

Illustrative Management Assertion and Service Auditor's Report for a SOC 3[®] Examination

This publication is nonauthoritative and is provided for informational purposes only.

In the following illustrative management assertion and service auditor's report, ABC Service Organization has engaged the service auditor to (a) examine the controls within the system relevant to security, availability, and confidentiality and (b) issue a SOC 3[®] report that can be posted on its website to encourage prospective customers to contract the service organization's services.

Illustrative Assertion by Service Organization Management

ABC Service Organization's Letterhead

Assertion of ABC Service Organization Management

We are responsible for designing, implementing, operating, and maintaining effective controls within ABC Service Organization's (ABC's) Chatbot System (system) throughout the period

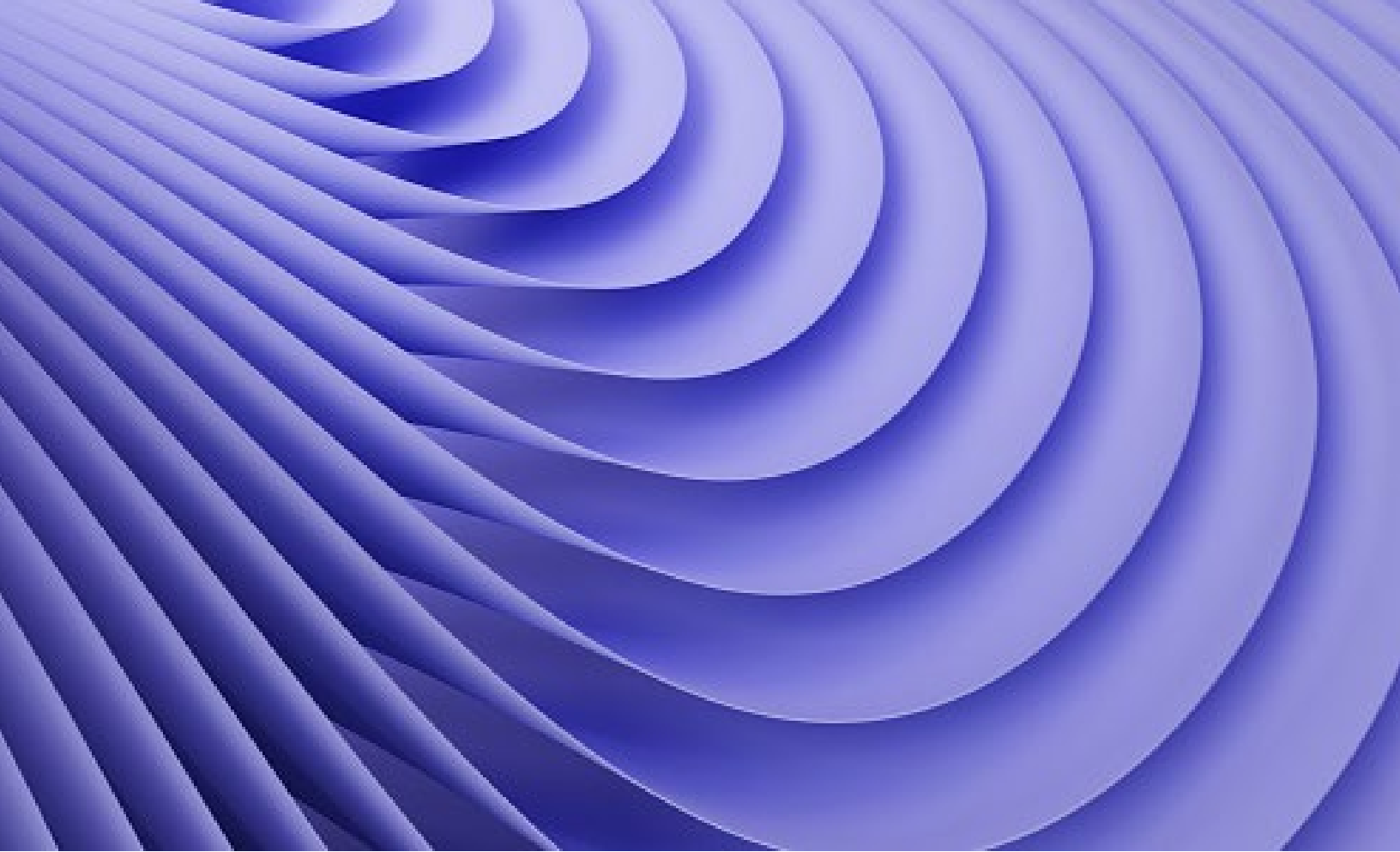
January 1, 20XX to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in [TSP section 100](#), *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria.^{fn 1} Our description of the boundaries of the system is presented in [attachment A](#) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 20XX to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria. ABC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in [attachment B](#).

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 20XX to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria.

^{fn 1} The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*. Because points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.



Attachment A

Note to Readers: *The following description of the boundaries of the system is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in a description of the boundaries of the service organization's system.*

ABC Service Organization's Description of the Boundaries of ABC's Chatbot System

Services Provided

ABC Service Organization, Inc. (ABC or the Company) provides a world-wide cloud-based software application. The Company was founded in 2019 to connect businesses to their respective customers through automated means. The ABC Chatbot System provides a customer interaction system to supplement the Company's processing system.

This description details the ABC Chatbot System and the related policies, procedures, and control activities for the ABC Chatbot System. This description does not include any other ABC services.

The system described herein is bounded by the specific aspects of ABC's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers, and the data that is processed by the system. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. The components that directly support the services provided to user entities are as follows:

Note to Reader: *A diagram or other graphic may also be provided.*

Infrastructure

The system's infrastructure is Windows-based and is hosted in ABC data center located in [city and state where data center is located]. The ABC backup data center is located in [city and state where backup data center is located] in support of availability commitments.

Software

The software component consists of the applications, programs, and other software that support the system. The list of software and ancillary software used to build, support, secure, maintain, and monitor the ABC Chatbot System are as follows: provide its services and that directly support the services provided to customers, and the data that is processed by the system. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. The components that directly support the services provided to user entities are as follows:

Production Application	Business Function
XYZ app software	Application monitoring for load and uptime performance.
XYZ logging system	SIEM/Logging system that provides log management and analytics that leverage machine-generated data to deliver real-time IT insights.
XYZ watch application	Infrastructure monitoring and analytics tool for IT and DevOps teams that can be used to determine performance metrics as well as event monitoring for infrastructure and cloud services.
XYZ patching tool	Patch management tool that can plan, manage, and deploy updates, patches, and hotfixes for Windows servers, client operating systems, and other Microsoft software.
XYZ file integrity platform	File integrity monitoring platform used to deliver security, monitoring, forensics, and collection of metrics about the environment.
XYZ anti-virus program	Anti-virus program that scans computers for security threats, prevents unapproved programs from running, and applies firewall policies that block or allow network traffic.

Production Application	Business Function
XYZ help application	Software application used for issue tracking and project management.
XYZ data loss prevention software	Data loss prevention software used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.
XYZ version control tool	Version control and DevOps tool used for source code management used to track changes in the source code.
XYZ IDS application	Intrusion detection system used to provide visibility into endpoint vulnerabilities by gathering data needed to identify, understand, and respond to attacks.

People

ABC has various personnel groups that directly support the ABC Chatbot System. The responsibilities of these groups are defined in the following table:

Group/Role Name	Business Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the ABC Chatbot System.
Software Product Management	Responsible for the software product life cycle, including adding additional product functionality.

Group/Role Name	Business Function
InfoSec	Responsible for the overall security of the production environment, including evaluation and management of controls and other activities that relate to the ability of the system to meet its service commitments and system requirements. Also responsible for evaluating and managing controls and other activities that prevent, detect, mitigate, and remediate system incidents.
Customer Service	Responsible for resolving issues raised by users of the ABC Chatbot System.
Human Resources	Responsible for onboarding new personnel, defining role or position of new hires, performing background checks, and facilitating the employee termination process.
Operations	Staff that provide the day-to-day services such as monitoring the operation of the chatbot system.

Processes and Procedures

ABC has developed and communicated policies and procedures involved in the operation of the ABC Chatbot System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system and facility access, auditing, configuration management, breach or incidents, disaster recovery, intrusion detection, vulnerability assessment, data integrity, vendor management, and so on. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business, but no less than once annually.

Data

Data related to the ABC Chatbot System consists of chatbot message streams. The chatbot may also access transaction streams, files, data stores, tables, and output used or processed by ABC.

Production Application	Description	Data Store
Chatbot scripts and algorithms	The chatbot responds to questions using pre-programmed scripts and machine learning algorithms.	XYZ knowledge database
Usage information	ABC keeps track of user activity in relation to the types of services users and their customers use, the configuration of their computers, and performance metrics related to their use of the ABC service.	XYZ databases
User and account data	ABC collects data from its employees, customers, customers' employees, and other third parties, such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Via the platform, ABC customers define and control the data they load and store in the ABC Processing System production network. Customer data is loaded into the system and accessed remotely by customers via the internet and by the chatbot system.	XYZ knowledge database

Production Application	Description	Data Store
Log information	ABC logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.	XYZ knowledge database



Attachment B

Note to Readers: *The following description of the service organization's principal service commitments and system requirements is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include a full list of principal service commitments and system requirements.*

Principal Service Commitments and System Requirements

ABC designs its processes and procedures related to the ABC Chatbot System to meet its objectives for its chatbot services. Those objectives are based on the service commitments that ABC makes to its customers, business partners, and vendors, and the operational and compliance requirements that ABC has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the ABC Chatbot System. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and include the following:^{fn 2}

- Commitments regarding the security and availability of the system and confidentiality of information processed by the system in accordance with contractual stipulations.
- Commitments regarding customer interactions as described in the master service agreement, service level agreement, and the system reference document.
- Commitments to support customer compliance with the security-related requirements of the EU General Data Protection Regulation, as set forth in the master services agreement.
- Chatbot message streams are retained for no more than 24 hours after the chat is initiated.

ABC establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements. These include system requirements (both functional and non-functional) derived from service commitments, published documentation of system functionality, and other descriptions of the system.

Such requirements are communicated in ABC's system policies and procedures, system design documentation, and contracts with customers.

^{fn 2} Service commitments are commonly reflected in existing documents, such as service level agreements, available to customers and business partners. In most situations, rather than including a reference to the principal service commitments in these existing documents, management would list the individual commitments in the description.

ABC has adopted the NIST Cybersecurity Framework as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the ABC Chatbot System. System requirements based on the NIST Cybersecurity Framework include the following:

- Data, personnel, devices, systems, and facilities are identified and managed.
- ABC management understands and manages the cybersecurity risk to organizational operations.
- ABC's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance and repairs of information system components are performed consistent with policies and procedures.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- Recovery processes and procedures are executed and maintained to help ensure restoration of systems or assets affected by cybersecurity incidents.



Illustrative Independent Service Auditor's SOC 3 Report

Independent Service Auditor's Report on a SOC 3 Examination ^{fn 3}

To: Management of ABC Service Organization

Scope

We have examined ABC Service Organization's (ABC's) accompanying assertion titled "Assertion of ABC Service Organization Management" (assertion) that the controls within ABC's Chatbot System (system) were effective throughout the period January 1, 20XX to December 31, 20XX, 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*, in *AICPA Trust Services Criteria*.

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. ABC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ABC is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

^{fn 3} The report may also be titled "Report of Independent Service Auditors."

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve ABC's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ABC's service commitments and system requirements based on the applicable trust services criteria

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

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 their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within ABC's Chatbot System were effective throughout the period January 1, 20XX to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

[Service auditor's signature]

[City and state where the report is issued]

[Date of the service auditor's report]





P: 888.777.7077 | F: 800.362.5066 | W: aicpa-cima.com

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

© 2022 Association of International Certified Professional Accountants. All rights reserved. AICPA and American Institute of CPAs are trademarks of the American Institute of Certified Public Accountants and are registered in the US, the EU and other countries. SOC 1®, SOC 2® and SOC 3® trademarks are registered trademarks of the AICPA. The Globe Design is a trademark of the Association of International Certified Professional Accountants and licensed to the AICPA. 2210-661720