Cybersecurity Risk Management — AICPA Introduces New SOC

10.16.17

In today's increasingly interconnected and IT-dependent business environment, cybersecurity is a concern for most organizations. Data breaches can have a significant impact on a company's earnings and stock price, as well as its reputation. So, it's critical for companies to evaluate their cybersecurity programs and educate their directors, investors, and other stakeholders about the extent and effectiveness of their risk management efforts.

SOC created

Earlier this year, the American Institute of Certified Public Accountants (AICPA) introduced its System and Organization Controls (SOC) for Cybersecurity. Using this SOC is strictly voluntary, but it offers numerous benefits. It enables CPAs to examine and report on an organization's cybersecurity risk management program.

The SOC provides companies and CPAs with a common language and framework for describing, evaluating and reporting on the effectiveness of a company's cybersecurity program. The framework can also be used to give stakeholders an independent, third-party assessment of the company's cybersecurity risk management efforts.

The AICPA determined that three separate reports were needed: at the entity, service provider and supply chain levels. The current SOC covers entity-level reporting. The AICPA will release additional guidance on the other two reporting levels in the future.

Components of entity-level reporting

The entity-level cybersecurity reporting framework contains three components:

1. Management's description. This component explains the company's cybersecurity risk management program using suitable description criteria. For example, management will describe how the company identifies sensitive information and systems, how it manages cybersecurity risks and how it protects information and systems against those risks.

2. Management's assertion. In this section of the report, management asserts whether its description meets the SOC's description criteria and whether the program's controls were effective in achieving the company's cybersecurity objectives based on suitable control criteria.

3. Practitioner's opinion. This component calls for a CPA to review whether management's description is fairly presented in accordance with the description criteria and the company's particular circumstances. The CPA's opinion must also state whether controls within the cybersecurity program effectively achieved the company's cybersecurity objectives based on the control criteria.

Description and control criteria

The AICPA has developed the following nine categories of description criteria for an organization's cybersecurity program:

- Nature of business and operations,
- Nature of information at risk,
- Cybersecurity risk management program objectives,
- Factors that have a significant effect on inherent cybersecurity risks,
- Cybersecurity risk governance structure,
- Cybersecurity risk assessment process,
- Communications and quality of information related to cybersecurity,
- Monitoring of the cybersecurity risk management program, and
- Cybersecurity control processes.

Within each category, the AICPA provides detailed implementation guidance and examples. The guidance is flexible, however. Management may select other criteria, as long as they're suitable in the circumstances.

The AICPA also revised its Trust Services Criteria for use as control criteria in cybersecurity examinations. These criteria were developed 20 years ago for use in evaluating the security, availability, processing integrity, confidentiality and privacy of entity systems.

You can find more about description and control criteria on the AICPA website at http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpacybersecurityinitiative.aspx

Reap the benefits

The SOC for Cybersecurity offers countless benefits: It addresses cybersecurity information requests from investors and others, provides stakeholders with a higher level of confidence in the company's cybersecurity efforts, helps compare the company's cybersecurity program with those of other companies and with its own program over time, and helps management identify and implement cybersecurity best practices. Consult with your management team and CPA firm to review the SOC and determine how it can work for you.