of a new engagement that CPAs can use to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of an …

Sep. 27, 2016

In an important step toward helping businesses and organizations report on their cybersecurity risk management efforts, the American Institute of CPAs' (AICPA) Assurance Services Executive Committee (ASEC) is exposing two sets of criteria for public comment.

The first exposure draft, *Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, is intended for use by management in designing and describing its cybersecurity risk management program and by public accounting firms to report on management's description. The second, *Proposed Revision of Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, outlines revised AICPA trust services criteria for use by public accounting firms that provide advisory or attestation services to evaluate the controls within an entity's cyber risk management program, or SOC 2® engagements. Management also may use the trust services criteria to evaluate the suitability of design and operating effectiveness of controls.

"In response to growing market demand for information about the effectiveness of an entity's cybersecurity risk management program, the auditing profession, through the AICPA, is developing a common foundation through the issuance of criteria and guidance," said Susan S. Coffey, CPA, CGMA, AICPA executive vice president for public practice. "Our primary objective is to propose a reporting framework through which organizations can communicate useful information regarding their cybersecurity risk management programs to stakeholders."

The development of a common set of criteria will pave the way for the introduction

"The existence of multiple, disparate frameworks and programs for evaluating security programs and their effectiveness, as well as different stakeholders' preferences for each, has created a chaotic environment that only increases the burden on organizations trying to communicate how they design, implement and maintain an effective cybersecurity risk management program," according to Chris K. Halterman, chair of the ASEC's Cybersecurity Working Group and an executive director, advisory services with Ernst & Young LLP. "The AICPA's cybersecurity engagement will be a consistent, market-driven approach for CPAs to examine and report on an entity's cybersecurity measures that addresses the information needs of a broad range of users."

The exposure drafts are the CPA profession's latest contribution to widespread efforts to help management and boards of directors address what has emerged as a risk for organizations of all sizes, and in all sectors. ASEC's work is just one aspect of the profession's multi-faceted approach to support CPAs in a leadership role and provide the resources they need to be successful in helping their companies and clients manage cybersecurity risk.

Comments on the cybersecurity attestation exposure drafts are due by Monday, December 5. Comments about the proposed *Description Criteria* should be sent to Mimi Blanco-Best at mblancobest@aicpa.org. Comments regarding the proposed revision of *Trust Services Criteria* can be directed to Erin Mackler at emackler@aicpa.org.

For additional information on the CPA profession's cybersecurity efforts, visit the AICPA's Cybersecurity Resource Center.

Accounting • Advisory • Auditing

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us