can be mitigated.

Risks arising from Third Party Contracts

Much has been read and written about Edward Snowden who was a SharePoint contractor for NSA and how he managed to leak sensitive information that caused much of embarrassment to the US government and other countries as well. What caused the information to travel from NSA premises to media outlets may very well have been the lack of contractual compliance, ineffective third party governance and security policies. Another very different form of third party risk is the healthare.gov website. Much of the development for the site was led by contractors that were in compliance with federal norms and regulations but still were not able to deliver for the government on time. Here the reasons are slightly different: ineffective vendor management or lack of co-ordination between government and vendors. In another instance, Boeing outsourced much of its manufacturing of components as well as the some of the design to outside contractors that made it look susceptible to financial risks[2]. Why? Outsourcing design to contractors with weak business implementation and requirement plans can cause a gap between what actually needs to be done. Such contractors don't have the vision or big picture in mind, and it is the job of the business owner to know about the end to end process. Similarly, managing contractors for construction and infrastructure management is a huge challenge and requires maximum scrutiny in order to avoid any substandard materials and procedures being used to build roads, bridges and buildings. These examples from different verticals point out that third party risks are prevalent in each sector and they differ from one another depending on the line of service outsourced.

Perhaps the most popular is IT outsourcing and almost every vertical market engages in this form of contractual arrangement. Companies are more than ever facing scrutiny to be able to protect customer data and sensitive information and create norms and regulations for third party vendors to handle this information discretely. Data security breaches have taken place in the past that comprises not only financial risk but reputational risk as well. Cloud computing and software as a services are examples of emerging risk areas that are privy to sensitive information and require strong regulatory environments[3].

Coordinating with vendors is a huge task and needs effective vendor project management. While contracting to vendors seems lucrative for driving decreased costs and increased revenues, an inherent understanding of what a complex ecosystem a company is venturing into should be apparent[4]. A strategy complete with risk and gap analysis as well as integration plan should be in place to begin with or else the project can be a huge failure.

Third Party Risk Management and Compliance

The landscape for risk and compliance continues to evolve[5] and not all risks are equal, a fact that a flexible framework should be able to take into account. Companies have contracts with multiple contractors and vendors, and to manage this comprehensive list should be the first step toward building a sustainable framework. Process mapping and accountability of work for each contractor can be managed and keeps the company aware of what's going on at each stage. Secondly, identification of core processes that are outsourced and whether the data or information can be comprised, as well as what impact it will have on the organization, is a useful matrix. If created, such a matrix can help in the monitoring and evaluation of risks that have the highest impact.

Prioritization of processes and risks is important as not all risks are equal and this will impact their handling and treatment. Cloud providers, helpdesk processes, outsourced financial processes, and medical claims processes are examples of critical processes that organizations outsource. Assigning risk ratings to these processes can make the audit and risk management process more streamlined. A dedicated team to handle and manage third party should be in place as well as identification of Key Risk Indicators also assist in managing risk. Internal controls are created as part of risk management framework for each process that should be accounted in Services Organizations Reports (SOC) as part of the audit and assurance practice[6].

Vendor Management

Vendor Management is a cross functional process schema that integrates IT, Compliance, Risk assurance and business owners to manage the risk portfolios of vendors[7]. It brings together all the individual business units and helps manage their third party processes to mitigate gaps and unify process framework. The heart of vendor management is managing and retaining ownership from a key or senior leader of the organization. The leader will oversee regulations, internal controls and standards to ensure that they are being followed, and to institute penalties for violations from the vendors.

Vendor training and assessment should be a part of vendor management and these trainings should be organized on annual or bi-annual basis depending on the need or criticality of the processes. Dedicated curriculum designers should hired to make the content relevant and effective.

Hiring Right Contractors

Hiring third party contractors and vendors is unavoidable due to the increased revenues, decreased cost of production and competitive advantage that make it so compelling. Companies must understand that hiring the right contractors that get the work done and pose minimum risks is the most optimum strategy. Besides the risk, governance and compliance that comes into effect when contracting work to third parties a key point to note is that a failure to align with business requirements can compromise the line of business being contracted and will result in a failed product or service. A detailed and comprehensive business plan that covers the scale of the project and business requirements should be prepared. An evaluation team that has a vested interest in selecting vendors should be formed as it ensures strong participation and less margin for errors. Define vendor requirements clearly and search for vendors that fulfill these requirement criteria. Evaluate proposals from vendors based on an already formed list of business requirements along with priority and importance for each requirement. This methodology will help assign scores to each vendors and display how their proposal aligns with the company's needs and requirements[8].

Conclusion

While third party contracts are here to stay if effective strategies, frameworks, trainings and process plans are in place companies get reap in more benefits rather than fighting it. Risk monitoring and assessment is the key in managing vendors and contractors. Identifying processes and hiring contractors based on the requirements is a complex process and specialized people should be assigned to effectively manage third party contactors. Companies should build guidelines and strategies to not only manage contractors, but to be constantly aware of the potential risks that might ensue and to mitigate them adequately.

References

[i] "Abusive Practices — Third Party Procedures". Retrieved 10 November 2013 http://www.fdic.gov/regulations/compliance/manual/pdf/VII-5.1.pdf

[2] Denise Harrison. "Lessons Learned from Boeing's Stumble: Risk Assessment is Key to a Successful Strategy". Retrieved 10 November 2013. http://www.cssp.com/CD1209a/StrategicRiskAssessment/

[3] Grant Thornton. "Keeping third party risks in check". Retrieved 10 November 2013. http://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/BAS-GRC-CG-WP_Keeping-Third-Party-at-Risk_FINAL.ashx

[4] "Third Party Risk and Vendor Management". Retrieved 10 November 2013. http://www.astea.com/en/solution-capabilities/solution-capabilities/third-party-and-vendor-management/page.aspx

[5] Dmitry Krivin, Hamid Samandari, John Walsh, Emily Yueh. Mckinsey and Company. "Managing third-party risk in a changing regulatory environment". May 2013. Retrieved 10 November 2013.

[6] http://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/BAS-GRC-CG-WP_Keeping-Third-Party-at-Risk_FINAL.ashx

[7] David Katz Nelson Mullins Riley & Scarborough. "Contracting in a World of Data Breaches and Insecurity: Managing Third-Party Vendor Engagements". LLPhttp://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2013/05/02/contracting-in-a-world-of-data-breaches-and-insecurity-managing-third-party-

vendor-engagements.aspx

[8] James Bucki. “The Successful Vendor Selection Process”. Retrieved 10 November 2013 http://operationstech.about.com/od/vendorselection/a/VendorSelectionHub.htm