Small Company Perspectives: How to Tackle SOC 2 If You Have No Board of Directors

Background

As service organizations transition to and begin using the 2017 Trust Services Criteria for SOC 2 reporting, some smaller companies are struggling with one of the new criteria related to the board of directors (CC1.2). Specifically, how can they address this criteria if they do not have a board of directors (BOD)?

Because CC1.2 comes directly from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2013 internal control framework, there will be references throughout this whitepaper to COSO 2013.

CC1.2 / COSO Principle 2 states that: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

In order to address this criteria, most companies have an independent board of directors that meets regularly and the duties and oversight responsibilities of the board are set forth in a charter document. Smaller organizations that do not currently have a BOD or whose board members are not independent are finding this criteria to be very challenging to address. The purpose of this whitepaper is to present strategies on how to address CC1.2 in a SOC 2 engagement when a company does not have an independent BOD.

Who should have a BOD?

Certain companies are required by law to have a BOD. This whitepaper does not apply to those organizations, regardless of their size, unless their board is not independent. Every public company must have a BOD. Every C Corp and S Corp must also have a BOD. But other types of entities, such as limited liability companies (LLCs) and sole proprietorships are not required (by law) to have a BOD. This whitepaper is geared toward these types of entities with no legal requirement for a board, which are often smaller companies.

By Jamie Kilcoyne, CPA, CISA, CITP, CIA, CFE - K Financial

Many people ask "when is the right time to implement a board of directors?" They expect a simple answer – "$20 million in revenue" or "100 employees." But the answer is not that simple. It is not revenue or the number of employees that matter at the end of the day. It is the complexity and the nature of the business. Determining whether it is the right time for a small company to implement a BOD requires an understanding of the company's goals, strategy and direction. In general, as small businesses grow in size and complexity they should consider implementing a BOD.

Boards provide oversight control, including discipline, independence, expertise and accountability. That is why the vast majority of successful companies have a board structure with an external chairman.

COSO Small Company Guidance

In 2006, COSO published a document entitled "Internal Control over Financial Reporting – Guidance for Smaller Companies." (Aspects of the COSO 2006 document related to smaller companies are incorporated into appendix C of COSO 2013.) Although the document is intended to help small public companies comply with the control requirements of the Sarbanes-Oxley Act, there are some important concepts in the document that are leveraged in this whitepaper and that are also applicable to small private companies undergoing a SOC 2 examination.

The COSO 2006 document identifies characteristics of "smaller" businesses and implies that it may be acceptable for these types of organizations to apply a different (more cost effective) approach to internal control than larger companies. The characteristics that are identified in COSO 2006 are the following:

- Fewer lines of business and fewer product lines
- Leadership by management with significant ownership interest or rights
- Fewer levels of management
- Less complex transaction processing systems and protocols
- Fewer personnel

The COSO 2006 document states that "Smaller companies typically have relatively straightforward business operations with less complex business structures…" It goes on to say that "Many small businesses are dominated by the company's founder or other leader who exercises a great deal of discretion and provides personal direction to other personnel. While key to enabling the company to meet its growth and other objectives, this positioning can also contribute significantly to effective internal control…"

Although CC1.2 appears to be black and white with regard to the requirement for a BOD, the interpretive text in COSO 2013 suggests otherwise. For instance, on page 40 under Authorities and Responsibilities, COSO 2013 says "The board of directors or equivalent oversight body (the board) understands the business and expectations of stakeholders…" This language supports our position that some small companies may be able to effectively address CC1.2 without a BOD if they have an equivalent oversight body. Some examples of oversight bodies that may satisfy CC1.2 are:

- IT Steering Committee
- Security Operations Committee
- Business Operations Committee

The name of the committee is not that important and can certainly be different than the examples above. What matters is the oversight responsibilities of the committee and these should be set forth in a charter document. At a minimum, the charter document should include:

- Definitions of the skills and expertise required of committee members
- Identification of the committee's oversight responsibilities, including internal control
- Frequency of meetings
- Topics to be covered in meetings
- Risk assessment responsibilities – consider internal and external factors that pose significant risks to the achievement of objectives (i.e., commitments and system requirements communicated to customers)
- Oversee the performance of control activities
- Communicate direction and tone at the top
- Assess and oversee monitoring activities

Independence

In order for a company that does not have a board of directors or an independent BOD to address the "independence" component of CC1.2, it is recommended that the committee discussed above or board include at least one member who is not involved in the performance of controls. This individual should also have the expertise and experience to appropriately oversee the control environment.

Conclusion

As auditors, we recognize that there are inherent risks associated with companies that do not have an independent board of directors (regardless of their size). In a SOC 2 engagement, these risks will be documented and evaluated as part of our required auditor risk assessment procedures. If a service organization undergoing a SOC 2 examination does not have an independent BOD to address CC1.2, we will do the following:

1. Evaluate whether the organization should have a BOD. This will be determined by the nature and complexity of the business and other information that we gather during the SOC assessment. This should include a candid discussion with management about whether a BOD will provide value to the organization from an oversight perspective. If we conclude that a BOD is necessary to address the oversight and / or independence components of CC1.2, then we will make a formal recommendation to this effect and our service auditor's report may include a modified opinion with respect to CC1.2.

2. If we determine that a BOD is not necessary given the nature and complexity of the business and will not provide value to the company, then we will evaluate whether there is an "equivalent oversight body" that addresses the requirements of CC1.2. Controls associated with the equivalent oversight body will be tested to determine if they are operating effectively.

An example set of key controls for CC1.2 for an organization that does not have an independent board of directors is as follows:

a. XYZ has an IT Steering Committee that exercises oversight of the development and performance of internal control. The committee includes at least one member who is not involved in the performance of controls.

b. XYZ has an IT Steering Committee Charter that includes roles and responsibilities relevant to internal control and sets forth the oversight responsibilities of the committee.