Third-Party Management Program Implementation Tips

Planning

- Ensure you know the regulatory requirements that impact your organization. Don't just copy another organizations program.
- Understand the organization's third-party relationships and determine which third parties should be considered "in scope" and therefore subject to risk-based due diligence.
- Define your current state. Conduct a process inventory to identify what vendor risk processes are ad-hoc or formalized. Review your strategic plans for growth and anticipate what your future needs may be.
- Develop a plan to manage the relationships based on a risk profile prior to engaging a vendor. Start with your baseline to address core risk, identify process maturity improvements, and gradually add the governance maturity you need for measurements and compliance.
- Don't treat all your vendors the same way. Establish risk-based criteria to focus your efforts and understand which regulations apply to which vendors and adjust your program accordingly.
- Define your governance model. Start with a scalable framework, based on your starting point in process maturity. Understand the level of formality you need to address management and board reporting. Don't forget to define exception processes and approvers of risk
- Obtain support from your top leadership who should make clear to everyone in the organization that all partnerships with third parties must be subject to risk-based due diligence to mitigate potential risks.
- Implement broad organization program awareness to socialize goals and requirements.
- Develop "checklists" to guide relationship owners as well as vendor management teams throughout the management lifecycle. These should include all the steps required to establish a new relationship, renew a relationship, or terminate a relationship. Ensure these checklists are communicated to the parties who will be responsible for executing each of the steps and to others involved in the process for awareness.

Initial Due Diligence

- Conduct due diligence before entering into a new business relationship with a third party.
- Partner with business owners early to help alleviate risks during vendor selection (i.e., RFP processes). Don't put the Vendor Risk Management program in the position of only saying "yes or no" – especially late in the process as the business owners are moving to contract signing.
- Prior to engaging a vendor, develop a contingency plan to ensure that your organization can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to your organization's or third party's business strategy.
- When performing Due Diligence, ask questions that pertain to your relationship and will provide a reasonable understanding of your partner's capability to mitigate risks to your firm. Don't ask standardized questions that don't pertain to the relationship or provide any actionable intelligence for your assessment and decision-making processes.
- Coordination with other internal due diligence partners (i.e., Information Security, Finance, Internal Audit, Risk Management, Sourcing)
- Develop a standardized, repeatable, but adaptable, assessment to ensure various risk categories are being evaluated in a consistent basis over time (i.e., performance risk, business involvement, information protection)
- Consider centralized communication with vendors (communication through one source)

Contract Negotiation

- Develop a contract that clearly defines expectations and responsibilities of the third party to help ensure the contract's enforceability, limit the firm's liability, and mitigate disputes about performance.
- Ensure you clearly define expectations with your vendors about how your sensitive (customer, associate, potential client, business, etc.) information is protected and that your vendor understands its obligations.

Ongoing Due Diligence

- Conduct ongoing due diligence on a regular basis to validate the suitability of the relationship as well as the current risk level.
- Monitor service providers via audits, test results, etc. to confirm that they have satisfied their obligations.

Oversight & Accountability

- Assign clear roles and responsibilities for managing third-party relationships and integrating your third-party risk management process with your enterprise risk management framework to enable continuous oversight and accountability.
- Consider establishing a RACI (Responsible, Accountable, Consulted, and Informed) matrix to clearly delineate responsibilities across the vendor management lifecycle.
- Establish an oversight committee made up of senior management of your organization to monitor the third-party risk management process, periodically review its suitability, adequacy and effectiveness, and implement improvements where needed. Risks as well as requirements may change the type of vendor oversight that is required.

Documentation and Reporting

- Ensure you have proper documentation and reporting to facilitate oversight, accountability, monitoring, and risk management associated with third-party relationships.
- Your organization should be able to explain and document the rationale for all decisions related to outsourcing.
- Consider centralization of document retention.
- Consider implementing a vendor / contract management tool to assist with program management.

Independent Review

- Conduct periodic independent reviews of the risk management process to assess whether the process aligns with your organization's strategy and effectively manages risk posed by third-party relationships.

General Tips:

- Apply tips to "more critical" vendors v. "all vendors"
- Don't be afraid to put in place a program that is "good enough" for now and can improve in the future....