



Ansys, Inc.

**System and Organization
Controls Report**

September 1, 2020 Through December 31, 2020

Deloitte.



Independent Service Auditor's Report

To Ansys, Inc
Canonsburg, PA 15317

Scope

We have examined Ansys, Inc. (the "Service Organization" or "Ansys") accompanying assertion titled "Assertion of Ansys" ("assertion") that the controls related to the Ansys Cloud system were effective throughout the period September 1, 2020 to December 31, 2020 (the "description"), to provide reasonable assurance that Ansys' 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*.

The description of the boundaries of the system indicates that certain applicable trust services criteria specified in the description of the boundaries of the system can be met only if complementary user-entity controls contemplated in the design of Ansys' controls are suitably designed and operating effectively, along with related controls at Ansys. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Ansys uses Microsoft Azure ("Azure") for public cloud infrastructure service and Rackspace Technology ("Rackspace") for managed cloud service (collectively "subservice organizations"). The description of the boundaries of the system indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system presents the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period September 1, 2020 to December 31, 2020.

Service Organization's Responsibilities

Ansys 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 Ansys' service commitments and system requirements were achieved. Ansys has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Ansys is responsible for selecting, and identifying in its assertion, the applicable trust service 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 whether 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 American Institute of Certified Public Accountants. 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.

Our examination included:

- 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 Ansys' 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 Ansys' service commitments and system requirements based 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 over the Ansys Cloud system were effective throughout the period September 1, 2020 to December 31, 2020, to provide reasonable assurance that Ansys' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The logo for Deloitte + Touche LLP, featuring the company name in a stylized, handwritten font.

July 8, 2021

Assertion of Ansys, Inc.

We are responsible for designing, implementing, operating and maintaining effective controls over the Ansys Cloud system throughout the period September 1, 2020 to December 31, 2020 to provide reasonable assurance that Ansys' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A below and identifies the aspects of the system covered by our assertion.

Ansys uses Microsoft Azure ("Azure") for public cloud infrastructure service and Rackspace Technology ("Rackspace") for managed cloud service (collectively "subservice organizations"). The description of the boundaries of the system includes only controls and applicable trust services criteria of Ansys and excludes controls and applicable trust services criteria of the subservice organizations. The description of the boundaries of the system indicates that the applicable trust services criteria specified in the description can be achieved only if controls at the subservice organizations contemplated in the design of Ansys' controls are suitably designed and operating effectively, along with the related controls at Ansys. We have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2020 to December 31, 2020, to provide reasonable assurance that Ansys' 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*. Ansys' 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 below.

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 September 1, 2020 to December 31, 2020 to provide reasonable assurance that Ansys' service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Ansys' Description of the Boundaries of the Ansys Cloud system

REPORT SCOPE

This report addresses the controls related to Ansys Cloud service relevant to the security, availability, and confidentiality of the Ansys Cloud system.

OVERVIEW OF THE ORGANIZATION & SERVICES

Company History

Ansys, Inc. ("Ansys") is an international public company founded in 1970. Ansys develops, markets, and supports software solutions for design analysis and optimization. Ansys' software accelerates product time to market, reduces production costs, improves engineering processes, and optimizes product quality and safety for a variety of manufactured products. Ansys' product suites include, but is not limited to: Ansys Workbench, High-Performance Computing (HPC), Structural Analysis, Fluids, Electromagnetics, Semiconductors, Embedded Software, System Stimulation, 3D Design, Optical Sensor and Closed-Loop Real Time Simulation, Material Intelligence, and Academic Product suites. Additionally, Ansys focuses on the development of open and flexible solutions that enable users to analyze designs directly on the consumer's desktop, providing a common platform for fast, efficient and cost-conscious product development. Ansys operates via a hybrid sales and distribution model by distributing its suite of simulation technologies through a global network of independent resellers and distributors (collectively, channel partners) and direct sales offices in strategic, global locations. The primary software and technologies developed by Ansys are widely used by engineers, designers, researchers, and students across a broad spectrum of industries and academia. These industries and academia include aerospace and defense, automotive, electronics, semiconductors, energy, materials and chemical processing, turbomachinery, consumer products, healthcare, and sports.

OVERVIEW OF OPERATIONS RELATED TO THE SYSTEM

Scope

Ansys provides services to user entities including the right to access the Ansys Cloud software as a service for high performance computing. The following description is intended for the customers of Ansys' Cloud system to provide them with information concerning the control environment as it relates to the in-scope trust services (security, availability, and confidentiality) at Ansys. The aim of this description is to provide the customers an adequate degree of understanding of IT processes and internal controls as they relate to the services provided by Ansys.

The description is intended to focus on certain features that are relevant to the internal controls provided to user organizations; it does not encompass all aspects of services provided or procedures followed for all user organizations nor any aspect of any business process or application processed for user organizations except as it relates to the areas described above. Further, this report does not provide information or coverage over services performed by Azure for cloud infrastructure services, or Rackspace for managed cloud services. As such, further information regarding other services and operations provided by Ansys is not provided. The description that follows outlines the processes and controls that are performed by Ansys for its customers.

SYSTEM DESCRIPTION

The system is comprised of the following components:

- **Software:** The IT application software that supports IT system functionality.
- **Infrastructure:** The resources which support the overall IT environment, including physical environment and related structures, IT, and hardware.
- **People:** The personnel involved in the governance, operation, and use of a system.
- **Data:** Transaction streams, files, databases, tables and output used or processed by a system.
- **Procedures:** The manual and automated processes performed to enable IT system functionality

Software

The software used at Ansys to deliver services to its customers includes the Ansys Account and Ansys Cloud platforms. The Cloud and Platform department maintains a master list of information assets that defines key system components and versions. The following is a description of the primary applications and main processes that are in-scope for this report:

Software	Description
Ansys Account	Central gateway that connects and manages application programming interface (API) communications between the systems within the Ansys Cloud and manages user account data.
Ansys Cloud	Primary application used by user entities to access, process, and store data via the Ansys Cloud.
Azure Portal (IAM)	Azure Portal provides a framework software development kit (SDK), telemetry pipeline and infrastructure for Ansys Cloud to be hosted inside of the Azure portal shell that manages and monitors the required components to allow Ansys Cloud to run in a single, unified console.

Infrastructure

The Ansys Cloud system is a multi-tenant service hosted by Microsoft Azure (“Azure”). The Cloud system is divided into two separate applications: Ansys Account and Ansys Cloud, with the Ansys Cloud application being the main system utilized by user entities. The Ansys Cloud application includes the following tiers:

- **Client Layer** - consists of a web-based portal and the Ansys Cloud Extension which is integrated with the Ansys desktop applications (e.g. Fluent, Mechanical) and desktop utilities including the Command Line Interface and File Transfer Agent
- **Application Layer** - consists of the Ansys Cloud Service (front-end), including the Ansys Cloud portal, and Azure Batch (back-end). Ansys Cloud Service is responsible for authentication and for processing input parameters in order to define a workflow to be processed by Azure Batch.
- **Storage Layer** - consists of Azure Storage, where the Azure Batch will download input data files from Azure Storage, process the models as specified by the workflow, and upon completion, upload the output data to Azure Storage.

Controls over the infrastructure hosted and managed by Azure are not included within the scope of this report. The Ansys Cloud department has shared responsibilities for configuring the relevant infrastructure components within the Azure environment supporting the Cloud system.

People

Ansys has approximately 4,800 employees, including contractors, and is headquartered in Canonsburg, Pennsylvania with operations in 50+ countries across three continents. Ansys has an established and formally defined organizational structure with assigned responsibilities to document, communicate and enforce accountability of Company objectives. The organizational structure is automatically updated by the HR system daily.

Data

Ansys has policies and procedures that define how confidential information should be received, stored, and distributed. Customer data is held in accordance with requirements set out in customer contracts, in which all customer data is considered confidential. In addition, customer data types that are required to be obtained in order for services to be provided via the Ansys Cloud are documented within the Ansys policies and procedures that are available company-wide via PolicyTech. Customer data is limited to authorized users only. Formal data retention and disposal procedures are in place to guide the timely and secure disposal of customers' data. By request, Ansys destroys customers' data in alignment with policies and contractual requirements.

Procedures

The Ansys Cloud and Platform department is responsible for supporting the Cloud IT system environment including the system and network infrastructure. Services provided by the Cloud and Platform department include enhancing, configuring, and monitoring the Ansys Cloud environment to allow for daily operations to go uninterrupted. Ansys' Information Security and Cybersecurity policies and procedures support management directives by clearly documenting key processes and establishing expectations and accountability for system usage, maintenance, and processing information utilized in control operations across the environment. Policies and procedures are reviewed, updated, and approved on an annual basis.

Complementary Subservice Organization Controls (CSOC)

Ansys’ controls related to the Ansys Cloud system cover components of overall internal controls for each user entity of Ansys. Each subservice organization’s controls must be contemplated in conjunction with Ansys’ controls and the related tests and results as described in Section IV of this report, considering the related complementary subservice organization controls (“CSOCs”) expected to be implemented at the subservice organizations as described below.

Criteria Reference	Complementary Subservice Organization Controls
CC6.1, CC6.3, CC6.5, CC6.6	Subservice organizations are responsible for maintaining logical security over the in-scope infrastructure components and hardware devices that are relevant to the system.
CC6.4, CC6.5	Subservice organizations are responsible for maintaining physical security over data centers and locations supporting in-scope applications, infrastructure components, networks, and other hardware devices that are relevant to the system.
CC6.7	Subservice organizations are responsible for protecting the transmission, movement, and removal of information relevant to the system.
CC6.8	Subservice organizations are responsible for preventing or detecting and acting upon the introduction of unauthorized or malicious software to meet the entity’s objectives.
CC7.1, CC7.2, CC7.3,	Subservice organizations are responsible for having threat and vulnerability scanning processes and the timely reporting of security incidents or breaches identified within the in-scope infrastructure components.
CC7.4, CC7.5	Subservice organizations are responsible for responding to identified security incidents by executing a defined incident response program to track, contain, remediate, communicate, and recover from security incidents, as appropriate.
CC8.1	Subservice organizations are responsible for verifying that changes relevant to the in-scope infrastructure components are authorized, tested, approved, and implemented appropriately.
A1.2, A1.3	Subservice organizations are responsible for verifying that data relevant to the in-scope infrastructure components are backed up regularly and is available for restoration.

Complementary User Entity Controls (CUEC)

The services provided by Ansys were designed with the assumption that certain controls would be implemented by the user entities. The application of certain controls by the user entities is necessary to achieve certain criteria identified in this report.

This section describes certain controls which the user entities should consider for achievement of certain criteria identified in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls which should be employed by the user entities. User entities and their auditors should consider whether the following controls have been placed in operation:

Criteria Reference	Complementary User Entity Controls
CC6.1, CC6.2, CC6.3	User entities are responsible for establishing appropriate controls over the use of their accounts and passwords.
CC6.1, CC6.2, CC6.6, CC6.7	User entities are responsible for restricting access to Ansys Cloud network connections.
CC6.2	User entities are responsible for reviewing user access to the system and communicating access modifications timely.
CC6.2	User entities are responsible for ensuring the confidentiality of any user IDs and passwords with access to the system.
CC6.2, CC6.3	User entities are responsible for timely notification of accounts requiring deleting/disabling when no longer required.
CC6.2, CC6.3	User entities with local Administrator authorities are responsible for deleting/disabling access to the system when no longer required.
CC6.4	User entities are responsible for appropriately restricting physical access to facilities and terminals used to access the system.
CC7.2, CC7.3, CC7.4	User entities are responsible for reporting any identified issues related to security, availability, or confidentiality.
A1.2	User entities are responsible for backing up its content uploaded to the system.

User entities can also consider the following user entity responsibilities:

- Managing compliance with applicable laws/regulations.
- Implementing workstation timeout for extended periods of inactivity.
- Monitoring the Ansys Cloud forum for alerts regarding system changes, maintenance, and/or incidents.
- Ensuring that their Internet Service Provider offers adequate internet connection for the purpose of utilizing the system.

Attachment B

Principal Service Commitments and System Requirements

Ansys' objectives relate primarily to the achievement of the principal service commitments made to customers related to the system used to provide the services and the principal system requirements necessary to achieve those commitments. Ansys is responsible for designing, implementing, and operating controls to provide reasonable assurance that it achieves the objectives.

Ansys' principal service commitments are based on the needs of user entities and are communicated to user entities in the form of Service Level Agreements (SLAs), customer agreements/contracts, system design documentation, and/or through the description of policies and practices outlined on Ansys' web portals. Service commitments include, but are not limited to, the following:

- Security - Ansys has made commitments related to security protections to secure customer data. These commitments are addressed through measures including authentication configurations, data encryption, logical restricted access, and other relevant security controls.
- Availability - Ansys has made commitments related to percentage available as well as commitments related to subscription credits for instances of unavailability.
- Confidentiality - Ansys has made commitments related to maintaining the confidentiality of customer's data through data classification, retention, and destruction policies, encryption, and other relevant security controls. Ansys has made a commitment to provide Customer access to data for 30 days after termination or expiration.

To support the service commitments to user entities, Ansys has implemented an internal control structure designed to achieve its objectives related to the effectiveness and efficiency of operations, reliability of information reporting, and compliance with applicable laws and regulations. This system of internal control works to support the achievement of Ansys' strategies and related business objectives and is organized into the following categories: control environment, risk assessment, monitoring, information and communication, and control activities. Ansys has also implemented various methods of external communication to support its user entities. Mechanisms are in place to notify user entities of potential operational or security issues that could potentially impact them.

The principal system requirements outline how the system should function to meet Ansys' service commitments. These requirements are specified in Ansys' system policies and procedures and contracts with user entities. These requirements address that logical security protections, including restricting access, use of encryption technologies, monitoring, and data retention and destruction policies, are in place; changes to the system are tested and authorized; and system operations and data are maintained, available, and recoverable. These requirements are further identified and described in the sections below and the associated controls are defined and mapped to the applicable AICPA Trust Services Criteria. The principal service commitments and system requirements drive the operation of the system and the evaluation of whether controls were in place and suitably designed, when considering the applicable Trust Services Criteria