Grant Thornton
An instinct for growth™

CorporateGovernor

Providing vision and advice for management, boards of directors and audit committees Summer 2013

Finding your place on the continuum: Mitigating third-party risk through ongoing monitoring

Kirt Seale, Principal and National Special Attestation Reports Leader

Most businesses today couldn't operate effectively without some reliance on third-party service organizations. But along with the benefits of outsourcing certain functions comes the requirement to oversee the activities of these third parties. Unfortunately, handing off responsibility to an outside vendor doesn't relieve you from managing the possible risks inherent in that relationship. That burden remains squarely with your organization. After all, it's your company's reputation and ability to operate that is on the line with every outside partnership you enter.

Not only should you perform due diligence on the front end to thoroughly screen service providers and gain assurance that their practices and procedures are up to standards, but you have to continually monitor the relationship so that once-sound practices don't veer off course.

There are various risk mitigation techniques that can be used when doing business with third-party service organizations. The primary question is: What level of assurance do you want or need?

The answer to this question is highly variable and depends on multiple factors, including the nature of your business, your risk appetite, the type of relationship and even your industry.[1] It may also depend on structural or cultural shifts within your organization, or changes to processes, people or the market landscape in which you operate. Additionally, external trends, such as an increase in the volume and intensity of external hacking attempts or regulatory change, can influence the level of assurance required.

continued>

[1] For more information on assessing your third-party relationships, see the *CorporateGovernor* white paper *Keeping third-party risk in check.*

Finding your place on the continuum: Mitigating third-party risk through ongoing monitoring (continued)

The assurance continuum

Just as the framework for assessing risk should be flexible enough to recognize that not all risks are created equal, so, too, should the framework for selecting mitigation techniques. It may help to think of this issue in terms of a continuum.

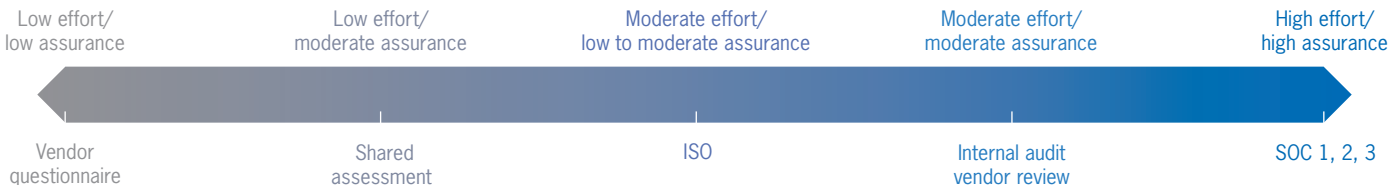
For instance, a lower level of assurance, requiring a minimal amount of work on the part of your organization, might be to ask an outside service organization to complete a standard, internally generated questionnaire. You would ask a consistent set of questions inquiring about certain controls and safeguards. Then you would evaluate responses and, ideally, escalate issues if deficiencies or other concerns regarding the vendor were identified. This type of assessment provides a low level of assurance as the responses from the vendor are not validated by an outside, independent party. But, depending upon the results of the risk assessment, this technique may be completely adequate to satisfy your needs.

A slightly higher level of assurance might be achieved by using a more standardized assessment tool, such as one that is specific to a particular industry (e.g., banking, health care), or one that is sponsored by a standard-setting group such as the National Institute of Standards and Technology or the International Organization for Standardization (ISO). These frameworks are typically designed to evaluate a vendor against industry standards. They provide greater assurance than a self-assessment due to the involvement of outside consultants engaged by the vendor to perform the assessment. Although there are some useful shared assessment frameworks available, the standard frameworks are not tailored to your company's risks and therefore may not provide sufficient risk mitigation. But again, if the results of the risk assessment suggest a moderate level of assurance, this type of assessment may be sufficient when coupled with other factors.

A next progression on the assurance continuum could entail deploying internal auditors to perform a custom vendor review or even to execute a tailored assessment based on one of the shared assessment frameworks. This approach provides a higher level of assurance because the review is customized to the specific risks identified during the risk assessment and performed by your internal audit team, which has a solid understanding of the services being provided. Unfortunately, one obstacle to this approach may be a scarcity of resources or competing organizational priorities for internal audit's time. Even if a company has in-house internal audit staff, the organization would need to determine that the risk associated with one or more vendors was sufficient to warrant the allocation of resources to that review. As with the other techniques, the results of the risk assessment should build the case for this type of technique to be applied.

The highest level of assurance would come from a custom, independent third-party review that is based on direct testing or evaluation. This might include a robust testing process consisting of inquiries, observations and inspections performed by a third party in order to form an opinion regarding the adequacy of the vendor's control environment. This form of evaluation is often based on one of the AICPA's attestation standards because these can help vendors demonstrate the strength of their internal controls to current and prospective customers. This review can also provide your organization with a description of the system of internal control as well as the results of the auditor's testing. For this type of report to be useful, however, companies need to understand which report will deliver the information they need.

continued>



Finding your place on the continuum: Mitigating third-party risk through ongoing monitoring (continued)

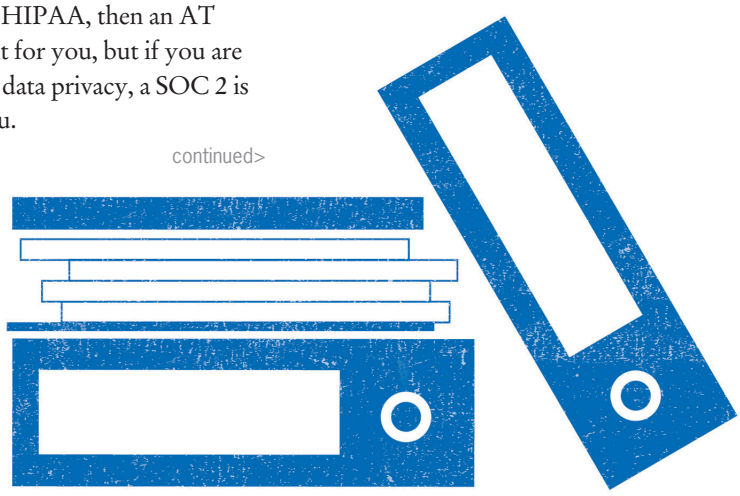
Types of attestation reports

The AICPA's attestation standards allow for a significant amount of flexibility. As long as an organization can establish suitable criteria (i.e., criteria that are objective, complete, available, relevant and measureable) against which an independent auditor may evaluate the organization, an auditor can build an attestation report. However, the most common attestation reports are categorized as Service Organization Control℠ (SOC) reports.[2] There are three different types of SOC reports:

- SOC 1 reports provide a vehicle for reporting on a service organization's system of internal control that is relevant to a user organization's internal control over financial reporting. SOC 1 reports are intended to be auditor-to-auditor communications, with specific content dependent on the service organization's system.
- SOC 2 reports address controls at a service organization that are pertinent to the Trust Services Principles (TSP) of security, availability, processing integrity, confidentiality and privacy. This type of SOC report addresses operational, regulatory compliance or privacy risks.
- SOC 3 reports allow service organizations to provide user organizations and other stakeholders with a report on controls that are relevant to the TSP. But unlike SOC 1 and SOC 2 reports, SOC 3 reports are short-form reports that can be distributed or posted on a service organization's website as a seal. If your organization must address subject matter that does not appear to be satisfied by one of these types of SOC reports, a customized attestation report using another AICPA attestation standard may provide the assurance you need. For example, AT 601 might be the appropriate standard if you need to demonstrate compliance with requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, or other regulatory or authoritative guidance.

As you can see, there are a number of options when it comes to obtaining a high level of assurance regarding a vendor's control environment. The key to selecting the right type of report is the risk assessment, because it is through the risk assessment process that you identify your needs. If you need to demonstrate compliance with HIPAA, then an AT 601 report is right for you, but if you are concerned about data privacy, a SOC 2 is the report for you.

continued>



[2] For more information, see www.aicpa.org/soc.

What's right for you?

How do you decide what level of assurance you need when it comes to mitigating risks from outside service providers? Key considerations include the following:

- Take into account the risk factors that surfaced during the risk assessment, which will highlight a vendor's potential impact on your organization. Obviously, a service provider that is entrusted with a significant amount of business or that has access to highly sensitive information may warrant greater scrutiny.
- Consider the culture, structure, people and processes of your organization. What type of industry or market do you operate in? How does your organization leverage vendors to be more competitive in the marketplace, and what is the regulatory environment in which you operate?
- Who will bear the costs involved? Although obtaining a third-party attestation report would likely be more costly than an internal review, it might be borne by a service provider as part of a contractual obligation. Even if it's not, the high level of assurance that can be obtained through third-party independent review may be what your business needs or what your stakeholders expect.

Keep in mind that deciding how to mitigate risks from third-party service providers can be highly subjective. The best course of action will vary considerably among companies and industries, depending on your unique universe of risks and the degree of assurance you feel is needed to keep risks in check and gain peace of mind. The most important thing is to proactively consider your options and find the risk mitigation techniques that are best suited to your organization. •

About the newsletter
CorporateGovernor is published by Grant Thornton LLP. The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest-quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the six global audit, tax and advisory organizations. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

For additional information on the issues discussed in this newsletter, consult your Grant Thornton client-services partner.

Contact information
For more information, contact:

Kirt Seale
Principal and National Special Attestation Reports Leader
T 214.561.2367
E kirt.seale@us.gt.com

Editor: Evangeline Umali Hannum, evangeline.umalihannum@us.gt.com