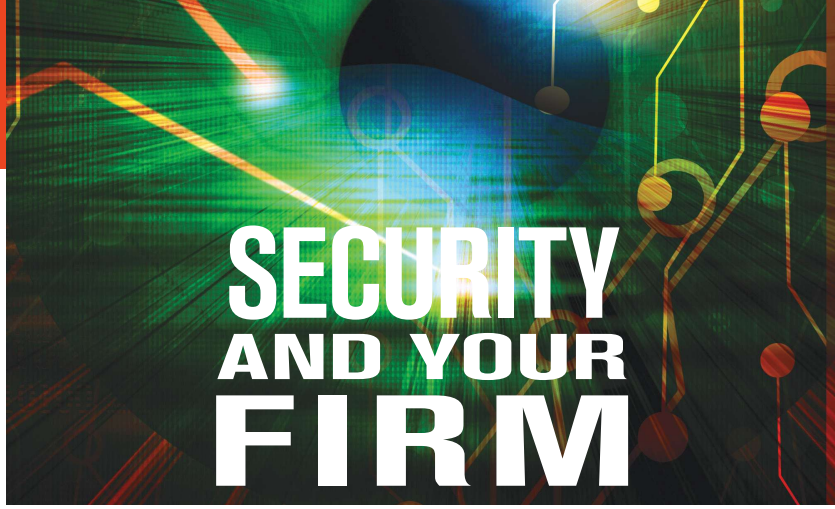

4 Tips for Managing Outsourcing Risks

By Benjamin A. Sady, CIA, CISA, CRISC

There are numerous benefits to outsourcing business processes and technology resources. You can shift some of the responsibility to another party, gain specialized knowledge and solutions, gain operational and financial efficiencies, increase the ability for management to focus on core business functions, accelerate the delivery of products or services, increase the ability to acquire and support current technology and avoid obsolescence and possibly reduce costs and conserve capital for other business ventures.

That being said, the perceived and real risk of outsourcing also seems to be increasing daily. News media and published reports frequently highlight cases of data breaches through rogue employees, hackers and lost/stolen devices. Additionally, there is a risk of receiving poor services from a vendor which can result in operational inefficiencies, lower quality of products and decreasing customer satisfaction.

Companies should be managing their outsourced vendor relationships to ensure their processes, data and systems are protected. The employees tasked with vendor management and managing these risks should consider implementing the following processes:

- Requirements Definition
- Vendor Selection and Due Diligence
- Contract Negotiation and Implementation
- Ongoing Monitoring

Requirements Definition

Before the decision is made to use a third party to outsource a process or technology, a company should identify the concerns and pitfalls associated with outsourcing and the risks associated with each perspective vendor. This process should include the appropriate stakeholders (e.g. process owners, IT, legal, internal audit) and can be used as the starting point to create risk-based written requirements. Documented requirements for each outsourced process are important to guide and manage the process from vendor selection through monitoring.

Vendor Selection and Due Diligence

A well defined vendor selection process will include evaluating proposals against the requirements definitions, performing vendor due diligence, obtaining the necessary approvals and retention of contracts in a central filing system or contract database. Involving the appropriate stakeholders in the vendor selection process is essential and provides the different perspectives needed to make sound decisions. The scope and effort of the vendor selection procedures should be consistent with the riskiness of the outsourced process.

As for due diligence efforts, this should be risk-based and done prior to entering into a contract. For low risk vendors, it may involve phone inquiries and reviewing company websites. For high risk vendors, it may involve site visits, reviewing financials, reviewing policies and procedures, reviewing internal controls and reviewing third party assessments.

Contract Negotiation and Implementation

The vendor management policy should identify who has the authority to execute contracts. Engage legal counsel to review the contract. You do not want to enter a contract that legal counsel disapproves, so use counsel in contract negotiation to filter out the unfavorable terms. The contract should clearly define the rights and responsibilities of both parties and contain adequate and measurable service level agreements. A few service level agreements to consider, include: timeliness of report delivery, timeliness of transaction processing, percentage of errors in processing, instances of IT security issues and non-compliance, and system uptime.

Most people think that service level agreements are meant only as a protective measure. They are protective, but the measurements can also be used to help identify chronic issues by all parties involved. Look for areas of consistent non-compliance or non-performance and ask your vendor, "Why is that occurring? Does there need to be a personnel, process, or technology change to improve?"

Ongoing Monitoring

The vendor management policy should identify an annual risk assessment approach that can be followed to identify high, medium and low risk vendors. To begin the monitoring process, you first need to identify your population of vendors and then perform your risk assessment for vendors according to your policy and methodology.

Be careful to avoid the trap of focusing only on traditional IT companies. The topic is bigger than just IT outsourcing. Companies often provide physical access, logical access and share sensitive information with not IT companies. Think about a bank that outsources direct marketing. They are not outsourcing to a traditional IT company, but they are most likely sharing their customers' names, mailing and email addresses, and account numbers. Look out for these types of companies in your population of vendors.

If vendors have access to the businesses data, then the ongoing monitoring program should include a plan on how to obtain assurance on the vendor's control environment. There are three primary methods to obtain assurance and any combination of them may be used. The first is to require vendors to perform self assessments annually. The business should provide standardized questions to be completed by the vendor. The questions should include a mix of yes/no and open ended questions. Consider requiring evidence to support the questions.

The second is for the business to conduct an assessment annually. Always seek to obtain a "right to audit" clause in the contracts, even if the business does not initially plan to perform an audit. There may be a day when it is needed. The assessment may include interviews of vendor staff, observations of controls, systems, tools, controls and configurations.

The third is to review third party assessments (e.g. SOC 1 / SSAE 16 reports, SOC 2 / 3 reports, PCI compliance, ISO certificate, Agreed Upon Procedures reports). When reviewing reports, there are a few key items to make sure of:

- The report covers the appropriate timeframe.
- The report covers significant services that you use.
- There are no significant control weaknesses identified in the report.
- Management should sign off that they have performed this review. A simple cover sheet, checklist and signature should do.

There is certainly a lot to consider in the outsourcing process. The most important thing to keep in mind is that a business can outsource the process and technology, but not the responsibility.

Benjamin A. Sady, CIA, CISA, CRISC, is the senior manager of Risk Advisory Services at Keiter, one of the largest accounting and business consulting firms in Virginia.