VMware Workspace ONE® Access™

System and Organization Controls (SOC) 3®

For the period November 22, 2022 to November 21, 2023

TABLE OF CONTENTS

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
Suite 800
1225 17th Street
Denver, CO 80202-5598

Independent Service Auditors' Report

Board of Directors of VMware LLC:

Scope

We have examined management of VMware LLC's End User Computing Division's (VMware's) accompanying assertion titled "Management of VMware's Assertion" (the Assertion) that the controls within VMware's Workspace ONE® Access™ system (the System) were suitably designed and operating effectively throughout the period November 22, 2022 to November 21, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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.

VMware uses a subservice organization identified in management of VMware's Attachment A. Management of VMware's Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at VMware, to achieve VMware's service commitments and system requirements based on the applicable trust services criteria. Management of VMware's Attachment A presents the types of complementary subservice organization controls assumed in the design of VMware's controls. Management of VMware'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, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

VMware 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 VMware's service commitments and system requirements were achieved. Management of VMware has provided the accompanying Assertion about the suitability of the design and operating effectiveness of controls within the System. VMware 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 VMware'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 VMware'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 VMware's service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve VMware'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 VMware 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 VMware 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.

Opinion

In our opinion, the Assertion that the controls within VMware's System were suitably designed and operating effectively throughout the period November 22, 2022 to November 21, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

KPMG LLP

Denver, Colorado
May 10, 2024

Section II.

Management of VMware's Assertion

VMware LLC
3401 Hillview Ave.
Palo Alto, CA 94304
(877) 486-9273 toll free
(650) 427-5000 main
(650) 427-5001 fax
www.vmware.com

Management of VMware's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within VMware LLC's End User Computing Division's (VMware's) Workspace ONE® Access™ system (the System) throughout the period November 22, 2022 to November 21, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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 VMware's Description of the Boundaries of Its System and Principal Service Commitments and Systems Requirements (Attachment A) and identifies the aspects of the System covered by the Assertion.

VMware uses a subservice organization 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 VMware, to achieve VMware'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 VMware's controls.
Our Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at VMware, to achieve VMware'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 VMware'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 November 22, 2022 to November 21, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria. VMware'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 November 22, 2022 to November 21, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria.

VMware LLC's End User Computing Division

May 10, 2024

Attachment A.

Management of VMware's Description of the Boundaries of Its Workspace ONE® Access™ System and Principal Service Commitments and Systems Requirements

SYSTEM OVERVIEW

COMPANY BACKGROUND

VMware LLC ("VMware") was founded on January 1, 1998, and its software powers the world's complex digital infrastructure. On November 22, 2023, VMware, Inc. was acquired by Broadcom, Inc. and VMware, Inc. became VMware by Broadcom (VMware LLC) as a result. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver applications on cloud environments. VMware provides infrastructure, services, and cloud solutions to organizations of all sizes. VMware is headquartered in Palo Alto, California, with strategic business offices around the globe. The End User Computing division of VMware by Broadcom provides a leading suite of digital workspace solutions that allow organizations to securely deliver and manage applications, desktops and data across any device or platform.

THE WORKSPACE ONE® ACCESS™ SERVICE

Workspace ONE® Access™

The Workspace ONE® Access™ system is a Software as a Service ("SaaS") offering, providing application provisioning, self-service catalog, conditional access controls and single sign-on ("SSO") for SaaS, web, cloud, and native mobile applications.

Workspace ONE® Access™ provides the following functionality:

- Enterprise SSO business mobility with included identity provider or integration with existing on-premises identity providers
- Ability to build a branded self-service app store so end users can subscribe to applications across devices with automated or manual provisioning
- Establishes trust between users, devices, and the hybrid cloud for a seamless user experience and conditional access controls

Workspace ONE® Access™ is offered as both an on-premise and SaaS offering, however, only the SaaS offering is included within the scope of this report.

Workspace ONE Hub Services

Workspace ONE Hub Services ("Hub Services") provides end-users with a single destination to access, discover, and connect with corporate resources, teams, and workflow. Hub Services features include an enterprise app catalog, people directory, actionable notifications, embedded portal, and help and support with and without a virtual assistant. The full Hub Services feature set is only available to customers with Workspace ONE® Access™ SaaS deployments; please consult product documentation for latest details.

The Hub Services application is co-located within the Workspace ONE® Access™ SaaS environment and is only delivered as a SaaS offering. It is possible to use Workspace ONE Hub Services solely with Workspace ONE Unified Endpoint Management ("UEM"), which is a single cloud native solution for unified endpoint management of all device types. However, users will only be able to access a limited subset of Workspace ONE Hub Services features with a Workspace ONE UEM deployment without also deploying Workspace ONE® Access™. The full workspace experience with a unified catalog, engagement features like people search, enhanced notifications, and a web browser interface require Workspace ONE® Access™ cloud deployments. Workspace ONE UEM is not included within the scope of this report.

VMware Identity Services

VMware Identity Services is a cloud service that integrates Workspace ONE® Access™ and Workspace ONE UEM with third-party cloud-based identity providers such as Microsoft Azure Active Directory for user provisioning and identity federation. Key features of VMware Identity Services include SCIM 2.0 user provisioning, identity federation using OpenID Connect (which is a decentralized authentication protocol) or SAML 2.0, and centralized user management across Workspace ONE services.

VMware hosts and manages the Workspace ONE® Access™, Hub Services, and VMware Identity Services SaaS tenant infrastructure on Amazon Web Services ("AWS"). Customer administrator users access and configure Workspace ONE® Access™, Hub Services, and VMware Identity Services through a web-based management console. End users access their assigned resources through web browser, desktop or mobile application. Integration with directory services requires Workspace ONE® Access™ Connector (customer hosted and managed), which is delivered as a virtual appliance and is not included within the scope of this report.

Workspace ONE Hub Services and VMware Identity Services are included within the Workspace ONE® Access™ environment and follow consistent processes as described throughout this report. As both Hub Services and VMware Identity Services are included in the scope of this report, further mentions of "Workspace ONE® Access™" are intended to include Hub Services and VMware Identity Services unless otherwise indicated.

EXAMINATION SCOPE

The scope of this description is limited to the Workspace ONE® Access™, including the infrastructure, software, people, procedures, and data that are managed by Workspace ONE® Access™. In addition, there are certain controls that are operated and managed at the entity level by VMware Corporate Operations ("Corporate Operations"). Workspace ONE® Access™ and Corporate Operations include relevant processes and controls within the following Trust Services Criteria:

- Security
- Availability

Relevant processes and controls for Workspace ONE® Access™ and Corporate Operations fall within the following domains:

- Access Control
- Asset Management
- Business Continuity Management
- Communications Security
- Compliance
- Human Resource Security
- Information Security Incident Management
- Organization of Information Security
- Risk Management
- Supplier Relationships
- System Acquisition, Development, and Maintenance
- System Availability
- System Monitoring
- Vulnerability Management

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The processes and procedures managed by Workspace ONE® Access™ are implemented to help ensure the Security and Availability of its service. Workspace ONE® Access™ has communicated its service commitments and Service Level Agreements ("SLAs") to customers in documentation posted on the publicly available VMware website.

VMware makes commitments regarding the Security and Availability of information in the Service Level Agreements Guide and the VMware Cloud Services Guide posted on the VMware website. Commitments include, but are not limited to, the following:

- VMware will protect the information systems used to deliver the service offering over which VMware has sole administrative level control.
- VMware will monitor security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the service over which VMware has sole administrative control. This responsibility stops at any point where the customer has some control, permission, or access to modify an aspect of the Workspace ONE® Access™ service.
- VMware will maintain the systems used to deliver the service, including the application of patches for the target systems.
- VMware will perform routine vulnerability scans to surface risk areas for the systems used to deliver the service offering and address vulnerabilities in a timely manner.
- VMware will monitor availability of the Workspace ONE® Access™ service and maintain availability as defined in the Workspace ONE Service Level Agreement.
- VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to availability of the Workspace ONE® Access™ service.
- VMware will encrypt data in transit over public networks with strong transport layer security (minimum of TLS v1.2) encryption.

To meet its service commitments to its customers, VMware has defined system requirements for Workspace ONE® Access's™ operations. VMware communicates these requirements in the policies and procedures it provides to all employees working on the system. System requirements include, but are not limited to, the following:

- VMware has the appropriate logical access controls around the system and backend infrastructure.
- There are various systems to monitor security events and logical and operational events logged from the backend infrastructure system controlled by VMware.
- VMware performs vulnerability scans on the backend infrastructure to help ensure that critical and high severity vulnerabilities are addressed in a timely manner.

COMPONENTS OF THE SYSTEM

INFRASTRUCTURE

The Workspace ONE® Access™ production system is hosted in Amazon EC2 instances running Amazon Linux 2 ("AL2") host operating system ("OS") and the VMware Photon OS Docker container. Workspace ONE® Access™ is hosted on Amazon Web Services ("AWS") locations listed in the table below:

COMPONENT	DESCRIPTION
Cloud Service Provider hosting the Workspace ONE® Access™ service	The service utilizes AWS in the following regions/availability zones ("AZs"): ■ United States (us-west-2) ■ Canada (ca-central-1) ■ Japan (ap-northeast-1) ■ Australia (ap-southeast-2) ■ Ireland (eu-west-1) ■ United Kingdom (eu-west-2) ■ Germany (eu-central-1)

The following AWS services are utilized by Workspace ONE® Access™:

AWS COMPONENT	DESCRIPTION
Amazon CloudWatch	Amazon CloudWatch is a monitoring and observability service that is used to monitor for system availability and health.
Amazon CloudWatch Log Agent	Amazon CloudWatch Log Agent was used to capture security logs and was replaced by Fluentbit on February 24, 2023.
AWS Kinesis Data Firehose	AWS Kinesis Data Firehose is used to ingest security logs into the VMware Security Operations Center ("SOC").
AWS Lambda	AWS Lambda was used to format security logs before writing to S3 for ingestion to the VMware Security Operations Center ("SOC") until February 24, 2023, when it was no longer necessary due to the implementation of Fluentbit.
AWS Simple Notification Service ("SNS")	SNS is used as a notification service used for security logging.
AWS S3	AWS S3 is used to store security logs for forwarding to the VMware Security Operations Center.
AWS CloudTrail	AWS CloudTrail is used to monitor access, events, and activity within AWS.

AWS COMPONENT	DESCRIPTION
AWS AL2, and Photon OS	Application platform providing end users with Workspace ONE® Access™ functionality.
AWS Elastic Compute Cloud (“EC2”)	AWS EC2 is a web service that provides compute capacity and manages instances supporting the Workspace ONE® Access™ platform.
AWS Relational Database Services (“RDS”) OS (AWS)	AWS Aurora, MySQL and DynamoDB databases supporting the Workspace ONE® Access™ platform.
AWS OpenSearch	Managed distributed search and analytics engine built on Apache Lucene.
AWS Security Traffic Controller	AWS Security Groups prevent unauthorized inbound traffic into the network from the Internet.
AWS Certificate Manager (“ACM”)	The AWS Certificate Manager is used to secure secret and authentication certificates.
AWS Key Management System (“KMS”)	The Key Management System is used to secure access to cryptographic keys.

SOFTWARE

The following table details the key software and network components which support Workspace ONE® Access™:

COMPONENT	DESCRIPTION
Cerberus	Cerberus is used as a secrets management tool used by Workspace ONE® Access™. as of December 11, 2022, when it replaced Password Manager Portal.
Docker	Docker is the platform used to develop containers for the Workspace ONE® Access™ application.
Duo MFA	Duo MFA is used to facilitate multi-factor authentication to Workspace ONE® Access™ components.
Falco	Falco is used for host-based intrusion detection and file integrity monitoring.
Fluentbit	Fluentbit is used to process security logs beginning on February 24, 2023, replacing AWS CloudWatch log agent and Lambda.
GitLab	GitLab is a git repository service used for source-code management.
Jenkins	Jenkins is the continuous integration and continuous delivery (“CI/CD”) tool used for continuous implementation/delivery.
Jira	Jira is the ticketing system used for issue tracking.

COMPONENT	DESCRIPTION
Logz.io	Logz.io is a cloud observability platform used to monitor the health of the Workspace ONE® Access™ environment.
Open VPN	The Open VPN enables authorized personnel to remotely connect to the Workspace ONE® Access™ infrastructure.
PagerDuty	PagerDuty is a SaaS incident response platform used to alert key personnel of time sensitive incidents and issues.
Password Manager Portal ("PMP")	The Password Manager Portal is used as a secret management tool until December 10, 2022, when it was replaced by Cerberus.
Slack	Slack is a workplace messaging program.
Uptime	Uptime is used to monitor system availability.
Wavefront	Wavefront is a VMware hosted cloud observability platform used to monitor the health of the Workspace ONE® Access™ environment.

The following table details the key Corporate software and network components which support Workspace ONE® Access™:

COMPONENT	DESCRIPTION
AccessNow	AccessNow is a tool used for access provisioning, access deprovisioning, and user access reviews.
Active Directory	Active Directory ("AD") is a directory service used for VMware's corporate network domain.
Brinqa	Brinqa is a ticketing system used to notify asset owners of identified vulnerabilities.
GlobalProtect	The GlobalProtect VPN (virtual private network) enables authorized personnel to remotely connect to the internal corporate network.
Nessus (Tenable, Inc.)	Nessus is a vulnerability scanning solution.
RiskVision	RiskVision is a ticketing system used to notify asset owners of identified vulnerabilities.
Splunk	Splunk is a software platform used for monitoring, identifying, and tracking security events.
VMware Carbon Black	VMware Carbon Black provides enterprise endpoint detection and response.
VMware Workspace ONE® Access™	VMware Workspace ONE Access is a single sign-on solution.

COMPONENT	DESCRIPTION
VMware Workspace ONE® Unified Endpoint Management (“UEM”)	VMware Workspace ONE UEM is the Mobile Device Management Solution installed on corporate and personal mobile devices that access company information. VMware Workspace ONE UEM provides controls to manage mobile device security and configuration management.

The risks relevant to the achievement of VMware’s service commitments and system requirements vary across these components, and VMware has designed its control environment accordingly.

PEOPLE

The Workspace ONE® Access™ service is managed by the following teams:

TEAM	DESCRIPTION
Engineering	Responsible for documenting development and system test plans.
DevOps	Responsible for automation, upgrades, patch management, monitoring maintenance, and troubleshooting incidents.

The Workspace ONE® Access™ service is supported by the following Corporate teams:

TEAM	DESCRIPTION
Executive Management	Responsible for overseeing company-wide activities, establishing overall goals, monitoring the achievement of identified goals, and overseeing objectives.
Human Resources	Responsible for human resources (“HR”) policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisition, pre-employment screening, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
Security and Resiliency	Responsible for managing the development, maintenance, and enforcement of information security policies and standards to help ensure VMware Information Assets are preserved in a secure environment, are in accordance with generally accepted best practices, and align with VMware business and risk objectives.
Risk Management	Responsible for managing the annual performance of risk assessments, maintaining a centralized risk register, and tracking and reporting risk mitigation activities throughout the organization.
Enterprise Resiliency Business Continuity	Responsible for managing the organization’s overall approach to business continuity, including the annual performance of Business Impact Assessments and testing and maintenance of Business Continuity Plans for VMware lines of business.

TEAM	DESCRIPTION
Security Operations Center	Responsible for intake of reported security events, including gathering, triaging, and providing first response. Security incidents are escalated to the VMware Security Incident Response Team.
Security Incident Response Team	Responsible for centrally managing all information security incidents for VMware, including ensuring proper collection of evidence, coordinating cross-functional incident teams, and developing effective response strategies for incident remediation.
Red Team	Responsible for performing penetration testing for VMware products and services, including tracking and escalating remediation of test findings.
Global Support Services	Responsible for handling customer support issues and inquiries.
Colleague Support Team	Responsible for the distribution, replacement, and collection of VMware-issued end user devices.
Executive Management	Responsible for overseeing company-wide activities, establishing overall goals, accomplishing goals, and overseeing objectives.

PROCEDURES

VMware has established policies and procedures to support the achievement of its service commitments and the applicable American Institute of Certified Public Accountants ("AICPA") Trust Services Categories and Criteria for Security and Availability.[1] These policies and procedures include guidance on designing and developing the service, operating the system, managing internal business systems, and hiring and training employees. In addition to these policies, standard operating procedures have been documented to detail specific processes required in the operation and development of the service.

The corporate information security policies and procedures are defined, approved, published, and communicated to users and relevant third parties. These documents are stored in a central repository accessible to employees and other appropriate staff and define the roles and responsibilities for the information security program. The information security policies are reviewed, updated, and approved at least annually to help ensure their continuing suitability and effectiveness.

DATA

VMware has established a Data Classification Policy which documents the various data classification criteria. This policy is reviewed and approved by management annually and communicated to internal personnel. In addition, the Data Handling and Protection Standards define procedures for handling information assets based on their classification, including requirements for media disposal.

Workspace ONE® Access™ collects customer profile information (e.g., username, email, first name, last name) and system configuration data. Customer profile information is keyed in by customers and utilized in the build out of the customer Workspace ONE® Access™ platform. The customer content listed above

[1] The AICPA Trust Services Categories consist of Security, Availability, Confidentiality, Processing Integrity, and Privacy. The Security Category provides criteria to assess whether information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives. The Availability Category provides criteria to assess whether information and systems are available for operation and use to meet the entity's objectives.

is collected and recorded in the Workspace ONE® Access™ production systems in the normal course of use of the service by the customer. Please see the Workspace ONE Privacy Disclosure on the VMware Privacy page for additional information.

This data is stored and maintained within the AWS Aurora, MySQL, and DynamoDB databases. Customer profile information is encrypted in transit over public networks using TLS encryption and data is encrypted at rest using a combination of application and volume encryption (AES 256).

Customer-specific configuration settings are also maintained within the AWS Aurora, MySQL and DynamoDB databases. AWS OpenSearch datastores are used for audit log and search indexing.

COMPLEMENTARY USER ENTITY CONTROLS

VMware's controls related to Workspace ONE® Access™ cover only a portion of overall internal controls for each user entity of Workspace ONE® Access™. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by VMware.

For user entities to rely on the controls reported herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls ("CUECs") have been implemented and are operating effectively.

The CUECs presented below should not be regarded as a comprehensive list of controls that should be employed by user entities. Management of user entities are responsible for the following:

TRUST SERVICES CRITERIA INTENDED TO BE MET BY THE CONTROLS OF THE USER ENTITIES	CONTROLS EXPECTED TO BE IMPLEMENTED AT THE USER ENTITIES
CC7.3	■ Controls should be established to help ensure that user entities report security issues, concerns, and incidents to the VMware customer service channels.
A1.2	■ Controls should be in place at the user entity to monitor the availability of the service to determine whether SLAs or uptime are met.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

The description of the Workspace ONE® Access™ system of controls presented in Sections III and IV represents the controls VMware has implemented to achieve VMware's service commitments and meet its system requirements. The controls do not extend to include the controls in place at the relevant subservice organization.

VMware utilizes the subservice organization described below to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only the policies, procedures and control activities at VMware and does not include the policies, procedures, and control activities at the subservice organization described below. The complementary subservice organization controls ("CSOCs") presented below should not be regarded as a comprehensive list of all the controls that should be employed by the subservice organization.

The table below reflects the subservice organization that is used by VMware. VMware's policies, procedures and control activities were designed with the assumption that certain CSOCs would be implemented by the subservice organization for achievement of service commitments and system requirements identified in this report.

VMware management receives an annual System and Organization Controls (SOC 2®) report from the subservice organization and reviews the report to determine if the controls at the subservice organization that are necessary to achieve the Trust Services Criteria are operating effectively.

SUBSERVICE ORGANIZATION	TRUST SERVICES CRITERIA INTENDED TO BE MET BY THE CONTROLS OF THE SUBSERVICE ORGANIZATION AND CONTROLS EXPECTED TO BE IMPLEMENTED AT THE SUBSERVICE ORGANIZATION	
Amazon Web Services Provides cloud hosting services	**CC6.1** **CC6.2** **CC6.3**	■ Policies and mechanisms are in place to restrict unauthorized system access. Access that is no longer required is removed in a timely manner.
	CC6.4	■ Requests for new or modified physical access to data center facilities are approved prior to provisioning. ■ Physical access to data center facilities is deprovisioned in a timely manner upon termination. ■ Physical access to data center facilities is reviewed for appropriateness on a quarterly basis. Access flagged for removal is revoked in a timely manner. ■ Data center access is restricted to authorized personnel and monitored on a 24/7 basis.
	CC6.5	■ Physical assets are wiped prior to disposal or re-use in accordance with the policy.

SUBSERVICE ORGANIZATION	TRUST SERVICES CRITERIA INTENDED TO BE MET BY THE CONTROLS OF THE SUBSERVICE ORGANIZATION AND CONTROLS EXPECTED TO BE IMPLEMENTED AT THE SUBSERVICE ORGANIZATION	
	CC7.1 **CC7.2** **CC7.3** **CC7.4**	■ Policies and mechanisms have been implemented for reporting security events and incidents. ■ Policies and mechanisms have been implemented to identify and triage security events. ■ An incident response process is documented and established for the identification and response to security events and incidents.
	A1.1 **A1.2**	■ Policies and mechanisms have been implemented to perform continuous backups and automated replication to support continuous availability.
	A1.2	■ Policies and mechanisms have been implemented to address system availability and recovery objectives, including environmental protection mechanisms. ■ Fire suppression, fire detection, and environmental monitoring systems have been installed at the data centers. ■ Protections against a disruption in power supply to the processing environment are implemented. ■ Regular maintenance of environmental protection at data centers is performed.
	A1.3	■ Business Continuity Plans are tested and updated at least annually or following significant organizational or environmental changes.