Daily Business Review
https://www.law.com/dailybusinessreview/2020/08/03/contractual-considerations-when-outsourcing/

Contractual Considerations When Outsourcing

The growth in outsourcing combined with a more rigid regulatory environment has led more firms and their financial statement auditors to request System and Organization Controls (SOC) reports from external service providers.

By **Mark Agulnik** | August 03, 2020

Many firms (i.e., user entities) outsource several functions, such as payroll processing, third-party administration of benefit plans, managed IT services and data centers. The growth in outsourcing combined with a more rigid regulatory environment has led more firms and their financial statement auditors to request System and Organization Controls (SOC) reports from external service providers. This trend will likely continue as businesses focus on core competencies while trying to emerge from the pandemic.

SOC reports can offer comfort to user entities and their auditors. Special contractual consideration when drafting an agreement between an organization and its vendors are essential, especially when the vendor is required to have a SOC report.

Basics of SOC Reports

SOC reports demonstrate that a Certified Public Accountant (CPA) with requisite expertise has evaluated the controls and systems of a service organization.

The three kinds of SOC reports:

- SOC 1–Reporting on an examination of controls at the service organization relevant to user entities' internal control over financial reporting.
- SOC 2–Reporting on an organization's controls around its data security program.
- SOC 3–The same purpose as a SOC 2; however, the content is significantly redacted and is usually more appropriate than a SOC 2 for marketing purposes.

SOC reports are also classified by type:

- Type 1–An opinion on whether the description is fairly stated and the controls are designed and implemented as of a point of time.
- Type 2–An opinion on whether the description is fairly stated and the controls are designed and implemented and operating effectively over a period of time (generally six months or greater).

A SOC 1 or SOC 2 can be a Type 1 or Type 2, while a SOC 3 is required to be a Type 2.

Fueling Demand

Legal and compliance departments, financial statement auditors and regulators require SOC 1 reports in an effort to reduce the risk of potential misstatement in the entity's financials. In many cases, independent auditors are required to obtain a SOC 1 if a significant service is outsourced (i.e., potential for material impact on financial statements)—particularly public companies.

Demand for SOC 2 reports stems from outsourcing, especially IT functions (e.g., data centers, managed IT services and software development). Legal and compliance departments are paying attention, given the prevalence of data breaches, when service organizations gain access to personally identifiable information (PII), Protected Health Information (PHI) and/or Intellectual Property (IP). The SOC 2 protocol provides criteria requiring service organizations to have controls to protect such sensitive data. Specifically, the SOC 2 can be tailored to focus on security, availability, processing integrity, confidentiality and/or privacy. There are also criteria to meet users' service commitments and system requirements.

Ensure Compliance Is Practical

Legal and compliance departments protect their by ensuring outsourced service organizations have robust processes and controls. Service organizations too often enter into agreements without the ability to meet contract terms—potentially due to lack of resources or unrealistic expectations.

Considerations to remember:

Legal and compliance departments may want a SOC 1 and SOC 2 from the service organization.

If the service has no or minimal impact on the user entity's financial statements, then the SOC 1 wouldn't carry much value. For example, if an organization outsources network security, it is unlikely to have a significant impact on financial statements, and a SOC 1 wouldn't be valuable. However, since the service organization has access to security features (i.e., protected data), a SOC 2 is more applicable.

Other types of non-SOC services may meet legal and compliance departments' needs, such as ISO 27001 certification, HITRUST Certification, PCI compliance, vulnerability assessments and/or penetration tests. Legal and compliance departments should question the reason for the SOC 1/SOC 2 and consider whether other types of certifications should be obtained.

Legal and compliance departments may want an opinion on all five trust criteria (security, availability, processing integrity, confidentiality and privacy) even though they all aren't applicable.

Consider if an organization outsources printing and mailing healthcare statements; processing integrity is likely important to ensure envelopes have the correct statements and are mailed to the designated recipients. If the service organization is a data center, processing integrity may not apply as data centers don't actually process data.

Regardless, if legal and compliance departments require a SOC 1 and/or a SOC 2, they'll likely want a Type 2 to provide more assurance that controls are operating effectively over a period.

SOC 1 and SOC 2 (Type 2) reports should cover at least six months. Furthermore, it may take months for a service organization to become compliant with specific requirements of the report type. The contract should reflect this.

In many cases, compliance with Type 2 requirements will take significantly longer. The user entity and service organization should consider language providing for the service organization to achieve Type 1 compliance before graduating to Type 2. This will provide quicker assurance that controls have been designed and implemented.

Legal and compliance departments may require that the SOC report opine on all subcontractor organizations (i.e., service organizations) and their subcontractors (i.e., subservice organizations) with access to confidential data.

The SOC auditor can include all service and subservice organizations within the report ("inclusive method"). However, this requires that subservice organizations allow access to their environments and could take longer than if the SOC report focuses only on the service organization's controls (carve-out method)—an important consideration when setting a due date in the contract.

Alternatively, the user entity and service organization can discuss which subservice organizations have access to the service organization's environment and determine alternative procedures for greater efficacy. For example, the service organization can obtain SOC reports and perform other monitoring procedures over subservice organizations to provide some assurance that the subservice organization's controls don't pose a significant risk.

Legal and compliance departments may require that the SOC report be unqualified (i.e., that the service organization's controls are designed and implemented and/or are operating effectively).

This requirement is important, but if there is language specifying that the report needs to be unqualified, there should be a time period where qualification needs to be remediated prior to the service organization being considered noncompliant. For example, if the report is issued on December 31, 2019, with a qualification, the agreement could allow for a three-month period to show the user entity that the deficiency has been remediated.

In Conclusion

Multiple factors have led to service organizations being required to become SOC-compliant. When determining the contractual language between user entities and service organizations, provisions should be transparent including the exact services required and a realistic timeline. If ever in doubt, an experienced service auditor (i.e., SOC auditor) can offer insight into relevant and meaningful contractual language based on trends in the marketplace and provisions that can be realistically met.

Mark Agulnik *is a partner at Marcum in Fort Lauderdale. He is an accountant and the firm's Southeast IT Risk and Assurance Services leader.*