Help Shape the AICPA's Cybersecurity Risk Management Initiative

Background

Given the immense scale and complexity of the cybersecurity challenge, every sector of the economy, public and private, has a measure of responsibility for promoting cybersecurity resilience. The auditing profession is in a strong position to play an important role in advancing cybersecurity risk management practices, bringing to bear the core values of independence, objectivity, and skepticism—as well as its deep expertise in providing independent evaluations of a broad range of subject matter in a variety of contexts, including that of cybersecurity risk management and information security.

In response to the challenges posed by cybersecurity threats, the American Institute of CPAs (AICPA) is developing a new engagement that CPAs can perform to assist boards of directors, senior management, and other stakeholders as they evaluate and oversee the effectiveness of their organization's cybersecurity risk management programs. This cybersecurity engagement could provide an overall benefit to the market by promoting a consistent methodology and reporting framework as well as fostering credibility through performance of objective, independent examinations. During development of the new engagement, the Center for Audit Quality (CAQ) is teaming with the AICPA to gain feedback from various stakeholders.

To enable management and CPAs to prepare for the engagement, the AICPA Assurance Services Executive Committee (ASEC) is exposing for public comment two sets of cybersecurity-related criteria including: (1) *Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (Description Criteria Exposure); and (2) *Proposed Revision of Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (Trust Services Criteria Exposure), collectively, (Exposure Drafts).

The Exposure Drafts can be found on the AICPA's Cybersecurity Intiative web page.[1]

Why Stakeholders Should Comment

We encourage stakeholders—including members of management with oversight of cybersecurity risk management, and internal and external auditors—to submit comments on the proposed Description Criteria Exposure and the proposed revisions to the Trust Services Criteria Exposure. Your input is necessary for several reasons:

- The Exposure Drafts provide an opportunity to contribute to a flexible, yet comprehensive, market-based solution to cybersecurity risk management.
- Your feedback will assist in the development of a common language and approach for establishing and monitoring cybersecurity risk management programs.
- The AICPA will consider adapting and advancing the engagement requirements according to feedback from users of this information. Your comments on the usefulness and completeness of both sets of the proposed criteria will serve to aid the AICPA and the audit profession in that endeavor.

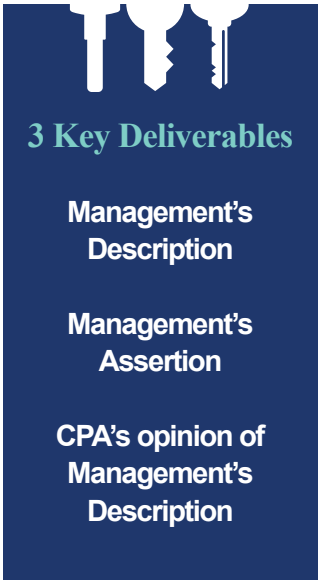
Complete details on how to submit comments can be found at the end of this document.

1 Available at http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

The Exposures

It is important to note that the Trust Services and Criteria Exposure includes updates for changes to technology that underpin not only the new CPA cybersecurity engagement, but also other attestation and consulting services related to information security and privacy.

This new cybersecurity examination engagement will be performed in accordance with existing attestation standards. Those standards require that management be accountable for what is contained in the report. In the case of the cybersecurity examination, the report's subject matter will include: (1) a description of the entity's cybersecurity risk management program prepared in accordance with suitable description criteria; and (2) an assessment of the effectiveness of the controls in a cybersecurity risk management program based on suitable control criteria. As a result, these two distinct—yet complementary—sets of criteria will form a critical basis for performing the future cybersecurity examination engagement.



The engagement will consist of three key deliverables. The first, Management's Description, will be a management prepared narrative description of the entity's cybersecurity risk management program. The Description Criteria Exposure provides proposed description criteria that would be considered suitable for management to utilize in developing Management's Description of the subject matter, and for CPAs in evaluating the description. The description criteria are categorized into nine areas so that Management's Description provides users with information about an entity that will enable them to better understand the entity and its cybersecurity risk management program. Management's Description is designed to provide users with information about the entity's operations, how the entity identifies its sensitive information and systems, the ways in which the entity manages the cybersecurity risks that threaten it, and a summary of controls implemented and operated to protect the information and systems against those risks.[2] Management's Description, as defined by the description criteria, is intended to provide the context needed to understand the conclusions expressed by management in its assertion.

Some questions to consider as you respond to the Description Criteria Exposure include:

- Are there any unnecessary or otherwise not relevant *description criteria* or *points of focus*? Please provide a list.
- Are there any missing *description criteria* or *points of focus*? Please provide a list.
- Are there any *description criteria* or *points of focus* that would result in disclosure of information that would increase the risk of a security event? Please provide a list.
- Do you have any concerns about the measurability of any of the *description criteria* or *points of focus*? Please provide a list.
- The AICPA developed the *description criteria* and related *points of focus* using an approach similar to the one used by the Committee of Sponsoring Organizations of the Treadway Commission Internal Control – Integrated Framework (COSO) when developing its *Integrated Framework—Internal Control*.[3] Similar to the COSO approach, a description of the entity's cybersecurity risk management program prepared in accordance with the *description criteria* would include information about each of the criteria in this document. The *points of focus* related to the criteria are important characteristics of the criteria. Consistent with the COSO approach, management may determine that some of the *points of focus* are not suitable or relevant and may identify and consider other characteristics based on specific circumstances of the entity. *Points of focus* assist management in determining the matters to be addressed in the presentation. However, use of the criteria does not require management to address every *point of focus* in its description. Do you believe this approach is appropriate? If not, please describe the approach you would recommend.

The second deliverable to the future cybersecurity engagement will be Management's Assertion that the controls implemented as part of the cybersecurity risk management program are suitably designed and operated effectively (during the designated period of the examination). Management will use control criteria when evaluating if their cybersecurity risk management controls are effective.

2 See paragraph .16 of the Description Criteria Exposure for a complete listing of all nine categories of the description criteria.

3 Available at http://www.coso.org/ic.htm

For this purpose, the revised trust services criteria for security, availability, and confidentiality (criteria for security, availability, and confidentiality) in the Trust Services Criteria Exposure have been designed to be suitable control criteria (both for a future cybersecurity examination and other attestations.) Much like management typically utilizes COSO as the control criteria to evaluate their internal control over financial reporting (ICFR), management could similarly use the criteria for security, availability, and confidentiality in the Trust Services Criteria Exposure as the control criteria in the future cybersecurity engagement to evaluate their cybersecurity risk management controls.

The final deliverable in this examination engagement is the CPA's opinion on Management's Description (i.e., its completeness and accuracy) and on whether the controls within that program were suitably designed and operated effectively to achieve the entity's cybersecurity objectives based on the control criteria.

Similar to the auditor's consideration of Generally Accepted Accounting Principles (GAAP) when determining whether the financial statements are fairly presented, the CPA in a cybersecurity engagement will evaluate whether Management's Description is fairly presented using the description criteria. As it relates to the evaluation of the effectiveness of the controls included in the cybersecurity risk management program, CPAs could use the criteria for security, availability, and confidentiality in the Trust Services Criteria Exposure, much like auditors apply COSO in evaluating the design and operating effectiveness of internal controls in an ICFR audit.

The criteria for security, availability, and confidentiality in the Trust Services Criteria Exposure have been mapped to other commonly used cybersecurity risk-management frameworks, such as COSO, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure (NIST), or the International Organization of Standardization Information Security Management (ISO 27001 and 27002). Management may choose other suitable frameworks.

As mentioned above, the criteria in the Trust Services Principles and Criteria Exposure will be utilized in other engagements in addition to the cybersecurity engagement, SOC 2 reports, for example.

However, some questions to consider, relative to the cybersecurity engagement, include:

- Are there any unnecessary or otherwise not relevant *supplementary criteria* or *points of focus*? Please provide a list.
- Are there any missing *supplementary criteria* or *points of focus*? Please provide a list.
- Do you have any concerns about the measurability of any of the *supplementary criteria* or *points of focus*? Please provide a list.
- The AICPA developed the *trust services criteria* and related *points of focus* using an approach similar to the one used by COSO when developing its *Integrated Framework—Internal Control.* The *points of focus* are important characteristics of the criteria. Consistent with the COSO approach, management may determine that some of the *points of focus* are not suitable or relevant and may identify and consider other characteristics based on specific circumstances of the entity. *Points of focus* assist management and the practitioner in evaluating whether the controls are suitably designed and operating effectively. However, use of the criteria does not require management or the practitioner to separately assess whether each point of focus is addressed. Do you believe this approach is appropriate? If not, please describe the approach you would recommend.

Submitting a Comment

Content: It is not necessary to respond to any and/or all questions. Comment letters can be at a thematic level and/or focus only on the question(s) or topic(s) on which you have a point of view. When commenting, consider referring to specific paragraphs or criteria numbers, include the reasons for the comments, and make specific suggestions for any proposed changes to wording.

Deadline: Comments are due on or before December 5, 2016. Note, however, that historically the AICPA has accepted comments after the deadline.

How to submit comments: Written comments on the Description Criteria Exposure should be sent to Mimi Blanco-Best at mblancobest@aicpa.org. Written comments on the Trust Services Criteria Exposure should be sent to Erin Mackler at emackler@aicpa.org.