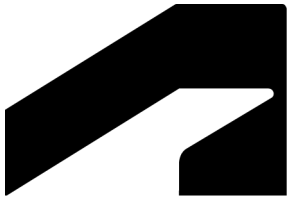

AUTODESK

AUTODESK, INC.

SYSTEM AND ORGANIZATION CONTROLS (SOC3®)

For the period August 1, 2023 to October 31, 2023

Table of Contents

Section I: Independent Service Auditors' Report Provided by KPMG LLP

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

KPMG LLP
Suite 1400
55 Second Street
San Francisco, CA 94105

Independent Service Auditors' Report

Board of Directors of Autodesk, Inc.

Scope

We have examined management of Autodesk, Inc.'s accompanying assertion titled "Management of Autodesk, Inc.'s Assertion" (the Assertion) that the controls within Autodesk, Inc.'s system (the System) were suitably designed and operating effectively throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Autodesk, Inc.'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*.

Autodesk, Inc. uses the subservice organizations identified in management of Autodesk, Inc.'s Attachment A – Management of Autodesk, Inc.'s Overview of Services and the System (Attachment A). Management of Autodesk, Inc.'s Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, Inc., to achieve Autodesk, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Management of Autodesk, Inc.'s Attachment A presents the types of complementary subservice organization controls assumed in the design of Autodesk, Inc.'s controls. Management of Autodesk, Inc.'s Attachment A does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Management of Autodesk, Inc.'s Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, Inc., to achieve Autodesk, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Management of Autodesk, Inc.'s Attachment A presents the complementary user entity controls assumed in the design of Autodesk, Inc.'s System. 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 complementary user entity controls.

Service Organization's Responsibilities

Autodesk, Inc. 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 Autodesk, Inc.'s service commitments and system requirements were achieved. Management of Autodesk, Inc. has provided the accompanying Assertion about the suitability of the design and operating effectiveness of controls within the System. Autodesk, Inc. is also responsible for preparing the Assertion, including the completeness, accuracy, and method of presentation of the Assertion; providing the services covered by the Assertion; selecting, and identifying in the Assertion, the applicable trust services criteria; identifying the risks

that threaten the achievement of Autodesk, Inc.'s service commitments and system requirements; and having a reasonable basis for the Assertion by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on the Assertion that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that Autodesk, Inc.'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 the examination to obtain reasonable assurance about whether the 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 Autodesk, Inc.'s service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve Autodesk, Inc.'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 suitably designed to provide reasonable assurance that Autodesk, Inc. would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- testing the operating effectiveness of controls within the System to provide reasonable assurance that Autodesk, Inc. achieved its 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.

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

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 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.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Opinion

In our opinion, the Assertion that the controls within Autodesk, Inc.'s System were suitably designed and operating effectively throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Autodesk, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

KPMG LLP

San Francisco, California
February 12, 2024

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Section II: Management of Autodesk, Inc.'s Assertion

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Management of Autodesk, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Autodesk, Inc.'s system (the System) throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Autodesk, Inc.'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*. Our description of the boundaries of the System is presented in our Attachment A – Management of Autodesk, Inc.'s Overview of Services and the System (Attachment A) and identifies the aspects of the System covered by the Assertion.

Autodesk, Inc. uses the subservice organizations identified in our Attachment A. Our Attachment A. indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, Inc., to achieve Autodesk, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Our Attachment A presents the types of complementary subservice organization controls assumed in the design of Autodesk, Inc.'s controls.

Our Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, Inc., to achieve Autodesk, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Our Attachment A presents the complementary user entity controls assumed in the design of Autodesk, Inc.'s System.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Autodesk, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. Autodesk, Inc.'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 our Attachment A.

We assert that the controls within the System were suitably designed and operating effectively throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Autodesk, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Sebastian Goodwin

Chief Trust Officer

February 12, 2024

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Attachment A: Management of Autodesk, Inc.'s Overview of Services and the System

AUTODESK

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Corporate Overview

Autodesk, Inc. (“Autodesk” or the “Company”), is a leader in 3D design, engineering, and entertainment software and Autodesk makes software for people who make things.

AUTODESK

System Overview and Services Provided

The scope of this report is applicable to the Autodesk Cloud Products and Infrastructure System (hereafter referred to as “Cloud Services”), BuildingConnected and TradeTapp, and covers the following Software as a Service (“SaaS”) products and platform services, located within Autodesk’s US and European regions. They are collectively referred to as “in-scope products” in this report.

Products	Tools/ Services	
Platform Services Supporting Multiple Autodesk Products	Identity Microservices	Identity Business API
		Authz & PingFederate
		SCIM
		ID Eventing
	• Forge Data Exchange (US and Europe) • Forge API Management Locale • Forge Data Layer 2 File System (US and Europe) • Stargate • ACC Sharelink • ACC AutoSpecs	

Products Tools/ Services	Description
BuildingConnected Pro	Helps general contractors and owners find and qualify the right subcontractors, send custom bid invites, identify the best bid, and centralize communication.
Bid Board Pro	Helps subcontractors win more work by tracking bid invites, staying ahead of due dates, and managing workloads across the entire office—all from one place.
TradeTapp	Proactively analyzes and mitigates project risk by ensuring customers only work with the most reliable, top-level subcontractors with access to over 1 million construction professionals.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Principal Service Commitments and System Requirements

Autodesk designs its processes and procedures related to their in-scope products and platform services to meet security, availability, and confidentiality objectives. Those objectives are based on the service commitments that Autodesk makes to user entities, the laws and regulations that govern the provision of Autodesk's services and the financial, operational, and compliance requirements that Autodesk has established for their services.

AUTODESK

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles and non-negotiables are embedded within the fundamental designs of the system.
- Access provisioning is designed to permit system users access to information they need based on their role in the system and restrict them from accessing information not needed for their role.
- Autodesk commits to securing customer data as part of its in-scope products.
- Autodesk uses encryption technology to encrypt uploaded customer data at rest and in transit.

Autodesk maintains High-Availability and Disaster Recovery procedures. Availability commitments include Autodesk maintaining high-availability architecture and ensuring demonstrating fail-over mechanisms are in place within Autodesk's in-scope products' environment. Autodesk also has a Global Business Continuity Program and disaster recovery plans for the environment within Autodesk's in-scope products.

Autodesk helps protect the confidentiality of customer data by limiting access. Customer data is limited and restricted to authorized individuals. Autodesk has commitments to their customers to delete data upon requests and initiate deletion after 30 days from termination of customer agreements. In addition, upon expiration or termination of a subscription or service, Autodesk will provide its customers with a 30-day period in order to retrieve their data.

The full Terms of Services and Terms of Use which detail Autodesk's commitments to its customers are made available publicly on Autodesk's website.

Components of the System

The components of the Autodesk's in-scope products include the following infrastructure, software, people, procedures, and data elements. The processes are applicable for all the in-scope products and services if not specifically mentioned.

Infrastructure

The above listed products utilize infrastructure provided by the subservice organization, Amazon Web Services, Inc. ("AWS"). AWS manages the virtualization layer and physical security of the facilities in which Autodesk's in-scope products' environment resides. The following is a list of key AWS services that Autodesk's in-scope products use:

- Elastic Compute Cloud ("EC2")
- Elastic Container Service ("ECS")

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

- Identity Access Management (“IAM”)
- Simple Storage Service (“S3”)
- Relational Database Service (“RDS”)
- Virtual Private Cloud (“VPC”)

The controls relating to the physical security, infrastructure maintenance, and network availability of AWS have been carved out of the scope of Autodesk’s SOC 2 Type II report. For additional information on Autodesk’s in-scope products’ use of AWS and other relevant subservice providers, please refer to the section below titled ‘Complementary Subservice Organization Controls.’

Separate network environments are maintained for staging and production. The production networks are logically segregated from other corporate networks, and access is granted only to authorized personnel using unique user identifiers and passwords. Traffic into production networks must traverse a fully redundant fault-tolerant infrastructure, and traffic is denied by default unless explicitly required for business reasons.

Software

Autodesk’s in-scope products encompass applications, supporting operating systems and databases. The following are the key components of Autodesk’s in-scope products along with key supporting software used to provide services for Autodesk’s in-scope products’ user entities:

- **Security and Availability Monitoring Systems**
  - Splunk Enterprise – security monitoring
  - New Relic – availability monitoring
  - SentinelOne – security monitoring and endpoint protection
  - Datadog – availability monitoring
- **Other Key Supporting Software Includes**
  - CrowdStrike (subservice organization) – antivirus / anti-malware solution
  - MS Authenticator Duo (subservice organization) – multi-factor authentication
  - Git / GitHub – centralized source code control system
  - SaltStack – configuration management
  - Jira – document tracking and ticket management system
  - ServiceNow – document tracking and ticket management system
  - Orca (subservice organization) – policy management and vulnerability assessment

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

People

Core functions manage aspects of Autodesk's internal controls to support the security, availability, and confidentiality categories and criteria.

- **Human resources (HR)** – Responsible for HR practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations, training, and development).
    - During the audit period, there were no annual performance assessments between employees and managers. The most recent annual performance assessments between employees and managers occurred in February of 2023.
- **Security and Compliance** – Responsible for risk management and identification, monitoring of security issues and incidents throughout the product delivery infrastructure, and compliance with security frameworks and regulations. The team also develops, documents, and implements security policies, standards, and processes.
- **Engineering** – Responsible for development of Autodesk Services features, including front-end development, back-end development, tool development, infrastructure expansion and automation, security feature development, testing, quality assurance (QA), and staging. The roles that contribute to this effort include reliability engineering, infrastructure engineering, automation engineering, business service engineering, cloud architecture, and a service operation center ("SOC").

Procedures

Autodesk's Security and Compliance team has documented policies and standards to provide guidelines and requirements for management and employees to monitor that security, availability, and confidentiality commitments are met. Relevant policies, standards, and procedures are documented for:

- Information Security Policy
- Acceptable Use
- Access Management
- Security SDLC and Change Management
- Availability Monitoring
- Configuration and System Hardening
- Security SDLC and Change Management
- IT Asset Management
- Business Continuity and Disaster Recovery
- Data Backup and Replication
- Data Classification
- Employee Termination
- Security Incident Management
- Network Security
- Security Risk Management

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

- Security Incident Management
- Security Logging and Monitoring Standard
- Third Party Security Risk Management Standard
- Vulnerability Management

AUTODESK

Data

Data includes electronic data or information uploaded to Autodesk's in-scope products by user entities. Data is considered confidential information for the purposes of this report. Data is protected based on risk throughout its full lifecycle from unauthorized use, loss, or acquisition from an unauthorized party. Security and Compliance has established framework and policies based on legal, statutory and regulatory requirements.

Cryptographic controls are implemented, as deemed necessary by the data classification. Cardholder data must be protected during the transmission, storage, and at rest. Security and Compliance has established framework and policies based on PCI DSS requirements.

Content, a subset of Data, includes files, designs, models, data sets, images, documents, or similar material submitted or uploaded to the in-scope products by user entities; and user entity specific output generated from the in-scope products, if any, based on the user entities own raw data or information. Content is considered confidential information for the purposes of this report.

Customers (also referred to as "user entities") maintain ownership of and responsibility for their Content and responsibility for their conduct while using Autodesk's in-scope products. Autodesk's in-scope products provide the ability to create, submit, post, or otherwise make Customer Content available to Autodesk and / or others. Autodesk personnel will not access Customer Content except (a) as part of providing, maintaining, securing, or modifying in-scope products, (b) at the Customer request or with Customer consent as part of addressing or preventing a service, support or technical issue, or (c) in connection with legal obligations or proceedings.

Autodesk also maintains internally generated information and configuration data (referred to as "Operational Data") from the normal operations of the systems.

Autodesk has procedures in place to securely delete customer data upon request in accordance with their data deletion commitments to its customers.

Relevant Changes

There were no significant changes to the system and controls that occurred during the examination period under review relevant to Autodesk's service commitments and system requirements.

System Incident Disclosures

There were no incidents noted during the examination period that caused Autodesk to not meet their security, availability, and confidentiality commitments.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Complementary User Entity Controls

This section highlights those internal control responsibilities that Autodesk believes should be present at each user entity (i.e., “customer”) and has considered in developing its own internal controls. Each customer must evaluate its own internal control environment to determine whether the following controls are in place.

AUTODESK

Controls expected to be implemented at user entity organizations	Complemented criteria ref. number
User entities are responsible for understanding and complying with their security and confidentiality contractual obligations to Autodesk.	CC2.2, CC2.3
User entities are responsible for the establishment and termination of user accounts within Autodesk.	CC6.1, CC6.2, CC6.3, CC6.6, CC6.7
User entities are responsible for keeping their user accounts credentials secure in Autodesk.	CC6.1
Customers are responsible for the management of files and permissions within their projects.	CC6.1, C1.2, C1.3
User entities are responsible for restricting access and distribution of reports generated from Autodesk.	CC6.1
Customers are responsible for setting password requirements for their internal users.	CC5.1, CC5.3, CC6.1
Customers are responsible for the provisioning, deprovisioning, and reviewing the list of users within their projects.	CC6.1, CC6.2, CC6.3
User entities are responsible for communicating relevant security, availability, and confidentiality issues and incidents to Autodesk through identified channels.	CC2.2, CC2.3, CC7.3, CC7.4, CC7.5
User entities are responsible for the management of their data uploaded to Autodesk’s system, including the movement and deletion of that data.	CC6.1, CC6.7
User entities are responsible for the integrity, accuracy, and completeness of data entered into Autodesk.	A1.2
User entities are responsible for developing their own business continuity plans that address their inability to access or utilize Autodesk.	A1.2, A1.3

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Complementary Subservice Organization Controls

Autodesk has contracted with subservice organizations in support of its in-scope products' system to provide supporting infrastructure, security, and authentication services. The controls relating to the physical security, infrastructure maintenance, and network availability of the subservice organizations have been carved out of the scope of Autodesk's SOC 2 Type II report.

AUTODESK

Subservice Organization	Services Provided
Infrastructure Provider	
Amazon Web Services, Inc.	Provides infrastructure for the Autodesk in-scope products' environment
Security Services Providers	
Sentinel Labs, Inc. Orca Security Ltd.	Provides security and threat monitoring, and vulnerability assessment services
Authentication Service Providers	
Duo, Inc. Microsoft Authenticator	Provides two-factor authentication software-as-a-service

Risks related to suppliers and partners are identified during Autodesk in-scope products' risk assessment process. On an annual basis, assessments are performed on the performance of suppliers and partners to determine whether there has been impact over the Autodesk in-scope products and if there are additional mitigating controls Autodesk should implement as a result.

The following table identifies the impacted criteria and the controls expected to be implemented at the applicable subservice organizations.

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	• Access to hosted systems requires users to use a secure method to authenticate. • User content is segregated and made viewable only to authorized individuals. • Network security mechanisms restrict external access to the production environment.	• Amazon Web Services, Inc. • Duo, Inc. • MS Authenticator

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
	• Requests for access to production data must be documented and approved by appropriate personnel. • Dual / multi-factor authentication is required for access to production environments, remote access to internal networks, and limited to authorized individuals. • Industry standard encryption algorithms are used to encrypt data at rest. Encryptions keys are managed through generation, use, storage and destruction.	
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	• New user accounts are approved by appropriate individuals prior to being provisioned. • Requests for access to production data must be documented and approved by appropriate personnel. • Access that is no longer required due to termination or role change is revoked in a timely manner. • Reviews of production access are performed at least semi-annually.	• Amazon Web Services, Inc.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the	• Requests for access to production data must be documented and approved by appropriate personnel. • Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.	• Amazon Web Services, Inc.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
concepts of least privilege and segregation of duties, to meet the entity's objectives.	• Access that is no longer required due to termination or role change is revoked in a timely manner. • User accounts are reviewed on a regular basis by appropriate personnel. • Reviews of production access are performed at least semi-annually.	
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	• Access to physical facilities is restricted to authorized users. • Requests for access to data center facilities must be documented and approved by appropriate personnel. • Reviews of data center facilities access is performed at least semi-annually. • Physical and environmental protections are in place to secure the data center facilities.	• Amazon Web Services, Inc.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	• Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	• Amazon Web Services, Inc.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	• Production systems have protection mechanisms in place to prevent or detect unauthorized or malicious software.	• Amazon Web Services, Inc. • Sentinel Labs, Inc. • Orca Security Ltd.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	• Production systems are hardened in accordance with security practices. • Vulnerability scans are performed on a regular basis and identified vulnerabilities are tracked and remediated. • Logging to support data capture for security incidents, policy violations or suspicious activity must be in place. Logs must be stored in accordance with log protection requirements and clocks reference a single time source.	• Amazon Web Services, Inc. • Sentinel Labs, Inc. • Orca Security Ltd.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	• Security events are monitored and evaluated to determine potential impact per policy. • External and internal security vulnerability and penetration testing is performed by a third-party organization on an annual basis. • Production systems are monitored for performance incidents. Identified performance incidents are tracked and remediated.	• Amazon Web Services, Inc. • Sentinel Labs, Inc. • Orca Security Ltd.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	• Production systems are monitored for security events. Identified security incidents are tracked and remediated.	• Amazon Web Services, Inc. • Sentinel Labs, Inc. • Orca Security Ltd.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	• Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.	• Amazon Web Services, Inc. • Sentinel Labs, Inc. • Orca Security Ltd.
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	• Changes to infrastructure are documented, tested and approved in accordance with a defined change management policy. • Infrastructure changes are documented, tested, and approved prior to migration to production. • Access to make infrastructure changes is restricted to appropriate personnel.	• Amazon Web Services, Inc.
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	• Operations personnel monitor processing and system capacity.	• Amazon Web Services, Inc.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***

Impacted Criteria	Controls expected to be implemented at subservice organizations	Applicable Subservice Organizations
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	• Environmental controls protect the physical devices supporting the production environment. • Fire detection and suppression systems are in place and maintained annually. • Humidity, ventilation and air conditioning systems are in place and maintained annually.	• Amazon Web Services, Inc.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	• System failover and backup procedures are tested.	• Amazon Web Services, Inc.

Autodesk, Inc. *The Landmark at One Market Street, Suite 400, San Francisco, CA 94105*
Ph ***+1 415 507 5000 autodesk.com***