The Institute of Internal Auditors

Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

December 7, 2016

American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

Response emailed to mblancobest@aicpa.org and emackler@aicpa.org

RE: AICPA Exposure Drafts: Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program and Proposed Revision of Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Dear Sir/Madam:

On behalf of the more than 185,000 global members of The Institute of Internal Auditors (IIA), I am pleased to provide our response to the recent Exposure Drafts concerning the AICPA's Cybersecurity Risk Management Initiative.

The AICPA's efforts to align with existing regulations, frameworks and standards regarding cybersecurity risks are commendable. However, while we agree SSAE 16 does not contain sufficient detail to address cyber risk in SOC reviews, we do not believe separate reviews and opinions by public accounting firms on an entity's cybersecurity risk management are the best next step in helping organizations address cyber risk.

Cybersecurity is an ever-evolving risk that increasingly demands greater attention from organizations. AICPA's proposed attestation services are unlikely to adequately address an organization's current needs or the needs of its stakeholders. The proposed attestation would most certainly be issued as of a specific point in time, mention significant inherent limitations, and bring significant cost. What's more, the proposed attestation services could provide an unrealistic appearance of certainty and likely divert organizational resources away from addressing the cyber risks themselves.

Global Headquarters
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

One of the key reasons the Cybersecurity Act of 2012 failed to pass in the U.S. Senate was because of concerns over added costs and an unnecessary burden on business. Past experiences, such as the impacts associated with complying with the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, further show that another framework and external review of an entity's cybersecurity risk management program would surely increase compliance costs. Of critical importance is not the cost in isolation, but the benefits of the proposed attestation work, which must outweigh the costs.

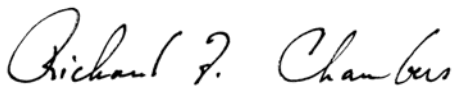
At this time, the focus should be on enabling organizations to address the risks and to accommodate emerging regulatory requirements. This may be best accomplished with a robust, objective, and independent internal audit function that has the skills set and is adequately resourced to address such risks. If an organization wishes to have limited assurance available through attestation services, some form of agreed-upon procedures engagement may be more appropriate. But a comprehensive external attestation is not appropriate at this time.

In addition, an effective evaluation of a cybersecurity risk management program requires specialized skills. While efforts have been made by public accounting firms to acquire these skills, it's crucial that firms ensure they have credible resources to perform these reviews. This would mean firms would need to aggressively seek out personnel who have the cyber related skills. It is unclear why it is in the best interest of organizations to look to public accounting firms for these skills. In fact, having firms aggressively recruiting personnel who have these skills could impede organizations from obtaining them to more directly address the cyber risks.

Supplemental, detailed comments are included as an appendix should the AICPA decide to move forward with this initiative. These comments are summarized by the questions raised by the Assurance Services Executive Committee (ASEC).

We appreciate the opportunity to provide our response to these Exposure Drafts. If you have any questions about our response or would like to discuss further, please contact Kathy Anderson, The IIA's Managing Director of North American Advocacy. Ms. Anderson can be reached at Kathy.anderson@theiia.org or 1-407-937-1291.

Sincerely,



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President & Chief Executive Officer

Attachment

APPENDIX

Detailed Comments re: AICPA Exposure Drafts
Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program and Proposed Revision of Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Are there any unnecessary or otherwise not relevant description criteria or points of focus?
There exists duplication in points of focus including the following: roles, responsibilities and accountabilities are addressed in DC6, DC9, DC11 and DC 13 and there exists some repetition. Communication criteria is also duplicated in several places including DC9, DC13, DC17, DC18 and DC19. DC30 and DC31 may be duplicative of the availability criteria discussed in DC3 and preventative controls in DC25. Continuous monitoring and assessments of cyber risk, as well as changes in business operations as required under DC7 may replace the need for updates to DC1 after the initial year.

Are there any missing description criteria or points of focus?
While the description criteria and points of focus align well with the "Identify", "Protect" and "Detect" function components of the NIST framework, there exist some gaps when attempting to align with the "Respond" and "Recover" functions. In particular, addition of the following NIST categories and subcategories would further enhance DC 27 and DC 28.

Category	Subcategory
Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies	• Personnel know their roles and order of operations when a response is needed • Events are reported consistent with established criteria • Voluntary information sharing occurs with external stakeholders to achieve cybersecurity situational awareness
Analysis is conducted to ensure adequate response and support recovery activities	• Incidents are categorized consistent with response plans
Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident	• Incidents are contained and mitigated • Newly identified vulnerabilities are mitigated or documented as accepted risks
Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTSs and vendors	• Public relations are managed • Reputation after an event is repaired

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?
While many of the description criteria require description of processes or a summary description, too much detail could expose an entity to increased risk of a security event.
DC2 – Nature of Information at Risk – This disclosure would alert the public to the types of sensitive, private and strategic information maintained by an entity.
DC5 – Detail technology and infrastructure information (particularly outdated or unsupported systems) may expose an entity to higher risks.
DC6 – Identifying system administrators could promote targeted cyber-attacks or phishing attempts.
DC8 – As it is noted in the exposure draft, information about security incidents should be shared on a "need to know" or required basis.

DC21 – Information about vulnerabilities or security threats may expose an entity to higher risks.
DC22 - Detail information about security configurations or network elements may expose an entity to higher risks.
DC25 – Detail about preventative controls, particularly access and provisioning controls may expose an entity to higher risks.
DC26 – Detail about detection mechanisms or monitoring processes may expose an entity to higher risks

The AICPA developed the description criteria and related points of focus using an approach similar to the one used by COSO when developing its *Integrated Framework— Internal Control*. Do you believe this approach is appropriate? If not, please describe the approach you would recommend.
The development of a COSO-type framework for evaluation purposes would provide standardization and efficiencies in the review process. We agree with this approach.