December 5, 2016

INTERNET SECURITY ALLIANCE

www.isalliance.org

Via mblancobest@aicpa.org
emackler@aicpa.org

Mimi Blanco-Best and Erin Mackler
American Institute of CPAs
1455 Pennsylvania Avenue, NW
Washington, DC 20004

Dear Ms. Blanco-Best and Ms. Mackler:

The Internet Security Alliance congratulates the American Institute of CPAs' for their effort to create a consistent assessment methodology for a company's cybersecurity risk management processes.

ISA represents some of the largest companies in the world. These companies are the intended buyers and audience for the AICPA's proposed cybersecurity attestation engagement. Our members are invested in ensuring that the finite company resources devoted to cybersecurity are spent efficiently and effectively.

We are gratified the AICPA recognizes that cybersecurity is a risk management issue requiring attention from boards of directors, senior management, business partners and investors.

Organizations that choose to voluntarily assess their own cyber readiness will be better able to understand their unique risk posture and be prepared to protect their systems. As these assessment tools are developed, it is imperative that they address the unique characteristics of the cyber threat. Thus, there are several unique characteristics that an appropriately designed cyber assessment tool would need to recognize.

1. These proposed engagements are assessments, not audits.

The term audit has a long and generally well-understood meaning. The integrity of the term audit should not be compromised by adapting it to the far less well-defined field of cybersecurity. ISA commends the AICPA for clarifying from the outset that they are not developing cyber auditing tools, but cyber assessment tools. This is an especially critical distinction as some in government often confuse the two and conflate them to be similar processes. While there are certainly some similarities, they are not and should not be considered equivalent.

Although CPAs traditionally perform audits, the AICPA appears to have taken great care to avoid the word "audit" when describing this proposed engagement. A cybersecurity "audit" calls to mind a mandatory, prescribed exercise that can actually be counterproductive to good cybersecurity by diverting resources away from dynamic and changing cybersecurity challenges.

Again, we concur with the AICPA's approach and feel it bears underlining. We believe independent *assessments* that describe how companies address cybersecurity risk have the potential to be useful in board-level oversight and as a tool for senior management.

While no one who has gone through a financial statement audit would ever characterize the process as simple, assessing the cybersecurity environment is in many respects more complicated. The financial audit model is essentially a backward looking, standards-based process that examines comparatively stable environments.

A properly designed cyber assessment would use a forward-looking risk management model. For example, determining the relative adequacy of an organization's cybersecurity cannot be assessed simply by cross-checking compliance with a pre-determined framework or set of standards. Indeed, over reliance on such backward looking methods can generate a false sense of security and detract scarce resources from more critical cybersecurity steps. Cyber defense is a much more affirmative and dynamic process than financial auditing, including anticipating potential threats and attackers, what sorts of data they may seek, and how their methods may change in light of various defenses.

This approach recognizes that the cybersecurity world is dramatically different than the financial statement audit world. Organizations facing cyber threats are dealing with sophisticated and pro-active agents who alter their methods in response to an organization's cyber defense implementation. In other words, it's a moving target. Thus, whereas a financial statement audit provides its value through a determination of whether or not an organization has complied with applicable standards as of a balance sheet date and for a historical period of time, a cyber assessment can only attest to the likelihood that an organization is more or less secure. A cyber assessment will, by definition, therefore, lack the clarity and finality that the audit community and their users have come to expect.

It is critical to appreciate that financial accounting standards or regulatory compliance are not equivalent to organizational cybersecurity.

2. Measuring cyber assessments should use a maturity model

Not only are cyber assessments conceptually different than financial statement audits, but also the scoring process needs to similarly reflect the unique cybersecurity environment. Cyber assessments cannot be graded on a pass-fail model. Whereas an organization may be able to determine it is either in or out of compliance with financial regulations and standards, there is no such clear demarcation between being secure and insecure. A properly designed cyber assessment cannot be used to pass judgment, but rather to offer guidance assisting the organization in responding to an ever-changing cyber threat posture. A key challenge that all assessments deal with is avoiding the binomial answer of yes/no but rather, determining "how well" a particular security process is working. For example, most current self-assessments ask whether a vulnerability management (e.g., patching process) is in place or not. They don't (and can't) measure how well the process is working. The AICPA will undoubtedly have to deal with this challenge in order to add real value.

In the current cyber environment, ultra-sophisticated attackers, including nation states, may successfully compromise virtually all organizations. There is no absolute security. Security is best understood as a continuum; thus, cyber assessments can be most useful if they illuminate the relative maturity of an organization's security posture. Accordingly, the premise or suggestion of a "clean"

cybersecurity assessment is not realistic. Maturity must take into account all three of the security pillars of Prevent, Detect, respond as even strong programs deal with cyber issues that make it past the firewall.

Not all companies need to obtain the same level of capability, especially since greater capabilities require greater investments in technical and organizational resources. As the AICPA's draft description criteria recognize, matters such as the nature of operations and the nature of information risk differ from company to company. So do the cybersecurity programs that result from distinctive responses to these questions. For some businesses, obtaining high levels of sophistication is unnecessary and a waste of limited available resources. In others, low levels of risk management controls indicate areas for needed improvement.

Accordingly, we urge the AICPA to incorporate a tiered-level evaluation into the assessment criteria, the method by which CPA practitioners will assess companies that hire them for this new engagement.

An assessment that hinges on fundamentally binary, yes/no responses to queries posted by points of focus fails to consider the spectrum of cybersecurity requirements and capability. A yes/no assessment fails to reward companies that have taken steps to improve their cybersecurity. Because binary assessments don't take into account a company's manner of satisfying a point of focus, they also fail to collect relevant information about the sophistication of the company's cybersecurity program, potentially leaving out from the assessment the company's range of actual capabilities.

For example, one point of focus under category CC2.1 asks whether "information systems process and transform relevant data into information." A sophisticated company's response might be that "the firm has an integrated, holistic and constantly updated view of its information technology assets and the security controls monitoring them." However, less sophisticated answers could also satisfy this point of focus, such as a response that "the company relies on disparate information systems with a slow refresh rate to convert IT asset performance data into information." Both responses might technically satisfy the point of focus, but the former company is clearly more mature in its cybersecurity capability.

A tiered approach also gives the right sort of incentive to companies desiring to improve their cybersecurity programs. Rather than reaching for a higher tier capability that will not bring their overall program into a higher level of maturity, companies guided by a maturity model can understand how to most cost-effectively improve their risk management posture by improving the things that keep them in a lower tier. This implies the number of tiers must be sufficiently granular that moderate investments or changes can yield achievable improvement in their tier score.

Finally, a maturity model allows companies, should they choose to do so, to integrate improved cybersecurity into their marketing strategies in order to distinguish themselves from their competitors by demonstrating improvements to their own previous scores or allowing clients to compare scores with other competitors. This characteristic of a maturity model can therefore improve the value proposition of security investments, thus incentivizing improved cybersecurity in a way that a binary assessment cannot.

3. Cybersecurity is not all about "IT"

One of the most fundamental truths the designers of an appropriate cyber assessment need to appreciate is that cybersecurity is not an "IT" (information technology) issue. It is an enterprise-wide risk management issue.

ISA again commends AICPA for embracing the notion of risk management in their proposal. However, it is important that this recognition be extended throughout the design of the assessment process itself.

While there is a foundational technology component to cybersecurity, an excessive focus on IT will not properly educate an organization about its cyber readiness or defense programs and will likely lead to the misallocation of organizational resources and reduced security.

While early research suggested large percentages of cyber attacks could be prevented with the use of basic cyber hygiene such as firewalls and passwords, as the attacks have increased in sophistication and expanded to even small and mid-sized organizations, the efficacy of basic cyber hygiene is no longer what it was.

Properly designed assessment tools need to appreciate the fullness of the modern cyber threat, including multi-staged attack methods using reconnaissance of organization's systems, people, and supply chain relationships to identify both technical and human weakness, which can be exploited via cyber means. Research has demonstrated that organizations (including the federal government) that rely excessively on IT aspects of cybersecurity – sometimes because the technical tools are so readily available — can lead to resource misallocation and actually undermine security.

4. Assessment tools need to focus primarily on techniques with proven effectiveness and cost effectiveness

A fundamental question assessment designers need to think through is what exactly should be the focus areas for assessments performed in a unique and fast changing environment. There are innumerable cyber threat vectors and almost as many technical standards and frameworks, most without empirical evidence of their efficacy.

Some current assessment programs attempt to analyze organizational preparation against the full universe of possible cyber threats and adherence to a wide range of various standards and frameworks. These programs can be extremely expensive and time-consuming and do little to help the company know where to spend their next dollar. For the AICPA's proposed engagement to have maximum utility for the intended consumers and thus market viability, it would be useful for cyber assessment reports to not only indicate the level of adherence to various standards and frameworks but also that such adherence will be effective and cost effective for the client.

One productive path AICPA should consider when designing their tools is to follow the work done by the National Association of Corporate Directors in their "Cyber Risk Handbook" published in 2015.

The NACD Handbook takes an enterprise-wide, risk management model built around five core cyber principles that are research based. These principles chart a clear path identifying tasks for corporate boards as well as management, including a blueprint for engaging the entire organization in productive cyber behavior.

The Institute of Internal Auditors Research Foundation, in coordination with the ISACA, has embraced the NACD Handbook and published a follow-up outlining further implementation procedures.

PricewaterhouseCoopers in its 2015 Global Information Security Survey reported on the positive impact the Handbook is having on multiple consensus security metrics. PWC reported:

> "Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. They should discuss cybersecurity risks and preparedness with management, and consider cyber threats in the context of the organization's overall tolerance for risk.
>
> Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending.
>
> Other notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. Perhaps more than anything, however, Board participation has opened the lines of communication between the cybersecurity function and top executives and directors."

Given that the NACD Handbook has been embraced by the auditing profession, which has itself documented its efficacy, perhaps it, rather than the multiple untested technical frameworks currently being considered, ought to be the initial and primary focus of designing a helpful cyber assessment tool.

It should be noted that ISA and NACD are also currently working on an updated version of the Handbook – focused on the appendices, not the core principles – and the audit profession is also well represented in that process with representatives from E&Y and the Center for Audit Quality serving on the updating committee.

Public policy has long called for the various technical frameworks to be assessed for cost-effectiveness. For example, President Obama's 2013 Executive Order 13636 explicitly called for NIST to develop a cybersecurity framework that would be cost effective. Although NIST released this framework in 2014, there has been no systemic effort to demonstrate its cost effectiveness. AICPA should consider collaborating with industry to conduct this assessment. Once completed, these frameworks will be more appropriate to be included in model cyber assessments.

5. The assessment tool needs to be a voluntary model – really voluntary

ISA's enthusiasm for senior-level oversight and measurement is tempered by recognition that mandatory audits of private sector cybersecurity practices are counterproductive to the goal of improved cyber defense. A properly conducted audit requires management-produced documentation and conformance to standards. As discussed above, that approach is perfectly reasonable in financial reporting, but it is ill suited to the ever-changing field of cybersecurity. Compliance is about what you do. Security is about how well you do it.

We concur with the AICPA that this engagement must be voluntary and market-driven in nature and that its adoption in the private sector depends entirely on the value organizations and stakeholders

perceive from it. To find a recent example of how "voluntary" becomes a de facto standard, look no further than the FFIEC CAT. A recent article highlights the exact concern very well: **http://bit.ly/2fpkrmI**

The voluntary quality of this engagement is a key characteristic that bears greater emphasis, especially in a marketplace apprehensive of the prospect of creeping and de facto regulation. With that in mind, we believe the requirement for a detailed management assertion is unnecessary in a voluntary program and will serve as a disincentive for participation.

We strongly urge AICPA to assure that the product not be designed in a fashion that can be misapplied by well meaning, but misguided government officials who misunderstand the nature of the problem and continue to think of the cyber assessments as audits. We are unfortunately already experiencing substantial misuse of propertied voluntary measures such as the NIST Framework, which even senior federal officials have acknowledged is being misapplied in regulatory contexts thus undermining the effectiveness of the Framework and the necessary trust that will be required to create a sustainably secure system. We urge the AICPA to aggressively guard against the misuse of their cyber assessment efforts.

6. We need to assure there will be adequate Talent Availability to perform the assessments

We believe the AICPA's proposal needs to be clear on the qualifications of the engagement team performing the examination. With the critical shortage of qualified cyber talent nationwide, it would be important for the AICPA to work with their membership to ensure that appropriately qualified professionals are in the marketplace. This may require coordinated efforts with members of the academic community and other stakeholders.

While we appreciate the profession's desire to move to market and address a growing need with a well-designed product, we must caution against sending a well-designed product into the field without sufficient and adequately clear expectation of the engagement team make-up. It is in the client's interest to have well trained professionals – in cybersecurity – as the front-line army for this program.

ISA is open to working with the AICPA and the CAQ to design a training program that will ensure personnel performing cyber assessments receive quality training equal in quality to the tool itself. ISA companies may even be willing to offer themselves as "test runs" for the assessment once it gets to a pilot phase. One element of the process that ought to be considered is creating a 360 review of the assessment by both the assessors and the clients, much like modern human resource programs use for employee evaluations. Such a process would engender learning on both sides and help build long-term trust in the process and the cyber assessment itself.

Sincerely,

Larry Clinton

Larry Clinton
President/CEO
Internet Security Alliance

APPENDIX – ADDITIONAL COMMENTS FROM ISA SPONSOR COMPANIES

ISA received additional comments from its members that could not be fully vented with the Association due to time constraints. Nevertheless, ISA finds these comments worthy of AICPA's consideration and thus have provided them in the following appendix:

- ISA sponsor companies applaud the effort AICPA has undertaken, however given the extensive detail provided in the exposures and the comparatively limited time to comment, several entities have informed us they simply have been unable to give the exposures the degree of attention they deserve. These organizations have noted that extending the time for filing comments might generate more feedback which will improve both the quality of the service and its attractiveness to potential users.

- The AICPA is trying to encourage a higher level of maturity in cybersecurity risk management and therefore consideration should be given to the accounting firm assigning a maturity level so that management can easily determine and assess their maturity level.

- AICPA is encouraging this as a means to provide comparability between organizations, however, there is no maturity levels or means of benchmarking the effectiveness of a cybersecurity risk program.

- The AICPA should consider utilizing more granular requirements to ensure a minimum level of effectiveness of their cybersecurity risk management program. As written, there is a lack of specificity such as requiring annual pen tests, quarterly vulnerability scans, annual review of risk program, etc. In addition, similar application should be applied to the control framework utilized to ensure effectiveness of the risk program. Lack of such benchmarks allows organization to potentially appear to have a more robust program when they may not meet a minimum level of control objectives such as minimum passwords, complexity, histories and other control aspects as mentioned earlier.

- Allows the organization to utilize their own control framework to ensure the effectiveness of their cybersecurity risk framework. Thus, the organization could leverage new SOC 2 criteria, ISO 27K, PCI, NIST, etc versus utilizing the revised framework proposed by the AICPA.

- AICPA intends for this to be utilized externally for customers and in their supply chain. However, some information required by the description criteria (DC) can be viewed as too sensitive for external distribution. For example, and most concerning, would be DC8 which requires reporting of incidents incurred, nature and extent of associated loss, etc. This information would be valuable for Boards and Executive Management but could easily be misused or misinterpreted if shared externally.

- Use of COSO framework imposes challenges for smaller organizations that an organization could partner with or in their respective supply chain. Has a strong focus on management level control and formalities that creates potential hurdles for this framework to be effective throughout these relationships. Again, use of maturity levels would help address this issue

- DC2 should have a stronger focus on third party contracts to help ensure necessary commitments to help minimize risk to the organization.

- DC4 should include a process to evaluate cybersecurity objectives on a routine basis.
- DC6 focuses on internal threats and not so much on external threats.
- DC15 points of focus should include consideration of establishing a threat reporting process.
- DC16 points of focus should include consideration of the use of new technologies.
- Lack of criteria that focuses of cloud vendor relationships.
- Lack of criteria that focuses on use of encryption and its application with third party relationships.