Appendix E

Illustrative Management Assertion in the Cybersecurity Risk Management Examination

This illustration is nonauthoritative and is included for informational purposes only.

[*ABC Entity's Letterhead*]

Assertion of the Management of ABC Entity

Introduction

We have prepared the accompanying description of ABC Entity's cybersecurity risk management program titled [*insert title of management's description*] throughout the period [*date*] to [*date*] (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in [*name of the description criteria, e.g., AICPA* Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program] (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established ABC Entity's cybersecurity objectives, which are presented on page ___ of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Assertion

We assert that the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls within the cybersecurity risk management program throughout the period [*date*] to [*date*] using the [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set*

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period [*date*] to [*date*] to achieve the entity's cybersecurity objectives based on the control criteria.
