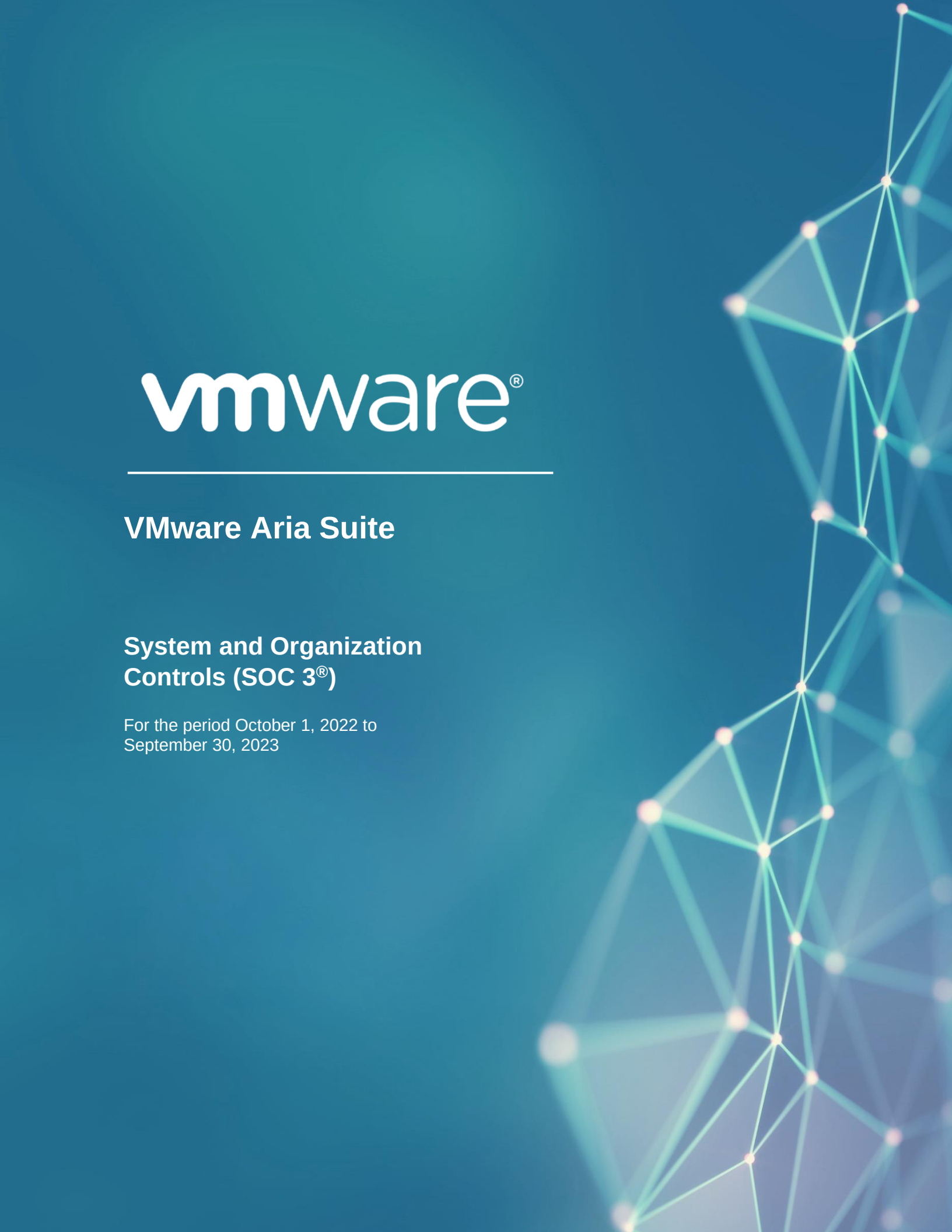

VMware Aria Suite

System and Organization Controls (SOC 3®)

For the period October 1, 2022 to September 30, 2023

TABLE OF CONTENTS

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
Suite 1100
4655 Executive Drive
San Diego, CA 92121-3132

Independent Service Auditors' Report

Board of Directors of VMware LLC:

Scope

We have examined management of VMware LLC's (VMware's) accompanying assertion titled "Management of VMware LLC's Assertion" (the Assertion) that the controls within VMware's Aria Suite system (the System) were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 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 subservice organizations 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 organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization 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 October 1, 2022 to September 30, 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

San Diego, California
December 14, 2023

Section II.

Management of VMware LLC'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 LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within VMware LLC's (VMware's) Aria Suite system (the System) throughout the period October 1, 2022 to September 30, 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 - VMware's Overview of Services and the System and identifies the aspects of the System covered by the Assertion.

VMware uses 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 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.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period October 1, 2022 to September 30, 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 October 1, 2022 to September 30, 2023 to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria.

VMware LLC

December 14, 2023

Attachment A.

VMware LLC's Description of the Boundaries of Its Aria Suite System and Principal Service Commitments and System Requirements

SYSTEM OVERVIEW

COMPANY BACKGROUND

VMware LLC ("VMware") was founded on January 1, 1998 and currently has over than 37,000 employees worldwide. VMware software powers the world's complex digital infrastructure. On November 22, 2023, VMware, Inc. was acquired by Broadcom, Inc. and VMware, Inc. became 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 VMWARE ARIA SUITE SERVICE

VMware Aria Suite, now part of Unified Hybrid and Multi-Cloud Management are a set of Software-as-a-Service (SaaS) based services that enable information technology (IT) administrators, DevOps engineers, and developers, the ability to provision, automate, manage, and optimize their applications and infrastructure availability, cost, security and performance across any cloud, both private and public. The following list of services together form the set of Aria suite

- VMware Aria Automation™ (formerly vRealize Automation) consists of the following component services:
    - VMware Aria Automation Assembler™ (formerly VMware Cloud Assembly) – Cloud automation service purpose-built for provisioning and managing workloads in software-defined data centers (SDDCs), VMware Aria Suite Cloud on AWS–based clouds, and public clouds. Cloud Assembly offers infrastructure-as-code capabilities to build, deploy, and iterate on applications with agile governance.
    - VMware Aria Automation Pipelines™ (formerly Code Stream) – SaaS-based application release automation offering that helps customers automate their continuous integration and continuous delivery processes. Aria Automation Pipelines focuses on ease of release pipeline modeling, deep integration with other VMware products such as Aria Automation Assembler, source code control systems, and provide reporting through dashboards to help DevOps teams with deep visibility and automation of the software release process.
    - VMware Aria Automation Consumption™ (formerly Service Broker) – Storefront for self-service consumption of ready-to-use templates and services with guardrails. This collection of ready-to-consume cloud services and templates is aggregated from multiple cloud platforms and providers. Automation Consumption offers IT organizations a maintainable and controlled platform for brokering cloud services and templates. With Automation Consumption, developers can acquire the tools or managed services they need (e.g., cloud database) on demand, freeing them from day-to-day management of these services, and allowing them to focus on their applications.
    - VMware Aria Hub Subscription™ (formerly vRealize Subscription Manager) –VACS service manages your license consumption across on-premise and cloud services. For on-premise products, Aria Central Subscription integrates with Aria Universal Suite to monitor the license consumption for the corresponding license keys, and provides billing services for your Aria Suite of products.
    - VMware Aria Operations for Logs™ (formerly Log Insight Cloud) – Log-based monitoring and troubleshooting service purpose-built for SDDCs, VMware Cloud on AWS, and public clouds. Aria Operations for Logs offers administrators rapid IT troubleshooting and operational visibility across multiple cloud environments, enabling IT teams to solve issues.
    - VMware Aria Hub (formerly Project Ensemble) – VMware Aria Hub provides centralized views and controls to manage the entire multi cloud environment. Aria Hub is powered by

a graph-based data store that captures the resources and relationships of a multi-cloud environment.

- VMware Aria Operations for Networks™ (formerly vRealize Network Insight Cloud) – Network and security analysis service purpose-built for SDDCs and public clouds. Aria Operations for Networks enables network visibility and understanding of traffic flows between applications to enable cloud security planning and network troubleshooting. Aria Operations for Networks also provides intuitive user interface (UI), simplifying search criteria for monitoring and administration allowing cloud administrators to manage and troubleshoot VMware NSX and public cloud deployments.
- VMware Aria Operations™ (formerly vRealize Operations) platform powered by artificial intelligence (AI) to optimize, plan and scale hybrid and multi-cloud deployments, from apps to infrastructure. The service delivers continuous performance, capacity and cost optimization, intelligent remediation and integrated compliance through AI/Machine Learning and predictive analytics.

EXAMINATION SCOPE

The scope of this description is limited to VMware Aria Suite, including the infrastructure, software, people, procedures. Data that is managed by VMware Aria Suite excludes collector and proxy agents installed on customer infrastructure. These VMware Aria Suite operations include relevant processes and controls within the following trust service categories:

- Security
- Availability

In addition, there are certain controls that are operated and managed at the entity level by VMware Corporate Operations (“Corporate Operations”). These Corporate Operations include relevant processes and controls 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
- Physical and Environmental Security
- Risk Management
- Supplier Relationships
- System Acquisition, Development, and Maintenance
- System Monitoring
- Vulnerability Management

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The processes and procedures managed by VMware Aria Suite are implemented to help ensure the Security and Availability of its service. VMware has communicated its service commitments and service level agreements ("SLAs") to customers within 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 (vmware.com/agreements). 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 from inappropriate access.
- VMware will control changes and prevent unapproved modification to the service offering through a defined change management process.
- VMware will monitor and respond to 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.
- VMware will maintain security incident response processes for information systems used to deliver the service offering over which VMware has sole administrative level control.
- 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 encrypt customer data at rest. Customer data transmitted over public networks will be encrypted using TLS v1.2 or higher.
- VMware will provide incident and problem management services pertaining to availability of the service. If customers have inquiries or require additional support, customer support lines are available 24/7 for severity 1 issues. Documentation, resources, and discussion forums are also available on the VMware website.
- VMware will monitor the availability of the service and communicate availability via the online status page (status.vmware-services.io). VMware will maintain a minimum monthly uptime percentage of 99.5%. Customers who experienced service below the minimum can request a credit from VMware after reviewing the availability report provided by VMware.
- VMware will maintain a business continuity program that is tested on at least an annual basis.

To meet its service commitments to its customers, VMware has defined a set of system requirements for the operations of VMware Aria Suite. VMware communicates these requirements in the policies and procedures that it provides to all employees working on the system.

- VMware has defined the appropriate logical and physical access controls around the system and backend infrastructure.
- VMware has implemented change management controls to require change review, approval, and testing (as applicable) prior to deployment into production.
- There are various systems VMware has processes in place to monitor security events and logical and operational events logged from the backend infrastructure system controlled by VMware.
- VMware has defined information security incident management processes.
- VMware performs patching of the backend infrastructure on a regular basis.

- VMware performs vulnerability scans on the backend infrastructure to help ensure that critical and high severity vulnerabilities are addressed in a timely manner.
- VMware has configured data stores and public endpoints to encrypt data at rest and in transit over public networks.
- VMware has defined controls to securely dispose of customer data in accordance with commitments made to customers.
- VMware has processes in place to document and track customer support Severity 1 issues to resolution.
- VMware maintains an online status page to communicate the status of services, scheduled maintenance, and incidents to customers.
- VMware has defined a Business Continuity Plan and performs annual business continuity exercises to test the plan.

COMPONENTS OF THE SYSTEM

INFRASTRUCTURE

The VMware Aria Suite production system is operated by VMware but hosted on Amazon Web Services ("AWS") in the following locations. The production system includes related servers and databases as indicated below. In addition, VMware has its corporate headquarters and corporate data center in the following locations that support, and are managed by, VMware Corporate Operations:

COMPONENT	DESCRIPTION
VMware Aria Automation™	AWS - availability zones ("AZs"): ■ us-west-2 ■ ca-central-1 ■ ap-southeast-1 ■ ap-southeast-2 ■ ap-northeast-1 ■ ap-south-1 ■ eu-central-1 ■ eu-west-2 ■ sa-east-1
VMware Aria Operations for Networks™	AWS - availability zones ("AZs"): ■ us-west-2 ■ ca-central-1WW ■ ap-southeast-2 ■ ap-northeast-1 ■ ap-south-1 ■ eu-central-1 ■ eu-west-2

COMPONENT	DESCRIPTION
VMware Aria Operations™	AWS - availability zones (“AZs”): ■ us-west-2 ■ ca-central-1 ■ ap-southeast-1 ■ ap-southeast-2 ■ ap-northeast-1 ■ ap-south-1 ■ eu-central-1 ■ eu-west-2 ■ sa-east-1
Corporate Data Center	VMware Corporate Operations utilizes a data center owned and managed by Sabey Data Center Properties LLC (“Sabey”) in the following location: ■ Wenatchee, Washington VMware Corporate Operations utilizes a data center owned and managed by Vantage Data Centers in the following location: ■ Santa Clara, California
Operations Support	The VMware global headquarters is located in Palo Alto, California. Additional offices are located throughout North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa.

The corporate data centers host certain corporate infrastructure used to support VMware’s suite of cloud services and products. This includes authentication and networking infrastructure such as Active Directory as well as internal tooling supporting the central security monitoring function.

The following AWS-services are utilized by VMware Aria Suite:

AWS COMPONENT	DESCRIPTION
Amazon Elastic Compute Cloud (EC2)	A web service used for launching and managing Linux/UNIX and Windows Server instances within Amazon data centers
Amazon Elastic Kubernetes Service (EKS)	SaaS based services that enable IT administrators, DevOps engineers, and developers, the ability to provision, automate, manage and optimize their applications and infrastructure.
Amazon DynamoDB	A fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.
Amazon GuardDuty	A continuous security monitoring service. Amazon GuardDuty can help to identify unexpected and potentially unauthorized or malicious activity in your AWS environment.
Amazon Relational Database Service (RDS)	Allows a user to set up, operate, and scale a relational database in the cloud while managing database administration tasks.
Amazon S3	Storage for the internet. You can use it to store and retrieve any amount of data at any time, from anywhere on the web.
Amazon Virtual Private Cloud (VPC)	Allows VMware to provision a logically isolated section of the AWS cloud where it can launch AWS resources in a virtual network.
AWS Key Management Service (AWS KMS)	A managed service that simplifies the creation and control of encryption keys that are used to encrypt data
CloudWatch	Allows you to store, search, analyze, monitor, and alert logging data and events

SOFTWARE

The following table details the key software and network components which support Aria Suite platforms:

COMPONENT	DESCRIPTION
Catchpoint	UI Synthetic Monitoring
Codestream	Continuous integration and continuous delivery (CICD) tool. Create pipelines that model the software release process in the DevOps lifecycle
Jira	A highly customizable tool for agile software development used to log and track progress for bugs, tasks, features, and other projects
Jenkins	Jenkins is a self-contained, open source automation server which can be used to automate tasks related to building, testing, and delivering or deploying software
Pagerduty	Enables rapid incident response with rich, contextual details and graphs to help you analyze trends and track performance of your applications and AWS environment
Tenable Nessus	Vulnerability assessment tool with live results
Terraform	A library of policies that can be used to accelerate adoption of policy as code
Wavefront	Monitoring, observability and alerting for Cloud workloads (not in use for vROPs).
VMware vCloud Director	Deployment, automation and management software for virtual infrastructure resources in multi-tenant cloud environments (not in use for vRA, vRAI, vRLI, vRSCM, nor Ensemble).

The following tables will list application that are specific to each Aria Suite platforms:

- VMware Aria Automation™
- VMware Aria Operations for Logs™
- VMware Aria Hub Subscription™
- VMware Aria Hub (Ensemble)

COMPONENT	DESCRIPTION
Gerrit	Highly extensible and configurable tool for web-based code review and repository management for VMware Aria Suite repositories. Serves as gated check-in tool for VMware Aria Suite services
Gitlab	Administers a complete continuous integration and deployment service that is delivered as a single application enabling DevOps to manage and maintain the software development lifecycle.
OSSTP	Open Source and Third-Party tools analyzer

- VMware Aria Operations for Networks™

COMPONENT	DESCRIPTION
Github	A distributed version control system based on git used as source code repository
VMware vCenter	Deployment, automation and management software for virtual infrastructure resources in multi-tenant cloud environments

- VMware Aria Operations™

COMPONENT	DESCRIPTION
CVE Repository	Portal for Aria for Operations vulnerability detected packages with appropriate CVE for each package
Gitlab	Administers a complete continuous integration and deployment service that is delivered as a single application enabling DevOps to manage and maintain the software development lifecycle.
Nebula	Automation tool for OSSPI
Perpetuum	Internal service orchestrating regression pipeline

The following table details the key Corporate software and network components which support VMware Aria Suite:

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.
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.
Palo Alto Networks	Palo Alto Networks firewall systems are in place to filter and restrict unauthorized inbound traffic to the corporate network.
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.

COMPONENT	DESCRIPTION
VMware CloudGate	VMware CloudGate is a proprietary cloud delivered service orchestration and authentication tool.
VMware Workspace ONE® Access™	VMware Workspace ONE Access is a single sign-on solution.
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. Workspace ONE 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 VMware Aria Suite service is managed by the following teams:

TEAM	DESCRIPTION
VMware Aria Suite Executive Management	Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
VMware Aria Suite Security Engineering	Responsible for implementing, testing, and overseeing VMware Aria Suite’s information security program to protect information, prevent unauthorized access, and respond to security incidents, vulnerabilities, and risks. Works with VMware central security teams to perform an annual risk assessment.
VMware Aria Suite System Engineering	Responsible for automation, development, system test plans and testing, and risk analysis.
VMware Aria Suite Technical Operations	Responsible for managing the Platform infrastructure and leading the development and maintenance of system and network security. Provides support for the Platform, first response for system and network issues, and performance monitoring.

The VMware Aria Suite service is supported by the following Corporate teams:

TEAM	DESCRIPTION
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing 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).

TEAM	DESCRIPTION
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, in accordance with generally accepted best practices, focusing on 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.
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.
Data Center Operations	Responsible for maintaining an inventory of physical assets.
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.

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 on how to carry out 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

[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 its 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.

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.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

The description of VMware Aria Suite's 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 effect at relevant subservice organizations.

VMware utilizes subservice organizations 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 organizations 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 organizations.

The table below reflects the subservice organizations that are used by VMware. VMware's policies, procedures and control activities were designed with the assumption that certain complementary subservice organization controls 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 each subservice organization and reviews the reports to determine if the controls at the subservice organizations that are necessary to meet 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	
Sabey Data Center Properties LLC Provides physical and environmental data center services	**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. ■ Physical security controls for data center facilities such as controlled badge access and video surveillance have been implemented to restrict physical access to authorized individuals. ■ Physical access will be provided by the subservice organization after approvals are obtained from VMware.

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	
	A1.2	■ Environmental controls, including HVAC controls, fire detection and suppression systems, and protection from power failures, are in place to protect information systems in data centers. ■ Equipment maintenance is performed and documented to help ensure the continued availability and integrity of equipment
Vantage Data Centers Provides physical and environmental data center services	**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. ■ Physical security controls for data center facilities such as controlled badge access and video surveillance have been implemented to restrict physical access to authorized individuals. ■ Physical access will be provided by the subservice organization after approvals are obtained from VMware.
	A1.2	■ Environmental controls, including HVAC controls, fire detection and suppression systems, and protection from power failures, are in place to protect information systems in data centers. ■ Equipment maintenance is performed and documented to help ensure the continued availability and integrity of equipment.
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	■ Physical security controls for data center facilities such as controlled badge access and video surveillance have been implemented to restrict physical access to authorized individuals.Data center access is restricted to authorized personnel and monitored on a 24/7 basis.

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	
	CC6.5	■ Physical assets are wiped prior to disposal or re-use in accordance with the policy.
	CC6.6 **CC6.7**	■ Policies and mechanisms have been implemented for secure authentication into the internal network. ■ Firewalls are configured and maintained to restrict access to the computing environment and enforce boundaries among compute resources. ■ Data is encrypted in transit either as part of the service provided or as enabled by the customer.
	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.
	CC8.1	■ Policies and mechanisms have been implemented to document and control changes to infrastructure and applications in accordance with a defined Change Management Policy.
	A1.2	■ Environmental controls, including HVAC controls, fire detection and suppression systems, and protection from power failures, are in place to protect information systems in data centers. ■ Equipment maintenance is performed and documented to help ensure the continued availability and integrity of equipment
	A1.3	■ Business Continuity Plans are tested and updated at least annually or following significant organizational or environmental changes.