Illustrative SOC 2® Type 2 Management Assertion on its description of a Service Organization’s System and the suitability of design and operating effectiveness of controls relevant to the Trust Services Criteria for Security, Availability, and Confidentiality and the HITRUST CSF Criteria

Illustrative Assertion by Service Organization Management

 [*ABC’s Service Organization Letterhead*]

**Assertion of ABC Service Organization Management**

We have prepared the accompanying description of ABC’s insurance claims processing system titled “Description of Insurance Claims Processing System” throughout the period January 1, 20X1, to December 31, 20X1” (description) based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2**® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the insurance claims processing system that may be useful when assessing the risks from interactions with ABC’s system, particularly information about system controls that ABC has designed, implemented, and operated to provide reasonable assurance that its service commitments and systems requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*,and the implementation requirements set forth in the HITRUST CSF version X [would replace X with corresponding HITRUST CSF version number] that are applicable to ABC’s insurance claims processing system required for a [*select the appropriate assessment type:* *HITRUST CSF Security Assessment, HITRUST CSF Security and Privacy Assessment, HITRUST CSF Comprehensive Security Assessment, or HITRUST CSF Comprehensive Security and Privacy Assessment*] (applicable HITRUST CSF criteria)***.***

The organization is classified as an insurance payor covering 20 million members; applicable HITRUST requirements have been determined based on the characteristics of the entity described in subsection xxx of the description.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the service organization, to achieve ABC’s service commitments and system requirements based on the applicable trust services criteria. The description presents ABC’s controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of XYZ’s controls.

We confirm, to the best of our knowledge and belief, that

*a.* the description presents ABC’s insurance claims processing system that was designed and implemented throughout the period January 1, 20X1, to December 31, 20X1, in accordance with the description criteria.

1. The controls stated in the description were suitably designed throughout the period January 1, 20X1, to December 31, 20X1, to provide reasonable assurance that ABC‘s service commitments and system requirements would be achieved based on the applicable trust services criteria and HITRUST CSF criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of ABC’s controls throughout that period.
2. the controls stated in the description operated effectively throughout the period January 1, 20X1, to December 31, 20X1, to provide reasonable assurance that ABC’s service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria, if complementary user entity controls assumed in the design of ABC’s controls operated effectively throughout that period.

Signature

Title

*Illustrative SOC 2® Type 2 Independent Service Auditor’s Report on a Description of a Service Organization’s System and the Suitability of Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality and HITRUST CSF Criteria*

**Independent Service Auditor’s Report**

To: ABC Service Organization

*Scope*

We have examined ABC Service Organization’s (ABC’s) accompanying description of its insurance claims processing system titled “Description of Insurance Claims Processing System” throughout the period January 1, 20X1, to December 31, 20X1,(description) based on the criteria for a description of a service organization’s system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20X1, to December 31, 20X1, to provide reasonable assurance that ABC’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the implementation requirements set forth in the HITRUST CSF version x that are applicable to ABC’s insurance claims processing system required for a [*select the appropriate assessment type:* *HITRUST CSF Security Assessment, HITRUST CSF Security and Privacy Assessment, HITRUST CSF Comprehensive Security Assessment, or HITRUST CSF Comprehensive Security and Privacy Assessment*] (applicable HITRUST CSF criteria).

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ABC, to achieve ABC’s service commitments and system requirements based on the applicable trust services criteria. The description presents ABC’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ABC’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

*Service organization’s responsibilities*

ABC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ABC’s service commitments and system requirements were achieved. In section 1, ABC has provided its assertion titled, “Assertion of ABC Service Organization Management” (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. ABC is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

*Service auditor’s responsibilities*

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves the following:

* Obtaining an understanding of the system and the service organization’s service commitments and system requirements
* Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
* Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
* Performing procedures to obtain evidence about whether controls stated in the description were suitability designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF criteria
* Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF criteria
* Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

*Inherent limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria and HITRUST CSF criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

*Description of tests of controls*

The specific controls we tested, and the nature, timing, and results of those tests are listed in section XX.

*Opinion*

In our opinion, in all material respects,

*a.* the description presents ABC’s insurance claims processing system that was designed and implemented throughout the period January 1, 20X1, to December 31, 20X1, in accordance with the description criteria.

*b.* the controls stated in the description were suitably designed throughout the period January 1, 20X1, to December 31, 20X1, to provide reasonable assurance that ABC’s service commitments and system requirements would be achieved based on the applicable trust services criteria and HITRUST CSF criteria, if its controls operated effectively throughout that period and user entities applied the complementary controls assumed in the design of ABC’s controls throughout that period.

*c.* the controls stated in the description operated effectively throughout the period January 1, 20X1, to December 31, 20X1, to provide reasonable assurance that ABC’s service commitments and system requirements would be achieved based on the applicable trust services criteria and HITRUST CSF criteria, if complementary user entity controls assumed in the design of ABC’s controls operated effectively throughout that period.

*Restricted use*

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of ABC, user entities of ABC’s insurance claims processing system during some or all of the period January 1, 20X1, to December 31, 20X1, business partners of ABC subject to risks arising from interactions with the insurance claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

* + - The nature of the service provided by the service organization
		- How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties
		- Internal control and its limitations.
		- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements
		- User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services
		- The applicable trust services criteria and HITRUST CSF criteria.
		- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

*Service auditor’s signature*

*Date of the service auditor’s report*

*Service auditor’s city and state*