Association of Local Government Auditors

December 5th, 2016

Mimi Blanco-Best
AICPA Assurance Services Executive Committee (ASEC)

RE: AICPA ASEC *Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* Exposure Draft

Ms. Blanco-Best,

The Association of Local Government Auditors (ALGA) appreciates the opportunity to respond to the ASEC's *Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*. ALGA represents more than 340 audit organizations and over 2,200 members. This topic is of interest to our members, and we encourage individual audit organizations and members to comment independently should they choose to do so.

We have reviewed the proposed exposure draft in its entirety. Overall, we feel that the proposed description criteria would provide useful guidance for organizations to assess and describe their cybersecurity program. We appreciate that the guidance requires organizations to develop a risk management plan based on their organizational objectives.

We offer the following comments which we believe will improve the description criteria and provide clarification on cybersecurity risk management as well as the assignment of related roles within the organization. We answered each of the questions in the *Guide for Respondents* and listed the description criterion to which it relates.

1. <u>Are there any unnecessary or otherwise not relevant description criteria or points of focus?</u>
   No comments

2. <u>Are there any missing description criteria or points of focus?</u>
   DC2: (*Page 18*)
   Bullet 3 – We recommend adding "financial" to the list of information whose integrity is critical to organizations.

   DC13: *(Page 24)*
   Bullet 2 – We recommend adding "and organizational policies", after the phrase "employee compliance with their responsibilities".

DC14: *(Page 24)*
This description criterion is about the process for identifying risks to the achievement of the entity's cybersecurity objectives and assessing risks to determine how such risks should be managed. However, the points of focus do not address how these risks should be managed. The management of risks through cybersecurity control activities are discussed later in DC22 to DC24 *(page 28)*. It may be more fitting to title this criterion as "The process for identifying and assessing risks to the achievement of the entity's cybersecurity objectives".

DC21: *(Page 27)*
It appears that this description criterion is based on Principle 17 of the COSO Internal Control Integrated Framework. COSO Principle 17 contains the following three points of focus:

- Assesses results: Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
- Communicate deficiencies: Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
- Monitors corrective actions: Management tracks whether deficiencies are remediated on a timely basis.

The point of focus for DC21 includes bullets 1 and 2 from Principle 17 – assessing and communication. They do not address monitoring though. Monitoring of corrective actions is necessary to ensure that identified security threats, vulnerabilities, and control weaknesses are remediated on a timely basis.

3. 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?
   No comments

4. Do you have any concerns about the measurability of an y of the description criteria or points of focus? Please provide a list.
   The following important items are highlighted within the description criteria. Measuring them may be difficult without additional guidance:

   - How often a risk assessment should be performed (DC10, DC16)
   - Time frame to implement program (DC10)
   - Improved results, better communications (DC8)

5. Use of the criteria does not require management to address every point of focus in its description. Do you believe this approach is appropriate?
   We believe it's appropriate to allow management to evaluate and determine how relevant each point of focus is to their cybersecurity program. Still, management should be able to explain to their auditors why they believe a point of focus is not applicable.

Respectfully submitted,

Larry Stafford
Chair, Professional Issues Committee

Key ALGA Contributors:
Neha Sharma, City of Austin, TX
April Jordan, Shreveport, LA