Q&A Section 9550

Performing a Third-Party Assessment Engagement Under a Third-Party Assessment Program

.01 Defining a Third-Party Assessment Program

Inquiry — What is a third-party assessment program?

Reply — A federal or state governmental agency, industry consortium, or group of subject matter experts (referred to as a *program body*[1]) may determine that it needs certain information about a specific subject matter (for example, security controls over sensitive information) from its members or other entities with whom it does business, such as contractors, vendors, or customers. For that purpose, the program body may develop a third-party assessment program that establishes requirements or instructions for entities to provide the requested information to the program body, along with an evaluation performed by a third-party "assessor." The assessor's evaluation is used by the program body to determine whether to provide the entity a certification, authorization, or other form of approval.

A third-party assessment program encompasses the following characteristics:

- Identifies publicly available criteria to be used to measure or evaluate the subject matter (often referred to as a *framework*). Often, the program body follows due process procedures, including exposure of the framework for public comment. Because the program body develops the framework or incorporates an existing framework into the third-party assessment program, the framework is deemed appropriate by the program body to meet the objective of its third-party assessment program.

- Requires the subject matter to be measured or evaluated against the framework identified in the third-party assessment program. The third-party assessment program may also require the entity to perform a self-assessment. The entity is responsible for the subject matter and, if applicable, its assessment of the subject matter based on the framework.

[1] For example, HITRUST, the Federal Risk Authorization Management Program (FedRAMP), and U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC).

- Approves an individual or organization as an assessor under the third-party assessment program, based on certain educational or experience requirements, and may establish guidelines for evaluating the quality of the assessor's work. The third-party assessment program also includes requirements regarding the assessor's objectivity or independence as defined by the program. Generally, both non-CPAs and CPAs can be hired as assessors.

- Requires a third-party assessor to comply with the requirements or instructions in the third-party assessment program, such as the procedures to be performed and the method to be used to communicate the results of those procedures to the program body (for example, through an online portal).

The absence of one or more of the preceding characteristics may indicate that a particular program does not qualify as a third-party assessment program to which this question and answer applies.

In addition to the characteristics described previously, a third-party assessment program may set out specific requirements or instructions relating to the following:

- The frequency of the assessment and the evaluation of findings, including materiality considerations
- The availability of the assessor's report to others beyond the program body

[Issue Date: January 2021.]

.02 Performing a Third-Party Assessment Engagement in Accordance With Standards Promulgated by Bodies Designated by Council

Inquiry — In a third-party assessment engagement, an assessor typically performs procedures outlined in the third-party assessment program and communicates the procedures performed and results determined or the conclusions reached by following the requirements or instructions under the third-party assessment program. An entity may request a member to act as an assessor in connection with a third-party assessment program. In such circumstances, the member is required to apply which professional standards to the third-party assessment engagement?

Reply — A third-party assessment engagement constitutes a professional service. When performing a professional service, the member is required to comply with the AICPA Code of Professional Conduct (AICPA code), including the "General Standards Rule" (ET sec. 1.300.001). Specifically, that rule requires members to comply with the following standards:

a. Professional Competence. Undertake only those professional services that the member or the member's firm can reasonably expect to be completed with professional competence.

b. Due Professional Care. Exercise due professional care in the performance of professional services.

c. Planning and Supervision. Adequately plan and supervise the performance of professional services.

d. Sufficient Relevant Data. Obtain sufficient relevant data to afford a reasonable basis for conclusions or recommendations in relation to any professional services performed.

The member performing a third-party assessment engagement is always required to comply with the AICPA code and the requirements or instructions of the third-party assessment program. In addition, the member

- if engaged to issue, or does issue, a practitioner's examination, review, or agreed-upon procedures report in connection with the third-party assessment engagement, is required to perform the engagement in accordance with Statements on Standards for Attestation Engagements (SSAEs).[2]
- may apply the Statement on Standards for Consulting Services when performing the third-party assessment engagement.

Any reports issued by the member other than reports issued under the SSAEs are written to be clearly distinguishable from and not confused with reports issued under the SSAEs.

In addition, members are to remain mindful of the various independence requirements that apply when performing third-party assessment engagements.

- The third-party assessment program typically includes requirements regarding the assessor's independence as defined by the program.
- The "Independence Rule" (ET section 1.200.001) of the AICPA code and its interpretations apply to attest engagements. A member is not required to be *independent* as defined by the "Independence Rule" to perform a third-party assessment engagement unless the member performs the engagement in accordance with the SSAEs or as described in the following bullet.
- When the third-party assessment engagement is not performed as an attest engagement, the engagement is considered a nonattest service. If a member performs another engagement that requires independence for the entity (for example, a financial statement audit), in order to maintain independence, the safeguards described in the "Nonattest Services" subtopic of the "Independence Rule" (ET sec. 1.295) must be applied when performing the third-party assessment engagement as a nonattest service.

[Issue Date: January 2021.]

[2] Paragraph .01 of AT-C section 105A, *Concepts Common to All Attestation Engagements*.