WHITE PAPER–JULY 2023

Compliance with Reserve Bank of India (RBI) - Master Direction on Outsourcing of Information Technology Services

VMware Cloud on AWS

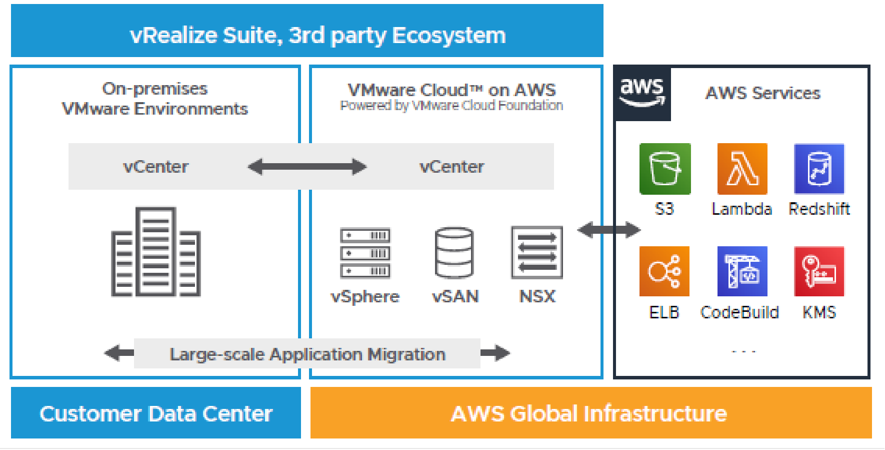
Table of contents

Introduction

In April 2023, the Reserve Bank of India (RBI) published the guidelines for regulated entities (RE) on managing the outsourced serviced providers. This was called the RBI Master Direction on Outsourcing of Information Technology Services. These guidelines cover a wide range of Governance and Security requirements that regulated entities should adopt to effectively manage their outsourced service providers, including cloud service providers. This whitepaper describes the security controls and processes VMware Cloud on AWS has in place to address these RBI Guidelines. Financial Institutions/Regulated Entities 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

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.



Managing outsourcing risk and compliance with VMware Cloud on AWS

VMware has implemented a wide range of security controls to help set up a secure and reliable environment for financial institutions to manage workloads and address various compliance requirements, including the RBI guidelines.

VMware Cloud on AWS 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 the following industry certifications: ISO 27001, ISO 27017, ISO 27018, SOC2 and PCI-DSS. You can view existing compliance certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance* .

Requirements in the RBI Master Direction on Outsourcing of Information Technology Services

The following table describes the requirements in the RBI's circular in the Master Direction on Outsourcing of Information Technology Services and how VMware Cloud on AWS supports these requirements.

RBI Guideline	VMware Response
Evaluation of Engagement of Service Providers	
Due Diligence on Service Providers a) In considering or renewing an Outsourcing of IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. b) A risk-based approach shall be adopted in conducting such due diligence activities. c) Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. Where possible, the RE shall obtain independent reviews and market feedback on the service provider to supplement its own assessment. d) REs shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.	As a cloud provider, VMware Cloud on AWS provides customers with various forms of compliance reports, technical documentation, and whitepapers necessary to conduct due diligence. The purpose of these reports and documents is to help customers and their auditors understand the controls and evidence gathered by 3rd party assessors evaluating support operations, security and compliance programs. VMware Cloud on AWS has been audited for the most of the key industry certifications ISO 27001, ISO 27017, ISO 27018, PCI-DSS, SOC2, OSPAR (Singapore), MTCS (Singapore), IRAP-CSG (Australia) and ISMAP (Japan). For more information on our compliance programs see *Trust Center (vmware.com)*
Outsourcing Agreement	
Legally Binding Agreement REs shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement. b) In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the RE, the associated risks and the strategies for mitigating or managing them. c) The terms and conditions governing the contract shall be carefully defined and vetted by the RE's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the RE to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations. d) The agreement shall also bring out the nature of legal relationship between the parties.	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. *Shared Responsibility Model Overview VMware Cloud on AWS* In line with the shared responsibility model 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 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 is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service. The VMware Cloud on AWS Terms of Service define the contractual conditions under which the VMware Cloud on AWS delivers service and the legal relationship between both VMware and Customer. For information on the terms of service see *VMware ONE Contract Center*

RBI Guideline	VMware Response
Risk Management	
Risk Management Framework: (a) REs shall put in place a Risk Management framework for Outsourcing of IT Services that shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements. (b) The risk assessments carried out by the REs shall be suitably documented with necessary approvals in line with the roles and responsibilities for the Board of Directors, Senior Management and IT Function. Such risk assessments shall be subject to internal and external quality assurance on a periodic basis as determined by the Board-approved policy. (c) REs shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the service provider. (d) Access to data at RE's location / data centre by service providers shall be on need-to-know basis, with appropriate controls to prevent security breaches and/or data misuse. (e) Public confidence and customer trust in REs is a prerequisite for their stability and reputation. Hence, REs shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. Access to customer information by staff of the service provider shall be on need-to-know basis. (f) In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the RE remains responsible for understanding and monitoring the control environment of all service providers that have access to the RE's data, systems, records or resources. (g) In instances where service provider acts as an outsourcing agent for multiple REs, care shall be taken to build adequate safeguards so that there is no combining of information, documents, records and assets (h) The RE shall ensure that cyber incidents are reported to the RE by the service provider without undue delay, so that the incident is reported by the RE to the RBI within 6 hours of detection by the TPSP. (i) The REs shall review and monitor the control processes and security practices of the service provider to disclose security breaches. The REs shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, REs shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management. (j) Concentration Risk: REs shall effectively assess the impact of concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by	In line with the Shared Responsibility Model. Customers are responsible for developing and implementing their risk management framework and processes to identify, measure and manage the reporting of their internal risks assessments. VMware provides customers with documentation to support their internal assessments, including audit reports and technical documentation. VMware Cloud on AWS goes through a rigorous compliance audits every year including SOC2, ISO and PCI-DSS that demonstrate the existence and effectiveness of VMware's internal controls. Customers retain control and ownership of their Customer Content. Access to customer Content, is governed by each customer's use of authentication and authorization mechanisms. VMware does not require any user accounts that would provide VMware employee access to any customer Content. It is the responsibility of customers to implement a structured data-labeling, secure data handling and other security standards to meet their requirements. The VMware Incident response program, plans and procedures are documented and implemented. If VMware becomes aware of a security incident on VMware Cloud on AWS, VMware that leads to the unlawful 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 assesses vulnerabilities across VMware Cloud on AWS platform 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.. Patch testing and rollback procedures are completed by the QA department to ensure compatibility with and minimal impact to the production environment.
Business Continuity Plan and Disaster Recovery Plan a) REs shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced	VMware Cloud on AWS has multiple disaster recovery mechanisms in place to recover from multiple concurrent failures. Redundancy and blast isolation are built into the architecture of the service to ensure high availability of the VMware Cloud on AWS, including regional independence and separation of console availability and customer service availability. VMware Cloud on AWS leverages the specific

RBI Guideline	VMware Response
activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements. b) In establishing a viable contingency plan, REs shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved. c) In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, REs shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations. d) REs shall ensure that service providers are able to isolate the REs' information, documents and records and other assets. This is to ensure that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the RE can be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.	underlying AWS provider's infrastructure to enable customers to run workloads in multiple areas within a region as well as in multiple geographic regions. VMware monitors the service's infrastructure and receives notifications directly from AWS in the event of a failure. VMware has developed processes with AWS to ensure that that we have defined responses in place if an upstream event occurs. The architecture of AWS provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. However, customers who require redundancy of their workloads on another provider can use VMware DRaaS. As a part of the VMware Business Impact Analysis, dependencies on third parties are documented to ensure appropriate business continuity measures are in place. The VMware business continuity plans and documentation are reviewed annually as part of the enterprise independent attestation process. The VMware Information Security Management System (ISMS) is based on the ISO 27001 framework. Business continuity and redundancy plans are reviewed by VMware third-party auditors who will perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under NDA as they become available. Customers can architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. Customers retain control and ownership of their Customer Content and can utilize their own backup and recovery mechanisms including establishing a redundant cloud infrastructure in their own data centers and/or using any one of thousands of VMware partners that run vSphere. Some of these BC/DR options can be automated to reduce changes required to management of customer workloads.
Monitoring and Control of Outsourced Activities	
Monitoring and Control of Outsourced Activities a) REs shall have in place a management structure to monitor and control its Outsourced IT activities. This shall include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc. b) RE shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by RE's internal auditors or external auditors appointed to act on RE's behalf. c) While outsourcing various IT services, more than one RE may be availing services from the same third-party service provider. In such scenarios, in lieu of conducting separate audits by individual REs of the common service provider, they may adopt pooled (shared) audit. This allows the relevant REs to either pool their audit resources or engage an independent third-party auditor to jointly audit a common service provider. However, in doing so, it shall be the responsibility of REs in ensuring that the audit	In line with the Shared Responsibility Model. Customers are responsible for developing and implementing their management structure to monitor the cloud service provider inline with their internal control framework. VMware provides customers with documentation to support their internal assessments, including audit reports and technical documentation. VMware Cloud on AWS goes through a rigorous compliance audits every year including SOC2, ISO and PCI-DSS that demonstrate the existence and effectiveness of VMware's internal controls. To maintain ongoing VMware Cloud on AWS compliance programs, independent 3rd party audits are performed at least annually that include network penetration testing and vulnerability scanning. The results from evidence compiled by 3rd party assessors are published in customer available SOC 2 and ISO 27001 compliance reports. The purpose of these reports is to help customers and their auditors understand the controls and evidence gathered by 3rd party assessors evaluating support operations, security and compliance programs. VMware does not share the details of the penetration testing and vulnerability scanning activities with any external parties to ensure the security of the cloud platform and protection of all customers. Final compliance

RBI Guideline	VMware Response
requirements related to their respective contract with the service provider are met effectively. d) The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact to the RE from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management and in case of any adverse development, the same shall be put up to the Board for information. e) REs, depending upon the risk assessment, may also rely upon globally recognised third-party certifications made available by the service provider in lieu of conducting independent audits. However, this shall not absolve REs of their responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end. f) The RE shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. RE shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience preparedness. g) In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the RE, the same shall be given due publicity by the RE so as to ensure that the customers stop dealing with the concerned service provider. h) REs shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the REs, their auditors, regulators and other relevant Competent Authorities, as authorised under law.	reports are available under NDA. A summary may be provided under NDA to customers. To support customers conduct financial and operational due diligence, VMware provides customers with necessary financial and legal documentation to assess the ability to continue to meet the service provision. Customers should contact their account managers to get any financial and legal reports. In the event of termination, Customers are responsible for backing up Content and migrating all workloads to their target environment, and deleting their SDDCs, prior to termination of their Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service). Termination of service provision is conducted in line with the Terms of Service, see *VMware Cloud Service Offerings*
Outsourcing within a Group/Conglomerate	
Outsourcing within a Group / Conglomerate a) A RE may outsource any IT activity/ IT enabled service within its business group/ conglomerate, provided that such an arrangement is backed by the Board-approved policy and appropriate service level arrangements/ agreements with its group entities are in place. b) The selection of a group entity shall be based on objective reasons that are similar to selection of a third-party, and any conflicts of interest that such an outsourcing arrangement may entail shall be appropriately dealt with. c) REs, at all times, shall maintain an arm's length relationship in dealings with their group entities. Risk management practices being adopted by the RE while outsourcing to a group entity shall be identical to those specified for a non-related party.	N/A for VMware – Customers are responsible for managing governance over their outsourcing activities within their group/conglomerate.

RBI Guideline	VMware Response
Cross-Border Outsourcing	
Additional requirements for Cross-Border Outsourcing a) The engagement of a service provider based in a different jurisdiction exposes the RE to country risk. To manage such risk, the RE shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the RE and the RBI will not be affected even in case of liquidation of the service provider. b) The governing law of the arrangement shall also be clearly specified. In principle, arrangements shall only be entered into with parties operating in jurisdictions upholding confidentiality clauses and agreements. c) The right of the RE and the RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction shall be ensured. d) The arrangement shall comply with all statutory requirements as well as regulations issued by the RBI from time to time.	VMware Cloud on AWS stores Customer Content inside of a geographic region chosen by the customer when they deploy a Software Defined Datacenter (SDDC). These locations include North America, Europe and Asia (Including India). Customer Content will not be relocated, replicated, archived, or copied without the explicit request or actions of the customer administrator. 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 governing law for VMware Cloud on AWS is documented in the VMware Cloud Terms of Service. All services are delivered in line with the contractual clauses agreed in the Terms of Service. See *VMware Cloud Service Offerings*
Exit Strategy	
Exit Strategy a) The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy, the RE shall, inter alia, identify alternative arrangements, which may include performing the activity by a different service provider or RE itself. b) REs shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the RE and new service provider(s) to ensure there is a smooth transition. Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised by the regulator/ concerned RE.	Termination of contract with VMware is managed in accordance with the Termination clauses in the VMware Cloud Terms of Service. See *VMware Cloud Service Offerings* Customers are responsible for backing up Content and migrating all workloads to their target environment, and deleting their SDDCs, prior to termination of their Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service). Customers can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration. For further information, contact a VMware sales specialist. Termination of your Service Offering instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations pursuant to VMware practices.
Usage of Cloud Computing Services	
In addition to the Outsourcing of IT Services controls prescribed in these Directions, REs shall adopt the following requirements for storage, computing and movement of data in cloud environments: 1. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs7. Cloud adoption ranges from moving only non-business critical workloads to the	Moving to VMware Cloud on AWS provides several benefits to customers by providing 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 Sales team can assist customers with getting a deeper understanding of benefits and architecture to

RBI Guideline	VMware Response
cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.	enable customers to develop an appropriate cloud strategy suited to their business goals. VMware assists customers in guiding through their cloud migration journey, including understanding of the costs, benefits of migrating both critical and non-business critical workloads. For more information reach out to your Account Manager.
2. In engaging cloud services, REs shall ensure, inter alia, that the Outsourcing of IT Services policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The REs shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.	VMware Cloud on AWS stores Customer Content inside of a geographic region chosen by the customer when they deploy a Software Defined Datacenter (SDDC). Customer Content will not be relocated, replicated, archived, or copied without the explicit request or actions of the customer administrator. The end-to-end security of the Service Offering is shared between VMware and the customer. Each customer is responsible for protecting all customer Content contained in their tenant space, applications and access to their SDDCs on networks that they configure. Customers are responsible for backing up Content and migrating all workloads to their target environment, and deleting their SDDCs, prior to termination of their Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service).
3. In adoption of cloud services, REs shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the RE and the Cloud Service Provider (CSP). REs may refer to some of the cloud security best practices for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.	The end-to-end security of the Service Offering is shared between VMware and the customer. The primary areas of responsibility between VMware and customers are outlined below. VMware will use commercially reasonable efforts to provide: •Information Security: VMware will protect the information systems used to deliver the Service Offering over which we (as between VMware and customers) have sole administrative level control. •Security Monitoring: VMware will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offering over which we (as between VMware and customers) have sole administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering. •Patching and Vulnerability Management: VMware will maintain the systems we use to deliver the Service Offering, including the application of patches we deem critical for the target systems. We will perform routine vulnerability scans to surface critical risk areas for the systems we use to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner. Each Customer is responsible for addressing the following:

RBI Guideline	VMware Response
	•Information Security: Customers are responsible for ensuring adequate protection of the Content that customers deploy and/or access with the Service Offering. This includes, but is not limited to, any level of virtual machine patching, security fixes, data encryption, access controls, roles and permissions granted to customer internal, external, or third party users, etc. •Network Security: Customers are responsible for the security of the networks over which they have administrative level control. This includes, but is not limited to, maintaining effective firewall rules in all SDDCs that customers deploy in the Service Offering. •Security Monitoring: Customers are responsible for the detection, classification, and remediation of all security events that are isolated with customer deployed SDDCs, associated with virtual machines, operating systems, applications, data, or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which customers are required to participate, and which are not serviced under another VMware security program. Customers must not upload, host, store, or process any Content that is restricted as specified in Section 3.2 of the Terms of Service"
4. Cloud Governance: REs shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, inter alia, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.	VMware takes privacy and data protection very seriously and is committed to providing clear information about how we collect, use and process your personal data. We have established policies and practices designed to protect the personal data we process on behalf of our customers (as a processor), and as a controller. We are also committed to privacy-by-design when designing our products and services and VMware's Privacy Team works with the development teams to identify and embed privacy controls for customers. VMware Cloud on AWS stores Customer Content inside of a geographic region chosen by the customer when they deploy a Software Defined Datacenter (SDDC). In connection with the provisioning of the Service Offering, VMware will process personal data contained in Customer Content (as such term is defined in the relevant VMware agreement, e.g. VMware Terms of Service) on behalf of the Customer. VMware's obligations and commitments as a data processor are set forth in VMware's Data Processing Addendum ("DPA"). VMware will process personal data contained within Customer Content in accordance with the applicable agreement and the DPA. Customers are responsible for developing policies related governance over their cloud providers.

RBI Guideline	VMware Response
5. Cloud Service Providers (CSP) Considerations for selection of CSP: REs shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. REs shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to REs, including those relating to aspects such as data storage, data protection and confidentiality.	As a cloud provider, VMware Cloud on AWS provides customers with various forms of compliance reports, technical documentation, and whitepapers necessary to conduct due diligence. The purpose of these reports and documents is to help customers and their auditors understand the controls and evidence gathered by 3rd party assessors evaluating support operations, security and compliance programs. VMware Cloud on AWS has been audited for most of the key industry certifications ISO 27001, ISO 27017, ISO 27018, PCI-DSS, SOC2, OSPAR (Singapore), MTCS (Singapore), IRAP-CSG (Australia) and ISMAP (Japan). For more information on our compliance programs see *Trust Center (vmware.com)*
6. Cloud Services Management and Security Considerations a) Service and Technology Architecture: REs shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. REs shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the RE. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture should be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data/ information security. .	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. All VMware Cloud on AWS customer environments are both logically and physically isolated in the following three ways: 1. 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. 2. 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. 3. All customer data imported to VMware Cloud on AWS is stored on dedicated physical hardware, including dedicated local self-encrypting self-encrypting NVME drives. The Self-Encrypting Drives (SED) use AWS 256- bit XTS encryption. 4. VMware Cloud on AWS leverages vSAN encryption to protect all 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

RBI Guideline	VMware Response
	leading encryption with minimal impact on performance. vSAN enables data security benefits of encryption with no loss of deduplication & compression efficiencies. 5. 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.
b) Identity and Access Management (IAM): IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented for access to cloud applications.	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 does not require any user accounts that would provide VMware employee access to any customer Content (virtual machines, operating systems, applications, file systems or data). 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
c) Security Controls: REs shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the RE; necessary procedures to authorise changes to cloud applications and related resources	Communication networks that transport sensitive information (authentication, administrative access, customer information, etc.) are encrypted with standard encryption mechanisms. VMware provides customers with the ability to create IPSEC and SSL VPN tunnels from their environments which support the most common encryption methods including AES-256. Also available is AWS Direct Connect to provide a private high bandwidth network connection between AWS and your datacenter, office, or colocation environment.
d) Robust Monitoring and Surveillance: REs shall accurately define minimum monitoring requirements in the cloud environment. REs should ensure to assess the information/ cyber security capability of the cloud service provider, such that, the i) CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats; ii) CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including	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

RBI Guideline	VMware Response
those resulting from changes to information assets or its business environment; iii) nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the RE and the threat environment; and iv) CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.	pertinent vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical and high vulnerabilty 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. VMware has an established third party risk management policy that mandates periodic review, monitor, and audit of third party service delivery to ensure alignment with agreed level of information security and service delivery in line with the third party supplier agreement. Based on risk and business impact, changes to the provision of services by the third-party suppliers shall be appropriately managed.
e) Appropriate integration of logs, events from the CSP into the RE's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud.	VMware vRealize Log Insight Cloud service can forward any log events it receives. When you configure log forwarding, you specify a filter to select which events are forwarded. You can also forward the SDDC audit logs that are automatically sent to VMware vRealize Log Insight Cloud to vRealize Log Insight, Splunk, or another destination.
f) The RE's own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / RE shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.	VMware will maintain the systems we use to deliver the Service Offering, including the application of patches we deem critical for the target systems. We will perform routine vulnerability scans to surface critical risk areas for the systems we use to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner. Customers are responsible for the detection, classification, and remediation of all security events that are isolated with customer deployed SDDCs, associated with virtual machines, operating systems, applications, data, or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which customers are required to participate, and which are not serviced under another VMware security program.
g) Vulnerability Management: REs shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.	VMware has a controlled trusted code build and deployment process using immutable artifacts. VMware has integrated validations that include container signing, certificates and auth token credential processes into the software supply chain to maintain a secure continuous delivery pipeline. VMware uses industry leading code scanning tools to detect potential security issues. VMware identifies security defects using multiple methods which can include automated and manual source-code analysis. Every release of VMware Cloud on AWS goes through a security architectural review, security audits by both the product security teams and the

RBI Guideline	VMware Response
	cloud security teams, manual & automated code analysis, vulnerability scans and additional reviews necessary to meet industry leading security standards. VMware Security personnel must approve each release to validate internal processes and mitigate software security risks to customers.
7. Disaster Recovery & Cyber Resilience a) The RE's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the RE can continue its critical operations with minimal disruption of services while ensuring integrity and security. b) REs shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured, inter alia, through robust incident response and recovery practices including conduct of Disaster Recovery (DR) drills at various levels of cloud services including necessary stakeholders.	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 manmade 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 Cloud on AWS offers the optional an add-on for vSphere Site Recovery Manager (SRM) to automatically restart a workload from any failure in a specific host on another host in the cluster. Site Recovery Manager provides an end-to-end disaster recovery solution that can help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. In the event of a host failure, a new host can be provisioned to a cluster within minutes in order to restore full capacity. The VMware Site Recovery offering provides native hypervisor-based replication using VMware vSphere Replication of workloads between vSphere instances in different regions or customer datacenters.
8. The following points may be evaluated while developing an exit strategy: a) the exit strategy and service level stipulations in the SLA shall factor in, inter alia, i) agreed processes and turnaround times for returning the RE's service collaterals and data held by the CSP; ii) data completeness and portability; iii) secure purge of RE's information from the CSP's environment; iv) smooth transition of services; and v) unambiguous definition of liabilities, damages, penalties and indemnities. b) monitoring the ongoing design of applications and service delivery technology stack that the exit plans should align with. c) contractually agreed exit / termination plans should specify how the cloud-hosted service(s) and data will be moved out from the	Termination of contract with VMware is managed in accordance with the Termination clauses in the VMware Cloud Terms of Service. See *VMware Cloud Service Offerings* Customers are responsible for backing up Content and migrating all workloads to their target environment, and deleting their SDDCs, prior to termination of their Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service). Customers can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration. For further information, contact a VMware sales specialist. Termination of your Service Offering instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the

RBI Guideline	VMware Response
cloud with minimal impact on continuity of the RE's business, while maintaining integrity and security. d) All records of transactions, customer and operational information, configuration data should be promptly taken over in a systematic manner from the CSP and purged at the CSP-end and independent assurance sought before signing off from the CSP.	environments and configurations pursuant to VMware practices.
Audit and Assurance: The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities of both RE and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response, and resilience preparedness and testing, etc.	VMware Cloud on AWS has been audited for most of the key industry certifications ISO 27001, ISO 27017, ISO 27018, PCI-DSS, SOC2, OSPAR (Singapore), MTCS (Singapore), IRAP-CSG (Australia) and ISMAP (Japan). For more information on our compliance programs see *Trust Center (vmware.com)* The SOC2 report lists the customer complementary controls that customers are expected to implement over their environment.

Conclusion

VMware software-defined data center (SDDC) technologies lead the industry in delivering the flexibility, protection, and scalability that financial services organizations need to deliver exceptional customer experiences and new business models across physical, virtual, and cloud environments. VMware has supported a wide range of financial services organizations across the globe to rapidly drive scalability and growth through future ready technology solutions, please visit *https://www.vmware.com/solutions/industry/financial-it-services.html*.

VMware Cloud on AWS will help financial institutions 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 environment.

Contributors

- Moin Nawaz Syed – Product Line Manager, VMware Cloud Solutions
- Patrick O'Brien – Director- Product Management, VMware Cloud Solutions
- Matt Dreyer – Senior Director, Product Management, VMware Cloud Solutions

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