June 15, 2016

What Do You Know About Your Outsourced Service Providers?

A tiered approach for assessing risks

By Ronald Kral, CPA, CMA, CGMA
Managing Partner of Candela Solutions LLC

When directors and C-suite executives are asked what scares them the most, a frequent answer is a lack of awareness on what risks can destroy their company. These 'unknown-unknowns' are risks that are not on a company's radar screen, yet exist with potentially devastating consequences. There are also the 'known-unknowns,' such as the realization that fraud or material errors may be lurking, but still not detected. Yes, companies have controls to mitigate these risks; however, absolute assurance is elusive since there are no guarantees that objectives will be reached. Since cybersecurity and reputational risks have recently dominated many boardrooms and executive meetings, adequate attention is warranted on outsourced service providers (OSPs) to turn 'unknowns' into 'knowns.'

Utilizing OSPs has proliferated as more companies are choosing to focus on their core competencies, thus relying upon vendors to perform a wide range of services from payroll processing to cloud enabled hosting and applications. While cost-saving opportunities are realized, organizations must consider a host of new risks pertaining to cybersecurity, competency, ethical behaviors, accountabilities, and communications. A dependency on key vendors significantly changes an organization's risk profile, and therefore the necessary control response. This article explores a risk-based approach for selecting and managing vendor relationships. Specifically, a tiered approach in assessing OSP risks is forwarded. However, first an understanding of responsibilities pertaining to Service Organization Control (SOC) reports is warranted since this is a common means to gauge risks of OSPs.

Leveraging Service Organization Control Reports

Companies often find comfort in obtaining a SOC report of the American Institute of Certified Public Accountants (AICPA) from the service organization's auditors (i.e., SOC 1, SOC 2, or SOC 3 reports). Each type of SOC report is designed to meet specific user needs and companies should confirm their understanding and needs of the various types. User entities can access this information at the AICPA's website. However, these reports cannot be completely effective by simply collecting them without paying adequate attention to user entity responsibilities.

While SOC reports are useful in gaining comfort, companies must also understand their limitations and residual risk exposures. These reports should be thoroughly read to confirm that they adequately cover the contractual scope of the user organization's objectives, as well as the identification of risks and control exceptions that may need additional attention. Some questions for the user organization to consider regarding SOC 1, type 2, reports include:

1. Are all relevant objectives, processes, and sub-processes included in the applicable report?
2. Is the design of controls and applicable testing procedures at the right depth for us?
3. If an outsourced area is not covered, what risk exposures remain and how should we address them?
4. Do any subservice organizations perform control activities for the OSP? If yes, are they included or carved-out?
5. What design or testing exceptions are identified and what is the impact to us?
6. Is the corrective action pertaining to applicable deficiencies appropriate?
7. Should we follow-up directly with the OSP on concerns or questions raised from the report?
8. Do we have controls consistent with suggested complementary user entity controls (CUECs)?
9. Have we evaluated the design and operation of our CUECs?
10. Is the SOC report signed by a licensed certified public accountant (CPA) or CPA firm? Keep in mind that only CPAs can sign reports of the AICPA.

Consider all Key Vendors

Companies often pay more attention to outsourced business controls pertaining to financial reporting, such as: technology, payroll, cash management, investments, equity compensation, and other business processes. This is often fueled to strengthen evidence for external financial reporting purposes and the audit process. As a result, inherent risks associated with traditional vendor relationships, including: legal services, consulting arrangements, agents, strategic partners, creditors, and suppliers often do not receive adequate attention. For example, how do you know that your outside legal counsel has strong controls to protect the sensitive information provided to them?

A SOC 2 or SOC 3 report can be helpful in addressing operational controls for services where security, availability, processing integrity, confidentiality, or privacy is a concern. Vendors utilizing enterprise cloud e-mail, cloud collaborative solutions, and software-as-a-service (SaaS) housing third-party data are especially ripe candidates for these reports. It is important to gain comfort that effective security and confidentiality controls are in place to protect information, and these reports provide such assurance. Still, just as with SOC 1 reports, complete reliance on these reports can be dangerous.

A Tiered Approach for Assessing OSP Risks

A simple tiered approach in assessing OSP risks is a useful tool in managing vendors. Categorizing OSPs into three tiers per the criteria in the following table enhances the ability to craft appropriate control responses to effectively and efficiently mitigate risks to best reach objectives:

Three Tiers in Assessing Vendor Risks

	Tier-1	Tier-2	Tier-3
Risk Level	**High**	**Moderate**	**Low**
Description *External Financial Reporting*	Material to financial statements and/or tied to a key control	Not material, but still significant risk exposure	Routine and not significant or material
Description *Operating & Compliance Objectives*	Critical to achieving operating, compliance, and non external financial reporting objectives	Significant to achieving operating, compliance, and non external financial reporting objectives	Not significant to achieving operating, compliance and non external financial reporting objectives

Once vendors are categorized on the risks of their services to the user organization's objectives, a cascading set of procedures and process activities can be applied. For example, a company may want to consider the following objectives and activities for Tier-1 vendors:

- Understand the governance structure, reporting lines, and communication channels of the OSP
- Identify key risks in utilizing the OSP and benchmark to competitors, especially utilization of subservice contractors including fourth party networks
- Gain comfort with the OSP's ethics, including officers and directors:
  - Consider interviews, background checks, and/or internet search engine queries
  - Obtain and review copies of their code of ethics, conflict of interest, fraud hotline policy, and other policies for preventing and detecting criminal conduct
  - Confirm how ethical values are reinforced, including discipline
- Set delivery expectations with the OSP and confirm how they plan to meet them
- Understand how the OSP assess risks relating to the scope of work under contract
- Gain comfort with the OSP's ability to protect confidential information and prevent cybersecurity attacks from being launched internally or externally
- Formalize communication channels and build strong two-way communications
- Negotiate a strong contract, including adequate insurance coverage and the right to send in internal auditors
- Obtain comfort with the competency of the OSP team assigned to your contract
- Consider extending your fraud hotline to the full OSP team
- Request SOC 1, type-2, report for external financial reporting objectives
- Request SOC 2, type-2, report for addressing operational controls for services where security, availability, processing integrity, confidentiality, or privacy is a concern
- Formalize a performance evaluation process and seek continuous improvements
- Define recourses in the event adequate OSP performance is not met

Many of these activities should ideally occur prior to signing a vendor contract. While the list of suggested activities for Tier-1 vendors is not meant to be exhaustive, it hopefully provides considerations in customizing a response to manage vendors associated with a company's most important objectives. Tier-2 and Tier-3 activities should then be reduced in scope to best match the proportional risks to the user organization. Controls cost money and it is important to keep the costs and benefits in mind.

*****

Ron Kral is the Managing Partner of Candela Solutions LLC, a public accounting firm with a national focus on governance, SEC compliance, and internal auditing. He is an educator, advisor, and internal auditor for boards and management teams. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. He can be reached at rkral@CandelaSolutions.com, or you can connect with him at www.linkedin.com/in/ronkral.

Candela Solutions LLC is a strategic CPA firm in providing services to US public companies that external auditors cannot due to independence concerns. Visit our website at www.CandelaSolutions.com

This is an article reprint from the Governance Issues™ Newsletter, Volume 2016, Number 3, published on June 15, 2016