Response To Singapore Multi-Tiered Cloud Security (MTCS) Standard Requirements

VMware Cloud On AWS

vmware

By opening this document, you agree that all 'information' presented in this document shall be considered VMware proprietary information. You agree to maintain the confidence of the information in this document and to prevent its further dissemination; provided however, that the information has not already or subsequently becomes generally known or available by publication or commercial use.

Recipient expressly agrees not to use the information for purposes other than those necessary to consider the possibility of entering into or continuing a business relationship with VMware. All information remains the property of VMware and no license or other rights to the information is granted hereby. All information is provided 'as is' and without any warranty, express, implied or otherwise, regarding its accuracy of performance.

Contents

Executive Summary

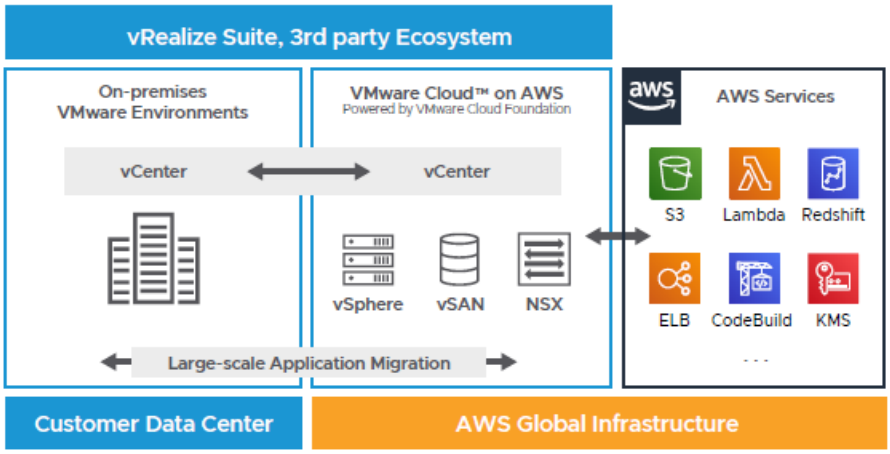
Cloud computing has transformed how government agencies manage their IT infrastructure. While it has opened opportunities to improve the quality and delivery of services and reduce operational costs, it has created unique challenges in maintaining security and availability of data and systems, scaling up IT infrastructure with changing business demands, and complying with stringent government mandates surrounding data security and privacy.

This whitepaper provides guidance on how VMware Cloud on AWS may help address the key requirements of the Singapore Multi-Tier Cloud Security (MTCS) standard. Government agencies in Singapore can use this whitepaper to understand the controls and processes that VMware Cloud on AWS has implemented to safeguard the workloads and provide customers a reliable infrastructure to meet their business needs.

VMware Cloud on AWS

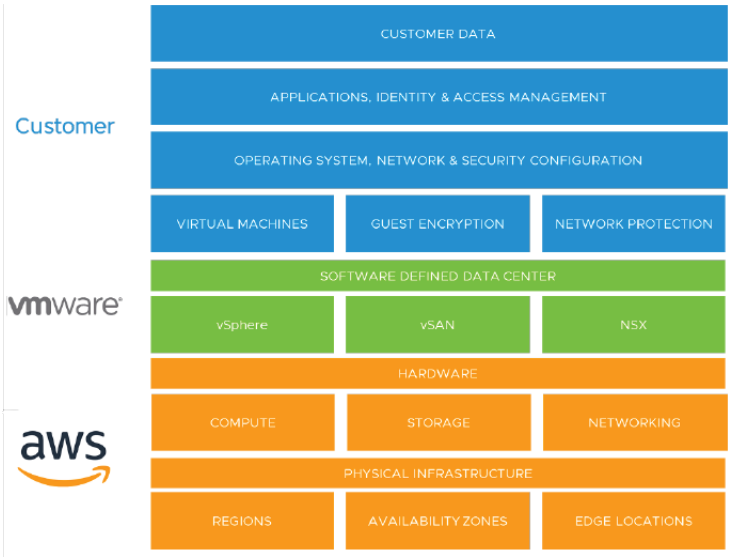
VMware Cloud on AWS brings VMware's enterprise class Software-Defined Data Center software to the AWS Cloud, and enables customers to run production applications across VMware vSphere-based environments, with optimized access to AWS services. Jointly engineered by VMware and AWS, this on-demand service enables IT teams to seamlessly extend, migrate, and manage their cloud-based resources with familiar VMware tools without the hassles of learning new skills or utilizing new tools. VMware Cloud on AWS integrates VMware's flagship compute, storage, and network virtualization products (VMware vSphere, VMware vSAN, and VMware NSX) along with VMware vCenter management, and optimizes it to run on dedicated, elastic, Amazon EC2 bare-metal infrastructure that is fully integrated as part of the AWS Cloud. This service is managed by VMware and sold by VMware and its partner community. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

VMware Cloud on AWS enables enterprise IT and operations teams to innovate, transform, and add value to the business while continuing to leverage their VMware expertise and without the need to purchase new hardware. With VMware Cloud on AWS you can quickly and confidently migrate applications currently deployed in on-premises and co-located data centers usually without refactoring. In addition, applications deployed in VMware Cloud on AWS become much easier to modernize with high-speed low-latency access to native cloud services from AWS.



Shared Responsibility

VMware Cloud on AWS implements a shared responsibility model that defines distinct roles and responsibilities of the three parties involved in the offering: Customer, VMware, and Amazon Web Services. The following diagram illustrates the high-level architecture for VMware Cloud on AWS and the associated security responsibilities for VMware, AWS and cloud tenants.



Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in-guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" – VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

AWS responsibility "Security of the Infrastructure" – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.

For further details on shared responsibility model, please see our 'Shared Responsibility Model' whitepaper at *https://assets.contentstack.io/v3/assets/blt58b49a8a0e43b5ff/blt097d7d0985cc2e3c/5f68de70a4d7b56a23866d55/Shared_Responsibility_Model_Overview_for_VMware_Cloud_on_AWS_Whitepaper.pdf*

Managing risk and compliance with VMware Cloud on AWS

VMware has implemented a wide range of security controls to ensure we deliver a secure and reliable environment for government agencies to manage their IT infrastructure needs and manage workloads in line with leading industry standards including MTCS. You can view existing compliance and certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance* .

In the sections below, we have highlighted how VMware Cloud on AWS may help address the key requirements in MTCS Standard. Government agencies can utilize this information to assess the service risk in terms of security, privacy and business value and establish an informed risk profile when moving workloads to VMware Cloud on AWS.

VMware Cloud on AWS service also undergoes independent third-party audits on a regular basis to provide assurance to our customers that VMware has implemented industry leading controls. VMware Cloud on AWS has been audited for most of the key industry certifications including ISO 27001, ISO 27017, ISO 27018 and SOC 2. A number of other compliance offerings are also in development, you can view them in our roadmap at *https://cloud.vmware.com/vmc-aws/roadmap*.

Conclusion

VMware software-defined data center (SDDC) technologies lead the industry in delivering the flexibility, protection, and scalability that government agencies need to deliver exceptional customer experiences and new business models across physical, virtual, and cloud environments.

VMware has supported a wide range of government agencies across the globe rapidly drive stability, growth through future ready technology solutions, please visit *https://www.vmware.com/solutions/industry/government.html* VMware Cloud on AWS will help enable government agencies to meet their security and privacy compliance obligations with an enterprise ready SDDC that leverages both on-premises and cloud resources for rapid application portability and operational consistency across the entire environment.

Structure of the MTCS Standard

In the pages that follow we will provide specific details on how VMware Cloud on AWS addresses the compliance guidelines set forth by Singapore MTCS.

	MTCS Structure
(a)	CORE INFORMATION SECURITY
	Cloud Governance
1	Information Security Management
2	Human Resources
3	Risk Management
4	Third Party
5	Legal and Compliance
6	Incident Management
7	Data Governance
	Cloud Infrastructure Security
8	Audit Logging and Monitoring
9	Secure Configuration
10	Security Testing and Monitoring
11	System Acquisition and Development
12	Encryption
	Cloud Operations Management
13	Physical and Environmental Security
14	Operations
15	Change Management
16	Business Continuity Plan and Disaster Recovery
(b)	CLOUD SPECIFIC INFORMATION SECURITY
17	Cloud Services Administration
18	Cloud User Access
19	Tenancy and Customer Isolation

(a) CORE INFORMATION SECURITY

MTCS Category	VMware Response
Cloud Governance	
Information Security Management Information security management controls ensure that information security is managed within the Cloud Service Provider's overall administrative structure. These include establishment of information security roles, responsibilities, coordination, and information security policies and standards, as well as demonstration of Cloud Service Provider's management involvement with information security	VMware Cloud on AWS has established an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. VMware has documented policies, standards and system and network diagrams supporting VMware Cloud on AWS. VMware documents, updates, and maintains baseline configurations for software and hardware installed in the production environment; changes are governed by a defined change management policy and baseline configurations are securely managed. VMware also utilizes internal and external audits to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and to identify areas of improvement. Audits are essential to the VMware continuous improvement programs In addition, VMware has also defined roles and responsibilities of staff involved in information security management of VMware Cloud on AWS service. Some of the key roles include: • Chief Security Officer: The Chief Security Officer (CSO) provides executive sponsorship of the VMware information security management policy, procedures, program, and team. • The VMware Security Incident Response Team (vSIRT) is responsible for developing breach handling procedures, forensics, and they handle incident management across VMware. • VMware Security Operations Center monitors information security events across various systems. The VMware Security Operations Center (SOC) team takes reported security events and escalates to the VMware Security Incident Response Team (vSIRT) for security incident management as appropriate based on defined criteria.
Human Resources Human resources security controls ensure that all employees and third parties are suitable for their roles prior to employment or contracting and that they understand their responsibilities, employment and contract terms and conditions (including termination) to reduce the risk of theft, fraud or misuse of facilities	VMware has established a Human Resources Information Security Policy that describes the requirements for implementing background checks and contractual requirements during the recruitment of employees and consultants. VMware also maintains Business Conduct Guidelines which explain how employees are expected to conduct themselves in a manner that reflects VMware's values, demonstrated ethical leadership, and promotes an environment that upholds our reputation for integrity, honesty, accountability, transparency, and trust. Business Conduct Guidelines training is required upon hire and annually for employees. VMware conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to the service. Applicable policies are reviewed at planned intervals by VMware. VMware Acceptable Use Policy applies to VMware employees, consultants, agents, vendors, and other independent contractors who have access to information systems and assets owned or leased by VMware, connected to a VMware network or residing at a VMware location. The use of VMware information and VMware information systems shall be managed responsibly by users to maintain the appropriate confidentiality, integrity, and availability of data and the infrastructure supporting the enterprise. VMware has also implemented information security training and awareness program in alignment with the ISO 27001 standard, new employees have to undertake security awareness training upon joining and VMware personnel are required to complete annual security awareness training. Personnel supporting VMware managed services receive additional role-based security training to perform their job functions in a secure manner.

Risk Management Risk management controls ensure that a cloud-specific risk management programme is established to identify, quantify, prioritise, and mitigate or resolve risks impacting the cloud service operations and information assets. Maintenance of risk register by the Cloud Service Provider is essential to ensure risks affecting the cloud environment tare tracked and followed up to closure	In alignment with the ISO 27001 standard, VMware maintains a risk management program to mitigate and manage risk. Risk assessments are performed at least annually to ensure appropriate controls are in place to reduce the risks related to the confidentiality, integrity, and availability of sensitive information. Risks identified during the risk assessment process are ranked and formally documented along with mitigation strategies. A formal process is documented to guide personnel when performing a risk assessment. The framework security requirements have been designed and implemented to address industry best practices around security and privacy. This requires the identification of applicable regulatory and contractual requirements, technical compliance with information security policies, protection of records, protection of information systems audit tools, and audit controls and reporting. This policy also requires VMware to adhere to the applicable legal, statutory, regulatory, or contractual obligations related to information security and security requirements. In addition, VMware's management and oversight bodies, where applicable, ensure that risk management is integrated into organizational activities by documenting risk management plans. Management ensures that the necessary resources are allocated to managing risk by assigning authority, responsibility, and accountability at appropriate levels within the organization.
Third Party Third party security controls ensure that the Cloud Service Provider has an effective control framework over its third party service providers supporting the cloud environment. The controls include third party service providers' due diligence, agreement, delivery management, assurances over their performance and compliance with internal controls.	VMware has a Third-party Risk Management Policy. This policy applies to VMware's management and oversight of third parties (vendor /supplier) accessing or processing company data facilities, information and/or information systems. It defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. Sourcing and business teams collaborate with the information security risk team to ensure a risk-based approach is taken with respect to third parties to ensure the security of information assets. VMware conducts security risk assessment on third parties that may have access to VMware's non-public information prior to working with VMware. Based on risk and business impact, periodic reviews and/or audits are conducted where there is determined to be a change to the third-party profile. VMware monitors, reviews, and audits third party service delivery to ensure alignment with agreed level of information security and service delivery in line with the third-party agreement. Based on risk and business impact, changes to the provision of services by the third party will be appropriately managed. VMware manages third party relationships and addresses any deficiencies in the third party's capabilities to securely deliver the services. Based on the risk and business impact VMware obtains completed third party security questionnaires from suppliers under the above scenarios if not already on file or not updated within the past 12 months.
Legal and Compliance Legal and compliance controls ensure that Cloud Service Provider and its third party service providers conform to the Cloud Service Providers' information security and risk management policies, standards, and procedures and contractual obligations.	VMware has an established Legal team that guides VMware's business units and functions in the areas of contracts, product development and launch, licensing, open source software, strategic alliances and ecosystem development, corporate marketing and communications, standards setting organizations, competition law and strategic corporate procurement. VMware also has an Information Security Compliance team that is responsible for implementation of security programs such as security training and awareness, information security governance reviews, vendor risk management and information security contract reviews, and compliance audits. VMware has a compliance program in place that is designed after several industry standards and frameworks including ISO 27001, ISO 27017, ISO 27018 and SOC 2. The program utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also to identify areas of improvement.
Incident Management	VMware has a documented security incident management policy which is reviewed every 12 months. VMware has also incident response program, plans, and procedures documented and implemented.

Incident management controls ensure that information security events and weaknesses impacting the information assets and systems in the cloud environment are communicated timely and in accordance with a set of pre-defined procedures for appropriate corrective measures to be taken. Incidents may encompass malicious and non-malicious events including unauthorised hardware or software modification, unauthorised access to systems or data, malware and other events that may impact confidentiality, integrity or availability.	VMware provides incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to availability of the service offering. Customers are responsible for incident and problem management (e.g., detection, severity, classification, recording, escalation, and return to service) for virtual machines that they have deployed in a SDDC. VMware has also defined roles and responsibilities of staff involved in incident management processes within the security incident management policy. Some of the key staff/teams include: • Chief Security Officer: The Chief Security Officer (CSO) provides executive sponsorship of the VMware security incident response policy, procedures, program and team. The CSO or his/her delegate are responsible to identify individual members from multiple departments and physical locations in VMware to establish security incident response team. • The Director, Threat Management, has the role of VMware Security Incident Response Team (vSIRT) program manager. The Director, Threat Management, shall approve the development and refinement of the incident response policy, standards, procedures, tools, and capabilities • vSIRT is responsible for developing breach handling procedures, forensics, and they handle incident management across VMware. • VMware Security Operations Center (SOC) monitors information security events across various systems. The SOC team takes reported security events and escalates to vSIRT for security incident management as appropriate based on defined criteria The vSIRT team is notified by the Security Operations Center of any potential breach and participates in any investigation. If VMware becomes aware of a security incident on VMware Cloud on AWS that leads to the unauthorized disclosure or access to personal information provided to VMware as a processor, we will notify customers without undue delay, and will provide information relating to a data breach as reasonably requested by our customers. VMware will use reasonable efforts to assist customers in mitigating, where possible, the adverse effects of any personal data breach.
Data Governance Data governance controls ensures that only authorised users have access to the data stored in a cloud environment at all times. Procedures to govern data such as classifying data, maintaining data ownership, secure data handling, and secure data disposal shall be established to prevent loss, misuse or unauthorised disclosure of sensitive data	VMware Cloud on AWS operates a Shared Responsibility Model for provision of service. Customers are responsible for controlling access to the content, including the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. Access to customer content is governed by each customer's use of authentication and authorization mechanisms. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users. For more details on shared responsibility model, please see the Shared Responsibility Model whitepaper at *https://cloud.vmware.com/vmc-aws/resources#whats-new*. VMware Cloud on AWS gives customers full control over their virtual machines and their content. Documentation exists along with additional tools and services to facilitate the migration of data. VMware Cloud on AWS natively runs VMware vSphere which stores customer data in a widely adopted virtual machine format, and vSphere natively supports the Open Virtualization Format (OVF), making it simple to download, clone, migrate, copy, port, or transfer workloads between environments. Additionally, customer may use the VMware Hybrid Cloud Extension service for bulk migrations of virtual machine images between cloud providers. These capabilities make it simple to download, clone, migrate, copy, port, or transfer workloads.

	It is important to note that VMware does not back-up or archive customer content. Automated processes handle media sanitization before repurposing of any hardware. Any deletion of a host on VMC results in an automated cryptographic wipe of the hard drive is performed via destruction of keys used by the self-encrypting drives. When a physical storage device has reached the end of its useful life, a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals is followed using techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. *From AWS regarding security & Compliance: Data Destruction* Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned. *3rd party security attestation* Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment. https://aws.amazon.com/compliance/data-center/controls/

MTCS Category	VMware Response
Cloud Infrastructure Security	
Audit Logging and Monitoring Audit logging and monitoring controls ensure that activities performed and events occurred in the cloud environment are being tracked and maintained for a period of time to detect any unauthorised activities and to facilitate investigation and resolution in the event of security incidents (e.g. access violations).	VMware Cloud on AWS service continuously collects and monitors the environment logs, which are correlated with both public and private threat feeds to identify suspicious and unusual activities. Physical and logical user access to audit logs is restricted to authorized personnel. Restricted, authorized personnel have access to the definitive central log servers for the VMware Cloud on AWS servers. The customer's access logs are replicated to other systems where they can be viewed by customers and other individuals with appropriate approvals. Audit logs are centrally stored and retained whenever required. The logs are monitored and reviewed for security events by the VMware Security Operations Center 24 hours a day, 7 days a week and the audit logging and monitoring controls are audited annually by internal and/or external parties. VMware has an intrusion detection system and other tools in place that continuously monitor for deviations in production from our baseline configurations and generate alerts monitored by the VMware SOC. Higher levels of assurance are required for the protection, retention, and lifecycle management of the VMware Cloud on AWS platform services audit logs. This ensures audit logs adhere to applicable legal, statutory, or regulatory compliance obligations; provide unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies; and support forensic investigative capabilities in the event of a security breach. VMware has implemented a secure logging pipeline with security and WORM policies to ensure log files are protected from unauthorized access, viewing, tampering, or deleting. Audit logs cannot be altered by enforcement of a tightly controlled access policy that is monitored in real-time. A storage policy enforces retention of 3 years and automatically purges log files that

	exceed the 3-year lifecycle. This logging pipeline feeds audit logs into a SIEM that is monitored by the VMware SOC that is operated by highly trained VMware security analysts 24x7x365. VMware vRealize Log Insight Cloud service can forward any log events it receives from the VMware Cloud on AWS SDDC. When you configure log forwarding, you specify a filter to select which events are forwarded. You can also further forward the SDDC audit logs sent to VMware vRealize Log Insight Cloud to downstream solutions including vRealize Log Insight, Splunk, or another destination.
Secure Configuration Secure configuration controls ensure that the systems in the cloud infrastructure and the supporting networks are designed and configured securely to prevent against unauthorised entry points or malicious activities through weak system configurations. Timely updates of vendor released patches are also critical to circumvent threats arising from newly discovered vulnerabilities.	VMware has documented policies, standards, and system and network diagrams supporting VMware Cloud on AWS. VMware documents, updates, and maintains baseline configurations for software and hardware installed in the production environment; changes are governed by a defined change management policy and baseline configurations are securely managed. Security baselines are documented to guide personnel to ensure appropriate configurations are in place to protect sensitive information. VMware follows security baseline configuration that includes pre-implementation approvals and alignment with industry benchmarks. . Security baseline configuration changes are reviewed for approval in a timely manner. VMware utilizes private networks and network security solutions, including firewalls and intrusion detection systems. VMware infrastructure is designed to ensure that networks and associated applications and systems are managed and monitored in such a manner as to prohibit unauthorized access. Key elements include network controls, configuration (default deny, firewalls, reviews), change management, connections/ connectivity, application policies, logging, documentation, audits, IP address, and protocol policies. VMware Cloud on AWS SDDCs are protected by two levels of network security and isolation leveraging AWS VPCs along with VMware NSX to provide granular segmentation and network security. VMware utilizes firewalls and additional AWS security services along with Cloud Trail logs and VPC Flow Logs. VMware continuously collects and monitors services operation logs using SIEM technologies. The 24x7x365 VMware Security Operations Center uses the SIEM to correlate information with public and private threat feeds to identify suspicious and unusual activities. VMware Cloud on AWS ensures that the VMC console, (a public-facing web application), and API endpoints are protected by a web-application firewall - WAF to continually inspect network traffic and defend the console by detecting and preventing web-based attacks. VMware assesses vulnerabilities across VMware Cloud on AWS platform information systems and applications on a regularly scheduled basis and whenever new potential vulnerabilities are reported or detected, using a wide range of tools and techniques including but not limited to scan engines, port discovery, and service fingerprinting. VMware patches or upgrades platform systems and applications after analyzing the severity and impact of potential vulnerabilities. VMware has subscriptions to pertinent vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical and high vulnerability patches are installed in a timely manner. Non-critical patches are included in the pre-defined patch schedule and applied within commercially reasonable timeframes. Changes are made using industry best practices. Patch testing and rollback procedures are completed by the QA department to ensure compatibility with and minimal impact to the production environment.
Security Testing and Monitoring	**Vulnerability management**: VMware has an established vulnerability management policy and vulnerability management standard that formalizes the Vulnerability Management program at VMware. The policy and standard are reviewed on an annual basis.

With the continuous introduction of vulnerabilities and malware in the cloud environment, security testing and monitoring controls are required to extend across multiple aspects of the cloud, including services, virtual machines and physical infrastructure. It is also essential to reaccredit the cloud's IT security and related processes in a proactive and timely manner.	VMware assesses vulnerabilities across VMware Cloud on AWS platform information systems and applications on a regularly scheduled basis and whenever new potential vulnerabilities are reported or detected, using a wide range of tools and techniques including but not limited to scan engines, port discovery, and service fingerprinting. VMware patches or upgrades platform systems and applications after analyzing the severity and impact of potential vulnerabilities. VMware has subscriptions to pertinent vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical and high vulnerability patches are installed in a timely manner. Non-critical patches are included in the pre-defined patch schedule and applied within commercially reasonable timeframes. Changes are made using industry best practices. Patch testing and rollback procedures are completed by the QA department to ensure compatibility with and minimal impact to the production environment. **Penetration testing:** As a part of the vulnerability management program, penetration tests are performed at least annually. Results are reviewed by the VMware security team(s) and remediation is performed based on the auditor recommendations and security team's guidance. In order to achieve more meaningful test results, VMware uses both white and gray box testing. A gray box approach is a mixture of black box and white box testing. White box testing means that the source code will be made available and black box testing means that the actual penetration test will be performed without any source code access. The gray box method enables the vendor performing the penetration test to have source code available to assist with penetration testing. This results in a more robust set of tests because the consultants can achieve deeper and broader access since they spend less time breaking into targeted assets. The third-party vendors have signed NDA agreements with the company and are allowed access to view source code at approved VMware facilities to help with finding attack vectors. VMware utilizes trained and experienced internal Information Security staff as well as third parties security auditors to periodically perform comprehensive penetration testing of systems and applications. **Security Monitoring:** VMware Cloud on AWS has several intrusion detection mechanisms in place and the service continuously collects and monitors the environment logs which are correlated with both public and private threat feeds to identify suspicious and unusual activities on service platform systems. VMware Cloud on AWS benefits from AWS's employment of various technologies that monitor configuration changes in the cloud infrastructure in near real-time (collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes). Additional capabilities are used to block network attacks (DDoS, MITM, IP Spoofing, and port scanning) through Internet access diversity, SSL protected endpoints, SSH host key regeneration, restrictive host-based firewall infrastructure, and reactive scanning detection backed by a strictly enforced Acceptable Use Policy. VMware has a compliance program in place that is designed after several industry standards and frameworks including ISO 27001, ISO 27017, ISO 27018, and SOC 2. The program utilizes internal and external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also to identify areas of improvement.
System Acquisition and Development System acquisitions and development security controls ensure that security is an integral	VMware's Security Development Lifecycle (SDLC) processes and change management processes are in place to ensure appropriate reviews and authorizations are in place prior to implementing any new technologies or changes within the production environment. Change management policies and processes are also in place to guide management authorization of changes applied to the production environment. Change management policy is reviewed every 12 months.

part of the information systems as well as the business processes associated with these systems. Software solutions acquired or built for the information systems in the cloud environment should be tightly controlled and tested prior to release or deployment, to prevent introduction of malware or security vulnerabilities due to mismanaged codes.	As part of the SDLC, VMware uses both manual and automated source code analysis tools to detect security defects in code as well as security vulnerabilities in applications multiple times prior to production. Vulnerabilities posing a significant risk are addressed prior to deployment. VMware verifies that software suppliers adhere to industry standards for SDLC security using its comprehensive vendor risk management process that includes review of our vendor's security controls, development processes, privacy controls, business conduct, and third-party audit reports and certifications. Change requests are documented in the change request tracking system and the required change management fields are completed. Change review and analysis are performed which include a risk assessment and analysis of the impacts of changes and specification of information security controls needed. The change request must be approved by appropriate personnel. VMware Cloud on AWS has a comprehensive testing system that covers the entire lifecycle of the release. Continuous testing occurs on the software development pipelines for individual products and components. VMware generates builds from approved components and runs these through BITs (Basic Integration tests), PVTs (Product Validation Tests), FS Lite (Feature Stress Lite tests), and continuous Loop tests for Deployment, Upgrade, and Cluster expansion / reduction across the supported regions. Additionally, we run performance tests, feature stress tests, security scans, vulnerability tests, and system tests at scale for every cycle. VMware has also established emergency change management procedures to manage any urgent change requests or response to incidents. VMware has well established controls in place to protect and control access to production systems and source code. Source code is restricted to authorized personnel only and is continuously monitored. No code can be inserted into a production release without multiple iterations of reviews, approvals, and security testing. Our SDLC processes are included in scope for annual SOC 2 audit which thoroughly inspects processes related to source code control and promotion into production. VMware Cloud on AWS implements a modern distributed control plane the is deployed in multiple AWS regions which are updated in a CI/CD model that ensures that components are updated in a timely fashion. During system maintenance and upgrades customers can utilize status.vmware-services.io to monitor status of the service.
Encryption Encryption and secure cryptographic key management ensures that sensitive information (i.e. trade secrets, personal medical information, credentials, and financial records) in transmission or in storage electronically is being protected against unauthorised use or disclosure.	VMware Cloud on AWS uses multiple levels of encryption in order to secure the contents of the SDDC and communications with the SDDC. a. Virtual Machines deployed in VMware Cloud on SDDCs may be encrypted using a number of in-guest encryption solutions. Customers that require VM level encryption are responsible for deploying and maintaining such solutions as is specified in the Shared Responsibility Model. b. VMware Cloud on AWS SDDCs implement VMware NSX network security that enable customers to create IPsec VPN encrypted connectivity between sites. c. VMware Cloud on AWS SDDCs implement vSAN Encryption that provides strong encryption for storage. Customers have the ability to rotate the data encryption Keys on-demand via vSphere UI and API d. Connectivity to management interfaces provided in VMware Cloud on AWS is performed via encrypted channels using TLS security. VMware Cloud on AWS customer data is encrypted by default using vSAN XTS AES-256 encryption with two levels of keys: key encryption key (KEK) and per-disk data key (DEK). The AWS Key Management Service (KMS) provides Envelope Encryption to protect the vSAN generated data keys. A unique AWS account is created for each customer and a unique AWS Key Management Service (KMS) generated Customer Master Key (CMK) is used to encrypt the vSAN data encryption key (KEK). Leveraging the AWS KMS enhances the security of the data encryption keys by providing a secure mechanism outside of the SDDC to encrypt and distribute

	the data encryption keys to vSAN Hosts. VMware provides for vSAN data key rotation in the vSphere UI and API as required by the customer. For additional detail: https://nicovibert.com/2019/01/22/encryption-on-vmware-cloud-on-aws-at-rest-and-in-transit/ As part of the shared responsibility model, customers are responsible for securing their sensitive data with in-guest encryption and/or application encryption software that may offer options for alternative key management systems to enable full control of the key management lifecycle.

MTCS Category	VMware Response
Cloud operations management	
Physical and environmental Physical and environmental security controls prevent unauthorised physical access, damage or interference to the cloud environment and infrastructure with the use of appropriate procedures and assessments(i.e. threat and vulnerability risk assessments) to identify risks and protect information assets.	VMware Cloud on AWS runs on AWS-provided servers that are located in AWS data centers. AWS security management standards follow the best practices and comprehensive security controls of ISO/IEC 27001:2013. AWS manages physical access to data centers as defined in the AWS Data Center Physical Security Policy. Physical Access is strictly controlled both at the perimeter and at building ingress/egress points and includes, but is not limited to fencing, walls, video surveillance, intrusion detection systems and other electronic biometric access controls and alarm monitoring systems managed by a 24x7x365 professional security staff. For more information on AWS controls, please visit: *https://cloudsecurityalliance.org/star/registry/amazon/* and data centers *https://aws.amazon.com/compliance/data-center/data-centers/* AWS performs regular audits of their physical infrastructure. For more information on AWS data center security controls and compliance reports, please visit *https://aws.amazon.com/compliance/* For more information please see *http://aws.amazon.com/security* AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. AWS monitors critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Through the use of Availability Zones and data replication, customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. AWS monitors and performs preventive maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventive maintenance is performed to maintain the continued operability of equipment. AWS handles physical equipment lifecycle. AWS uses techniques described in industry-accepted standards to ensure that data is erased when resources leave the service. When a storage device has reached its end of life, and to ensure that no residual data can be exposed, AWS follows the procedures detailed in DoD 5220.22-M (“National Industrial Security

	Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"). This includes degaussing and physically destroying magnetic storage devices.
Operations Operations security controls ensure that the operations of the cloud's information processing facilities are documented, secure, reliable, resilient and recoverable.	VMware has a defined Information Security Program that includes Business Continuity and Disaster Recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. This program implements appropriate security controls to protect its employees and assets against natural and man-made disasters. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training. VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. Risk assessment is performed on a regular basis to identify natural and man-made threats based upon a geographically specific business impact assessment. Reviews are triggered through change management, new projects, and critical process reviews. The resulting security mechanisms and redundancies are in turn reviewed through regular audits. VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify dependencies, critical products, and services. The real-time status of the VMware Cloud on AWS along with past incidents is publicly available at https://status.vmware-services.io/. Customers have the ability to architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. For example, an SDDC may be deployed as a "stretched cluster" that provisions hosts in 2 distinct availability zones. Customers retain control and ownership of their customer content and have the ability utilize their own backup and recovery mechanisms. VMware Cloud on AWS SDDC also has an optional (paid) disaster recovery feature called VMware Site Recovery that greatly simplifies disaster recovery management and operations. VMware has established RTO and RPO for cloud services. VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as multiple geographic regions. Each Availability Zone is designed as an independent failure zone. In case of failure, customers can configure automated processes to move customer data traffic away from the affected area. The architecture of the AWS infrastructure provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. VMware monitors AWS infrastructure and receives notifications directly from AWS in the event of a provider failure. VMware has developed processes with AWS to ensure that that we have defined disaster recovery mechanisms in place in the event that an upstream event occurs. VMware Cloud on AWS has conducted successful DR testing and continues to test annually. VMware has made SLAs, Terms of Service, Data Processing Addendums, Privacy notices publicly available. They can be found here: VMware Cloud on AWS Service Description *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf* VMware Cloud on AWS Service Level Agreement *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf* VMware Universal End User License Agreement (EULA): *https://www.vmware.com/download/eula.html* Data Processing Addendum https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-data-processing-addendum.pdf

	VMware Privacy Policy *https://www.vmware.com/help/privacy.htm* The above documents cover terms and conditions across various areas such as governance, risk management, disaster recovery arrangements, sub-processors and compliance with applicable laws and regulations. VMware Cloud on AWS provides a dedicated environment to customers. VMware Cloud on AWS continuously monitors platform metrics to ensure sufficient capacity for customers in each data center. https://status.vmware-services.io/ is used to communicate services status outages and is updated in real time.
Change Management Change management controls ensure that changes to the cloud infrastructure are carried out in a planned and authorised manner. These include documenting and assessing the change required, identifying the specific configurations and IT services affected by the change, planning the change, testing the change and having a rollback plan should the change have an adverse effect on the components	VMware's Security Development Lifecycle (SDLC) processes and change management processes are in place to ensure appropriate reviews and authorizations are in place prior to implementing any new technologies or changes within the production environment. Change management policies and processes are also in place to guide management authorization of changes applied to the production environment. Change management policy is reviewed every 12 months. Change requests must be documented in the change request tracking system and the required change management fields are completed. Change review and analysis are performed which include a risk assessment and analysis of the impacts of changes and specification of information security controls needed. Change requests must be approved by appropriate personnel. VMware Cloud on AWS has a comprehensive testing system that covers the entire lifecycle of the release. Continuous testing occurs on the software development pipelines for individual products and components. VMware generates builds from approved components and runs these through BITs (Basic Integration tests), PVTs (Product Validation Tests), FS Lite (Feature Stress Lite tests) and continuous loop tests for deployment, upgrade, and cluster expansion / reduction across the supported regions. Additionally, we run performance tests, feature stress tests, security scans, vulnerability tests, and System Tests at scale for every cycle. VMware has also established emergency change management procedures to manage any urgent change requests or response to incidents. Procedures for aborting and recovering from unsuccessful changes are documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities are noted for the recovery and continuity of the affected areas. Fall back procedures are in place to ensure systems can revert back to what they were prior to implementation of changes VMware has well established controls in place to protect and control access to production systems and source code. Source code is restricted to authorized personnel only and is continuously monitored. No code can be inserted into a production release without multiple iterations of reviews, approvals and security testing. VMware Cloud on AWS implements a modern distributed control plane the is deployed in multiple AWS regions which are updated in a CI/CD model that ensures that components are updated in a timely fashion. VMware has policies and procedures in place to ensure that test data is not used in production environments. Development, QA, and production use separate equipment and environments and are managed by separate teams. VMware Cloud on AWS regularly performs updates on your SDDCs. VMware Cloud on AWS notifies customers of changes to each customer environment in advance, and if we have occasionally access systems supporting a customer environment to troubleshoot an infrastructure rollout or operational issue that is SLA impacting. These updates ensure continuous delivery of new features, new functionality and bug fixes, and maintain consistent software versions across the SSDC fleet. When an SDDC update is upcoming, VMware sends a notification email to you. Typically, this occurs 7 days before a regular update and 1-2 days before an emergency update. You also receive notifications by email when each phase of the update process starts, completed, is rescheduled, or is cancelled.

Business Continuity Planning and Disaster Recovery Business continuity planning and disaster recovery controls ensure timely resumption from, and the possible prevention of interruptions to business activities and processes caused by failures of information systems and disasters.	VMware has a defined Information Security Program that includes Business Continuity and Disaster Recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. This program implements appropriate security controls to protect its employees and assets against natural and man-made disasters. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training. VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. A Risk Assessment is performed on a regular basis to identify natural and man-made threats based upon a geographically specific business impact assessment. Reviews are triggered through change management, new projects, and critical process reviews. The resulting security mechanisms and redundancies are in turn reviewed through regular audits. VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify dependencies, critical products, and services. The real-time status of the VMware Cloud on AWS along with past incidents is publicly available at *https://status.vmware-services.io/.* VMware Cloud on AWS is architected to be highly available. In the event of a hardware failure, this unique cloud service is configured to automatically migrate to, or restart workloads on another host machine in the cluster and automatically restart the failed host. If the host machine fails to restart, or the performance of the restarted host is degraded, the service is capable of automatically replacing the failed host in a cluster with an entirely new host within minutes. Customers have the ability to architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. For example, an SDDC may be deployed as a “stretched cluster” that provisions hosts in 2 distinct availability zones. Customers retain control and ownership of their customer content and have the ability utilize their own backup and recovery mechanisms. VMware Cloud on AWS SDDC also has an optional (paid) disaster recovery feature called VMware Site Recovery that greatly simplifies disaster recovery management and operations. For details on these unique capabilities, please see the VMware Cloud on AWS service description *https://www.vmware.com/content/dam/digitaCustomerarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf* VMware has established RTO and RPO for cloud services. VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as multiple geographic regions. Each Availability Zone is designed as an independent failure zone. In case of failure, customers can configure automated processes to move customer data traffic away from the affected area. The architecture of the AWS infrastructure provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. VMware monitors AWS infrastructure and receives notifications directly from AWS in the event of a provider failure. VMware has developed processes with AWS to ensure that that we have defined disaster recovery mechanisms in place in the event that an upstream event occurs. VMware Cloud on AWS has conducted successful DR testing and continues to test annually.

(b) Cloud Specific Information Security

MTCS Category	VMware Response
Cloud Services Administration Cloud services administration controls ensure the enforcement of policies, standards and procedures relating to the creation, maintenance and removal of privileged accounts used for managing cloud services and supporting networks. As privileged accounts have extensive access rights on the systems and infrastructure in the cloud environment and are the primary targets for attackers, itis essential that these accounts are secured and tightly controlled. These controls apply to all accounts with access to the Cloud Service Management Network and accounts within the Cloud Service Delivery Network controlled by the Cloud Service Provider.	VMware has implemented a shared responsibility model that outlines the responsibility of VMware and cloud tenants. As part of this model, each customer is responsible for protecting customer content contained in their tenant space, applications, and access to their SDDCs on networks that they configure. Access to customer content, is solely governed by each customer's use of authentication and authorization mechanisms to secure access to VMs, applications and filesystems that hold their data. For more information about VMware Security programs: https://www.vmware.com/security.html Access privileges to VMware systems are controlled based on the principle of least privilege – only the minimum level of access required shall be granted. Access policy is based on an individual's "need to know," as determined by job functions and requirements. Access privileges to computers and information systems are authorized by the appropriate level of management and documented prior to being granted. Managing access to information systems is implemented and controlled through centralized identity stores and directory services. VMware has established an authentication and password policy that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC 2 report. To support the VMware Cloud on AWS platform, a tightly controlled "Delegated Access" process is in place that enables only VMware engineers with the appropriate permissions to authenticate (using MFA) to a system to generate one-time use credentials that are user-specific with limited time-bound access to troubleshoot and remediate issues on the physical hosts, hypervisors and service management appliances. Access must be tied to a support ticket and access is logged & monitored and any suspicious activity is investigated by VMware's Security Operations Center (SOC). The audit log information that is collected by VMware Cloud on AWS is limited to the SDDC operating environment, including vCenter, ESXi and the VMC management appliances that support functionality and service the SDDC. These audit logs apply only to administrative activity recorded in Administrative logs for security monitoring purposes. Logs are encrypted in motion and at rest. User Information is limited to information used to self-service administration of the VMware Cloud on AWS service (username, IP address, email address). The 24x7x365 VMware Security Operations Center utilizes SIEM technologies to monitor the audit logs to identify suspicious and unusual activities. Physical and logical user access to audit logs is restricted to authorized personnel. Restricted, authorized personnel have access to the definitive central log servers for the VMware Cloud on AWS servers. The customer's access logs are replicated to other systems where they can be viewed by customers and other individuals with appropriate approvals. Audit logs are centrally stored and retained whenever required and are monitored and reviewed for security events by the VMware Security Operations Center 24 hours a day, 7 days a week. VMware has implemented a secure logging pipeline with security and WORM policies to ensure log files are protected from unauthorized access, viewing, tampering, or deleting. Audit logs cannot be altered by enforcement of a tightly controlled access policy that is monitored in real-time. A storage policy enforces retention of 3 years and automatically purges log files that exceed the 3-year lifecycle. This logging pipeline feeds audit logs into a SIEM that is monitored by the VMware SOC that is operated by highly trained VMware security analysts 24x7x365. VMware vRealize Log Insight Cloud service can forward any log events it receives from the VMware Cloud on AWS SDDC. When you configure log forwarding, you specify a filter to select which events are forwarded. You can also further forward the SDDC audit logs sent to VMware

	vRealize Log Insight Cloud to downstream solutions including vRealize Log Insight, Splunk, or another destination.
Cloud User Access Cloud user access controls ensure that policies, standards and procedures are established and implemented to govern the creation, maintenance and removal of user accounts to restrict access and safeguard user credentials to prevent unauthorised access to information and information systems. There are two components of cloud user access: (i) cloud user's administrator who manages its own environment via an administrative interface, and (ii) end users who access the systems to use specific cloud services.	As part of Shared Responsibility Mode, customers are responsible for managing end-user access to their Software Defined Data Center deployed in VMware Cloud on AWS. Federating corporate domain allows customers to use their organization's single sign-on and identity source to sign into VMware Cloud on AWS. Customers can also set up multi-factor authentication as part of federation access policy settings. Federated identity management allows customers to control authentication to their organization and its services by assigning organization and service roles to their enterprise groups. In VMware Cloud on AWS, the VMware management appliance VMs and customer Workload VMs reside on the VMware managed storage subsystem (encrypted vSAN), meeting requirements for encrypted data at rest. Customer data is stored within customer managed virtual machines to which only customers control access to. In addition, only customers control access to data stored on the associated virtual machine file systems. Virtual machine access is governed by each customer's implementation of an authentication and authorization mechanism, like LDAP services, Microsoft Active Directory services or local accounts configured within the virtual machine operating system. For VMware staff, VMware has implemented HR systems, policies, and procedures are in place to help guide management during termination or change of employment status. Access privileges to systems are removed with a status change. Employees or contractors who change roles within the organization will have access privileges modified according to their new position. A semi-annual access review audit is performed to ensure service access is still appropriate. Controls are in place ensuring timely removal of systems access that is no longer required for business purposes. Entitlement actions are recorded via the systems used to grant/revoke access and provide evidence to support compliance programs. Remediation actions related to access violations will follow user access policies and standard procedures. VMware has established an authentication and password policy that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC 2 report. VMware cloud is hosted within AWS data centers, which follows best practices in data center physical security. AWS data centers are nondescript facilities with military-grade exterior physical security. Personnel who enter the facility are authorized and verified by government issued ID, two-factor authentication at each ingress point. Each ingress point is monitored by video surveillance, and access is logged and audited.
Tenancy and customer isolations In cloud environments, multiple tenants or cloud users share infrastructure and databases in order to gain price and performance advantages and this is known as multi-tenancy. Tenancy and customer isolation controls require the Cloud Service Providers to restrict users' access within the same physical resource and segregate network and	Tenant isolation is employed both in virtual and physical with dedicated hardware per customer. VMware Cloud on AWS customer environments are both logically and physically isolated in the following ways: • VMware Cloud on AWS has independent and comprehensive isolation layers in place to segregate customers' environments. A Software Defined Data Center (SDDC) is deployed in a dedicated AWS Virtual Private Cloud (VPC) that is owned by an AWS Account created exclusively for each customer. Amazon Accounts and Amazon VPC's are the mechanisms implemented by AWS to logically isolate sections of the AWS Cloud for each customer. • VMware Cloud on AWS leverages bare metal servers from AWS to provide each customer with dedicated physical server hardware used to build each VMware cluster. • Customer data imported to VMware Cloud on AWS is stored on dedicated physical hardware, including dedicated local self-encrypting NVME drives. The Self-Encrypting Drives (SED) use AWS 256- bit XTS encryption.

system environments such that the cloud users do not pose a risk to one another in terms of data loss, misuse and privacy violation.	• VMware Cloud on AWS leverages vSAN encryption to protect customer data at rest. VMware vSAN provides storage array level encryption in addition to the existing VMware Cloud on AWS physical disk encryption found on NVMe self-encrypting drives. Encryption is implemented using XTS AES 256 cipher with Intel AES-NI, in both the cache and capacity tiers of vSAN datastores, for industry leading encryption with minimal impact on performance. vSAN enables data security benefits of encryption with no loss of deduplication & compression efficiencies. Each Customer is responsible to encrypt and protect the customer content contained in their tenant space. As part of the shared responsibility model, customers are responsible for securing their sensitive data with in-guest encryption and/or application encryption software that may offer options for alternative key management systems to enable full control of the key management lifecycle. VMware Cloud on AWS have logically separated networks that restrict the customer's access to their own private networks. The services' system and network environments are protected by a firewall or virtual firewall to ensure business and customer security requirements, as well as to ensure protection and isolation of sensitive data. Firewalls act as critical components of the VMware network and information security architecture and are used to restrict and control network traffic and access to systems, data, and applications. VMware firewalls are operated in compliance with the Infrastructure Security policy in order to support the protection of VMware information systems.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.