Response To OSPAR (Outsourced Service Provider Audit Report) ABS (Association of Banks) Guidelines

VMware Cloud On AWS

vmware

Contents

Executive Summary

Cloud computing has transformed how financial institutions manage their IT infrastructure. While it has opened opportunities to improve the quality and delivery of banking and financial 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 demand and complying with stringent government mandates surrounding data security and privacy.

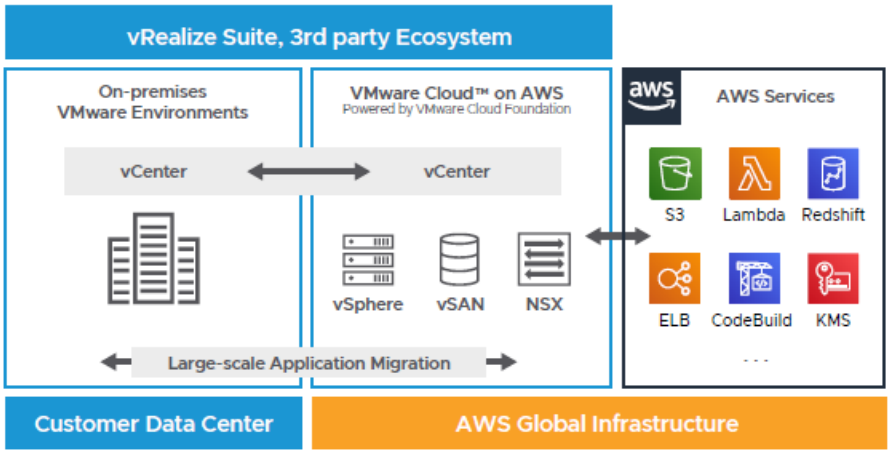
The Association of Banks (ABS) is an organization that represents the interests of commercial and investment banking community in Singapore. ABS have laid out guidelines that financial institutions in Singapore should consider when outsourcing their functions, including cloud outsourcing. The Outsourced Service Provider Audit Report (OSPAR) is based on these guidelines.

This whitepaper provides guidance on how VMware Cloud on AWS addresses the requirements in OSPAR ABS guidelines . Financial institutions can use this whitepaper to understand the controls and processes that VMware Cloud on AWS has implemented to safeguard their workloads and provide customers a reliable infrastructure to meet their business needs.

VMware Cloud on AWS

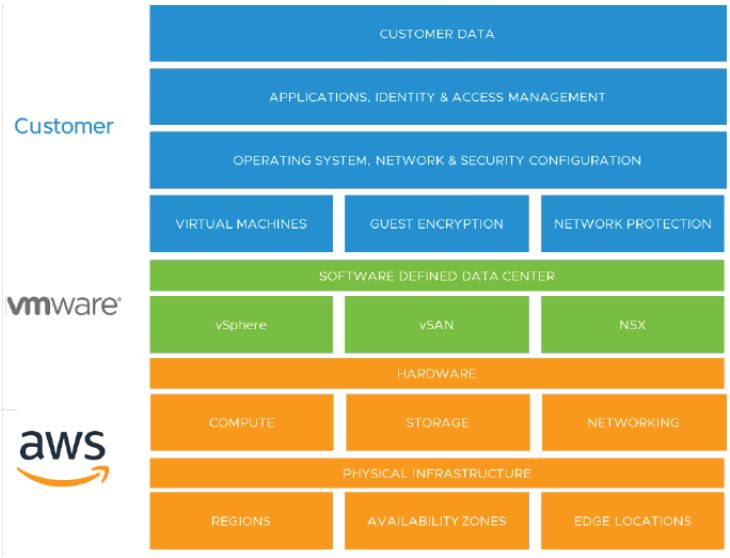
VMware Cloud on AWS brings VMware's enterprise class Software-Defined Data Center software to the AWS Cloud, and enables customers to run production applications across VMware vSphere-based environments, with optimized access to AWS services. Jointly engineered by VMware and AWS, this on-demand service 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 as well as robust disaster protection, 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 delivered and supported 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 outsourcing 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 financial institutions to manage workloads and address various compliance requirements, including the ABS OSPAR guidelines. You can view existing compliance certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance* .

In the sections below, we have demonstrated how VMware Cloud on AWS addresses the requirements in OSPAR ABS guidelines. Financial institutions 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 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, SOC2 and HIPAA. 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 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.

Scope of ABS Controls Applicability

The following table summarizes the applicability of the ABS controls criteria for VMware Cloud on AWS

Sections of the ABS Guidelines	ABS Control Criteria	Applicability (Applicable / Not-Applicable/ Partial-Applicable)
I	**Entity Level Controls**	
(a)	Control Environment	Applicable
(b)	Risk Assessment	Applicable
(c)	Information and Communication	Applicable
(d)	Monitoring	Applicable
(e)	Information Security Policies	Applicable
(f)	Human Resource Policies and Procedures	Applicable
(g)	Practices related to Sub-Contracting	Applicable
II	**General Information Technology (IT) Controls**	
(a)	Logical Security	Applicable
(b)	Physical Security	Applicable*
(c)	Change Management	Applicable
(d)	Incident Management	Applicable
(e)	Backup and Disaster Recovery	Applicable
(f)	Network and Security Management	Applicable
(g)	Security Incident Response	Applicable
(h)	System Vulnerability Assessments	Applicable
(i)	Technology Refresh Management	Applicable
III	**Service Controls**	
(a)	Setting-up of New Clients/Process	Applicable
(b)	Authorising and Processing Transactions	Not applicable
(c)	Maintaining Records	Applicable
(d)	Safeguarding Assets	Applicable
(e)	Service Reporting and Monitoring	Applicable

* VMware Cloud on AWS utilizes Amazon Web Services data centers. Physical security for AWS data centers is managed by AWS. Please visit *https://aws.amazon.com/compliance/data-center/data-centers/* for more information on AWS data center security.

Entity Level Controls Criteria

(a) Control Environment

The control environment sets the priority and culture for the OSP, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure. Aspects of the OSP's control environment may affect the services provided to the FIs. For example, the OSP's hiring and training practices may affect the quality and ability of the OSP's personnel to provide services to the FIs.

ABS Control Criteria	VMWare Response
The control environment includes the following elements: i. Communication and enforcement of integrity and ethical values ii. Commitment to competence iii. Management's philosophy and operating style iv. Organisational structure as well as assignment of authority and responsibility.	
i. Communication and enforcement of integrity and ethical values The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to the ABS controls criteria.	i. VMware is committed to conducting business with integrity and in full compliance with the law. This commitment is the foundation on which we built our Business Conduct Guidelines (BCG). VMware's Business Conduct Guidelines explain how we are expected to conduct ourselves 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 all 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.
ii. Commitment to competence Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting the ABS controls criteria have the qualifications and resources to fulfil their responsibilities.	ii. The following key personnel are involved in the design, development, operation, implementation, maintenance and monitoring of VMware Cloud on AWS: • **Executive Management**: Responsible for overseeing companywide activities, establishing, and accomplishing goals and overseeing objectives • **Human resources:** Responsible for HR policies, practices, and processes with a focus on the key HR delivery areas (e.g., talent acquisitions, pre-employment screening, employee retention, compensation, benefits, performance management, employee relations, and training and development) • **VMware Engineering**: Responsible for design, development, documentation, and system test plans • **VMware System Reliability Engineering (SRE) team:** Responsible for automation, upgrades and patch management, monitoring, maintenance, and troubleshooting • **VMware Information Security team**: Responsible for security operations, incident management, compliance certification, security audits, and risk analysis. • **Global Support Services:** Responsible for handling customer support issues and inquiries. VMware is committed to competence at all levels. Management considers the competence levels for particular

	jobs and translates the required skills and knowledge levels into position responsibilities.
iii. Management's philosophy and operating style • The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to the ABS controls criteria. • The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to the ABS controls criteria.	iii. The management philosophy and operating style of VMware encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitude towards information processing, accounting functions and personnel. VMware management believes that establishing a relevant organizational structure includes considering key areas of authority and that serve both external customers, as well as other business units within the company. Business units maintain their own independent organizational structure and assignment of authority and responsibility within themselves that fall within the greater VMware wide organizational structure. VMware has established business conduct guidelines which are communicated to all employees. VMware has established screening procedures, where allowed by local laws VMware performs background checks for new hires. The results are evaluated to determine employment eligibility.
iv. Organisational structure as well as assignment of authority and responsibility • Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting the ABS controls criteria have the qualifications and resources to fulfil their responsibilities. • Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operation. • The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to the ABS controls criteria.	iv. The VMware organizational structure provides the framework within which its activities for achieving the entity-wide objectives are planned, executed, controlled, and monitored. VMware has organizational charts in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees via the company intranet and updated as needed. VMware also maintains documented position descriptions to define the skills, responsibilities, and knowledge levels required for specific jobs.

(b) Risk Assessment

ABS Controls Criteria	VMware Response
The OSP's risk assessment process may affect the services provided to FIs. The following is a list of risk assessment factors and examples of how they might relate to the OSP:	
i. Changes in the operating environment - Prior to introducing changes to the operating environment (including technology components), OSP should assess the materiality of the changes to the FI's outsourced arrangement using a change management framework and should notify and/or seek approval from FIs. This is applicable to sub-contractors used by the OSP. ii. New personnel - New personnel without adequate training and / or background screening may increase the risk that controls may not be performed effectively	VMware has considered significant interactions between itself and relevant external parties and risks that could affect the company's ability to provide reliable service to its user entities. Key members of management and operational teams meet on an annual basis to perform the mandatory risk assessment. Risks identified during the risk assessment process are ranked and formally documented along with mitigation strategies. A

iii. New or revamped information systems – The OSP may incorporate new functions into its systems or implement new systems that could affect the FIs' outsourced arrangements iv. Rapid growth - If the OSP gain a substantial number of new customers, the operating effectiveness of certain controls could be affected v. New technology – If the OSP implements a new technology, its risks and impact to the FIs should be assessed vi. New business models, products, or activities - The diversion of resources to new activities from existing activities could affect the operating effectiveness of certain controls at the OSP vii. Corporate restructurings - A change in ownership or internal reorganisation could affect reporting responsibilities or the resources available for services to the FIs viii. Expanded foreign operations – The OSP that use personnel in foreign locations may have difficulties responding to changes in the FI's requirements ix. Environmental scan – The OSP should scan for emerging threats that may impact its operations or services (e.g. cyber threats, geographic risks, etc.).	formal process is documented to guide personnel when performing a risk assessment. VMware maintains an ISMS framework to manage information security risks. VMware performs annual risk assessments as part of the VMware ISMS program to support security and compliance programs. 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.

(c) Information and Communication

ABS Control Criteria	VMware Response
Adequate information and effective communication are essential to the proper functioning of internal control. The OSP's information and communication component of internal control include the following:	
i. The information system must be documented with procedures for initiating, authorising, recording, processing, and reporting FIs' transactions for proper accountability	i. VMware has documented policies, standards and system and network diagrams supporting VMware Cloud on AWS. VMware documents, updates, and maintains baseline configurations for all 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.
ii. Communication involves how the OSP communicates its roles and responsibilities, significant matters relating to the services provided to the FIs, including communication within its organisation, with the FIs and regulatory authorities. This may include the OSP's communication to its staff on how its activities impact the FIs, escalation procedures for reporting exceptions within the OSP and to the FIs, and seeking FIs' approval prior to any sub-contracting	ii. VMware has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for employees, and the use of email messages to communicate time sensitive information. VMware utilizes various internal tools for communication of VMware policies. These policies are maintained by the Chief Security Officer, reviewed, and updated on an annual basis. VMware has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include service level agreements on the VMware website, external memorandums, and regular meetings with representatives from customers and the use of email messages and other customer contact lines for time sensitive messages.

(d) Monitoring

ABS Control Criteria	VMware Response
Many aspects of monitoring may be relevant to the services provided to FIs. For example, the OSP may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, either by ongoing activities, periodic evaluations, or combinations of the two. OSPs should have processes in place to bring significant issues and concerns identified through such evaluation to the OSPs' senior management and additionally, if impacting the services provided, e.g. adverse developments, to the FIs. The OSP's monitoring of its sub-contractors' activities that affect the services provided to the FIs is another example of monitoring. This form of monitoring may be accomplished through visiting the sub-contractors' organization, obtaining and reading a report containing detailed description of the sub-contractors' controls, or conducting an independent assessment of whether the controls are placed are suitably designed and operating effectively throughout the specified period. Copies of any such reports and findings made on the OSP and/or its sub-contractors, in relation to the outsourcing arrangement, must be provided to the FIs. Results should be discussed as part of ongoing service discussions. Monitoring external communications, such as customer complaints and communications from regulators, would be important and results of such monitoring should be provided to FIs. Often, these monitoring activities are included as control activities for achieving a specific control objective.	Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. In carrying out its regular management activities, operations management obtains evidence that the company's internal controls continue to function, including error and performance reports. Communications from external parties and customers corroborate internally generated information or indicate problems. Organizational structure and supervisory activities provide oversight of internal control functions and identification of deficiencies. Operations management monitors delegated access to systems providing approval and temporary access to critical systems for system administration functions. Results of backup jobs are monitored by VMware personnel to help ensure that backup jobs are completed successfully. VMware utilizes network monitoring applications to analyze network device logs and report possible or actual network security breaches and monitor the central logging. VMware performs vulnerability assessment on a quarterly basis and performs a penetration test annually to identify and monitor systems for potential security vulnerabilities. Information security personnel perform monitoring of authentication and authorization systems, system audit log collection and analysis, security event management and security incident investigations 24 hours per day, 365 days a year.

(e) Information Security Policies

ABS Control Criteria	VMware Response
Information Security (IS) policies and procedures are established, documented and reviewed at least every 12 months or as and when there are changes. IS policies and procedures should state the person(s) responsible for information security management. These documents are reviewed and approved by management. Specific security controls for systems and networks are defined to protect the confidentiality, integrity and availability of systems and data. Any identified deviations are documented, tracked and remediated. Deviations which impact the services rendered should be communicated to the FIs immediately.	VMware has an established information security framework and policies which have integrated with the ISO 27001 framework. The policies are published on intranet and name of the person responsible for policy is shown. Policies are reviewed every 12 months. In alignment with the ISO 27001 standard, all 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. Compliance audits are periodically performed to validate that employees understand and follow the established policies.

An information security awareness training programme should be established. The training programme should be conducted for OSP's staff, subcontractors and vendors who have access to IT resources and systems regularly to refresh their knowledge.	Upon hire, personnel are required to read and accept the Acceptable Use Policy and the VMware Business Conduct Guidelines.

(f) Human Resource Policies and Procedures

ABS Control Criteria	VMware Response
The OSP should establish standards for workplace conduct, implement candidate background screening procedures, and conduct enforcement procedures to enable it to meet its commitments and requirements as they relate to the ABS controls objectives and MAS Guidelines on Outsourcing. OSP's staff (including sub-contractor staff) involved in delivering the outsourced services to FIs should understand their responsibilities and be suitable for the roles for which they are employed. The OSP should ensure that individuals considered for employment are adequately screened for experience, professional capabilities, honesty and integrity. Screening should include background checks to assess character, integrity and track record. The following are non-exhaustive examples of OSP staff screening requirements: i. Subject of any past or current proceedings of a disciplinary or criminal nature; ii. Convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty); iii. Accepted civil liability for fraud or misrepresentation; and iv. Are financially sound. The listed examples are non-exhaustive and do not necessarily preclude an individual from taking on a particular role within an OSP organization as screening procedures should be commensurate with the role that the employees are performing. Contracts with OSP's staff (including sub-contractor staff) should specify their responsibilities for maintaining confidentiality of customer information in accordance with s47 of the Banking Act (Chapter 19) on Banking Secrecy.	VMware has established screening procedures, where allowed by local laws VMware performs background checks for new hires. The results are evaluated to determine employment eligibility. New hires are required to attend orientation meetings to review corporate security policies and obligations. The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. AWS also conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees. As part of the on-boarding process, all personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. Additionally, AWS maintains employee training programs to promote awareness of AWS information security requirements, including periodic Information Security training and compliance audits to validate that employees understand and follow the established policies. VMware has documented terms and conditions for maintaining confidentiality as part of the VMware Cloud on AWS Terms of Service.

(g) Practices related to Sub-Contracting

ABS Control Criteria	VMware Response
FIs expect sub-contractors of OSPs to be managed with the same rigour as the OSPs themselves. Thus, OSP should require and ensure that their sub-contractors adhere to the requirements of these Guidelines. OSPs in managing sub-contractors should: i. Obtain approvals from the FIs before engaging sub-contractors ii. Be able to demonstrate due diligence and risk assessment of the sub-contractors iii. Implement processes to inform and consult the FIs on material changes to the sub-contractors' operating environment iv. Conduct a review of its sub-contractors every 12 months	VMware has a Third-party Risk Management Policy. This policy applies to VMware's management and oversight of all 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 all third parties to ensure the security of information assets.

v. Monitor the performance and risk management practices of the sub-contractors Due diligence and risk assessments of sub-contractors should involve evaluation of relevant information as specified in section 5.4.3 of the MAS Guidelines on Outsourcing, e.g. experience and capability of the sub-contractor to implement and support the outsourcing arrangement over the contracted period and financial strength and resources of the sub-contractors. Sub-contracting within the OSP's group should be subjected to similar due diligence. OSPs should take note of the requirements of section 5.10 of the MAS Guidelines on Outsourcing when outsourcing to a sub-contractor that is operating outside Singapore.	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, review, and audit 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 address 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.

General Information Technology (IT) Controls Criteria

(a) Logical Security

These controls provide reasonable assurance that logical access to programmes, data, and operating system software is restricted to authorised personnel on a need-to-have basis.

ABS Control Criteria	VMware Response
Logical access to programs, data, and operating system software is restricted to authorized personnel on a need-to-have basis.	
i. Logical access requirements to IT systems, i.e. programmes, data and operating system software are defined, as agreed with FIs. Logical access requirements include the following, where applicable: (a) Definition of the "least privilege" required by each user group, including privileged users, to: • Production and backup data • Sensitive information, including FI's customer information • Commands, services, e.g. application, web and network services, and sensitive files, e.g. system logs and audit trails • Non-production systems, e.g. UAT and DR environments (b) Password management rules and parameters (e.g. password complexity, lockout settings, password history) in line with the FI's password management requirements; and (c) Procedures to manage privileged / system administration accounts (including emergency usage).	i. 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 is based on an individual's "need to know" as determined by job functions and requirements. Access privileges to computers and information systems is authorized by the appropriate level of management and documented within the ticket lifecycle, and such access is monitored (in use) and revoked when no longer required. 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. Information system documentation is made available to authorized personnel to ensure configuration, installation, and operation of the information system.
ii. Access to IT systems software is only granted based on a documented and approved request, and on a need-to-use basis.	ii. The VMware access control policy addresses requirements for the end-to-end access management lifecycle including access provisioning, authentication, access authorization, removal of access rights, and periodic access reviews. Access is based on an individual's "need to know" as determined by job functions and requirements.

	Access privileges to computers and information systems is authorized by the appropriate level of management and documented within the ticket lifecycle, and such access is monitored (in use) and revoked when no longer required. 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 certificates and 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 all access is logged & monitored and any suspicious activity is investigated by VMware's Security Operations Center (SOC).
iii. All users' access to IT systems, including sub-contractors' access, are reviewed periodically in accordance with a frequency agreed with the FIs.	iii. 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. All entitlement actions are recorded via the systems used to grant/revoke access and provide evidence to support compliance programs. All remediation actions related to access violations will follow user access policies and standard procedures.
iv. Access to IT systems are revoked or disabled promptly in accordance with the SLA when the access is no longer required.	iv. 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. Customers are responsible for managing end-user access to their Software Defined Data Center deployed in VMware Cloud on AWS.
v. Strong physical or logical controls are used to identify, segregate and protect individual FI's information. Such controls survive the tenure of the contract.	v. VMware Cloud on AWS has three 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. Each SDDC is deployed on dedicated bare metal hardware - providing physical isolation between customers' environments. Dedicated hardware means that customers do not share the physical processor, memory, or storage with anyone else. VMware vSphere is deployed in each SDDC which allows customers to logically isolate their content by creating Resource Pools and configuring vSphere permissions to control who has access to content within their own organization. VMware NSX Datacenter is deployed in each SDDC which allows customers to additionally isolate their content by creating network configurations including firewalls, VPNs, and network segments to provide fine grained access control.

vi. Procedures are established to securely destroy or remove the FI's data as per the agreed retention and destruction policies as well as upon termination. This requirement also applies to backup data.	vi. VMware does not back-up or archive customer content. When a host is deleted from the customer SDDC, VMC cannot recover customer data and the process is irreversible. 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. https://aws.amazon.com/compliance/data-center/controls/
vii. Industry-accepted cryptography standards agreed with FIs are deployed to protect FIs' customer information and other sensitive data in accordance with the MAS Technology Risk Management (TRM) guidelines: (a) Stored in all type of end-point devices, e.g. notebooks, personal computers, portable storage devices and mobile devices. (b) Transmitted between terminals and hosts, through networks and between sites, e.g. primary and recovery sites. (c) Stored in computer storage, including servers, databases, backup media and storage platforms, e.g. storage area network ("SAN"). (d) Electronically transmitted to external parties (where permissible). When transmitted electronically to external parties, e.g. via email, the decryption key are communicated to the intended recipient via a separate channel, e.g. via telephone call.	vii. 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 in-guest encryption solutions. Customers that require VM level encryption are responsible for deploying and maintaining such solutions as 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 option of managing the encryption keys for vSAN encryption to provide an additional level of security. d. Connectivity to all management interfaces provided in VMware Cloud on AWS is performed via encrypted channels using TLS security.
viii. Password management controls for applications/systems are periodically reviewed with FIs according to the agreed information security requirements/standards.	viii. 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 SOC2 report.
ix. Users with elevated access privileges are subjected to strict controls such as: (a) Split-password control, never-alone principle, two-factor authentication (2FA), etc. (b) Passwords are changed regularly and access is removed when no longer required. (c) Timely review of privileged users' activities.	A "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 certificates and 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 all

	access is logged & monitored and any suspicious activity is investigated by VMware's Security Operations Center (SOC). Although VMware employs 2-Factor authentication as a method to protect VMware Development and Operations and Support teams' access to the internal platforms, it is an internal only service. 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.

(b) Physical Security

These controls provide reasonable assurance that Data Centre (DC)/ Controlled Areas are resilient and physically secured from internal and external threats.

ABS Control Criteria	VMware Response
Data Centre/Controlled Areas are physically secured from internal and external threats.	
i. Access to data centre/controlled areas is restricted: (a) Access is physically restricted (e.g. via card access, biometric systems, ISO standard locks) to authorised personnel on a need-to-have basis only. Access mechanism may include 'anti-passback' feature to prevent use of card access for multiple entries and mantraps to prevent tailgating (b) Requests for access to DCs by employees, contractors and third parties must be approved and documented. (c) All visitors must be registered. Visitors are issued with clear identification (e.g. an ID badge) and escorted by authorised personnel at all times. ii. All access points, including windows, to controlled areas are fitted with audible intruder alarms that are monitored by security personnel. Doors are fitted with door-ajar alarms. The alarm system is tested regularly and the test documentation is retained. iii. Entries and exits to secure areas have an audit trail (i.e. entry/exit log from door access system, CCTV footage, manual log-book with visitor's name, date, time, purpose, escort's name, etc.). iv. Access rights to data centre/controlled areas are reviewed at a frequency agreed with FIs. Access violations are monitored, followed up and reported to FIs in accordance with the SLA. v. Physical access credentials are revoked or disabled promptly when not required. Inventory of security access cards is managed and damaged or lost cards are invalidated or revoked in the access control system promptly. vi. An appropriate risk assessment, such as a Threat and Vulnerability Risk Assessment ("TVRA") is performed	VMware Cloud on AWS uses AWS datacenters. AWS security management standards follow the best practices and comprehensive security controls of ISO/IEC 27001:2013. AWS manages physical access to datacenters 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* VMware also has an established Third Party IT Risk Management policy. The policy applies to VMware's management and oversight of all 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 all third parties to ensure the security of information assets.

for the data centre, server room and any other controlled areas housing FIs' customer or sensitive information (e.g. hardcopy FIs' customer information, FIs' procedural documents, contractual documentation, etc.). If an OSP shares premises with other organisations, a risk-based TVRA or similar appropriate risk assessment is performed to assess the relevant control areas, e.g. data centre, server room and/or any other relevant physical premises. The scope of the assessment is agreed with the FIs and include, at a minimum, the physical perimeter and surrounding environment of the premises. The assessment includes various threat scenarios such as theft, explosives, arson and internal sabotage. Gaps identified by the risk assessment are remediated timely. *Note: Before FIs procure DC services from the OSP, FIs will ensure that all identified risks are adequately addressed. Subsequent assessments may also be conducted at a frequency that commensurate with the level and type of risk to which a DC is exposed as well as the criticality of the DC to the FIs. FIs will obtain and assess the TVRA report from the OSP on the DC facility.*	
1. Data Centre/Controlled areas are resilient to protect IT assets	
i. The following environmental control features are installed at the data centre: (a) Locked cabinets for systems and network equipment (b) Uninterruptible power supply and backup generators (c) Air conditioning and humidity control systems (d) Temperature and humidity sensor (e) Fire and smoke detection systems (f) Water sprinkler system (dry-piped) (g) FM200 or other fire suppression system (h) Raised floor (i) CCTV cameras (j) Water leakage detection system (k) Hand-held fire extinguisher	i. 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. Highly resilient systems, and therefore service availability is a function of the system design. Through the use of Availability Zones and data replication, AWS 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.

ii. Environmental control equipment are inspected, tested and maintained regularly.	ii. 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/

(c) Change Management

These controls provide reasonable assurance that changes to applications, system software, and network components are assessed, approved, tested, implemented, and reviewed in a controlled manner.

ABS Control Criteria	VMware Response
1. Changes to the applications, system software and network components are assessed, approved, tested, implemented, and reviewed in a controlled manner.	
i. A formal change management process is established, documented and reviewed at least every 12 months or when there are changes to the process. The change management process is reviewed and approved by management. Segregation of change management duties is also specified.	i. VMware's Security Development Lifecycle 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.
ii. The following controls exist for changes applied to the production environment: (a) Changes are initiated through a formal change request process and classified according to the priority, risk and impact of the changes. (b) Change requests are approved in accordance to an established Change Authority Matrix (includes internal and FIs' approvals), as agreed with FIs. (c) A risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems is performed. (d) All changes are tested and appropriate approvals are obtained prior to implementation. System Integration Testing ("SIT") and User Acceptance Testing ("UAT") test plans are prepared and signed off in accordance to the established Change Authority Matrix. (e) Emergency change escalation protocols (e.g. by telephone and email) and approval requirements are established in the change approval matrix (includes internal and FI approvals) as agreed with FIs. Documented approval are obtained after the emergency change. (f) A rollback plan (which may include a backup plan) is prepared and approved prior to changes being made. (g) System logging is enabled to record activities that are performed during the migration process. (h) Segregation of duties is enforced so that no single individual has the ability to develop, compile and migrate object codes into the production environment. (i) Disaster recovery environment versions are updated timely after production migration is successfully completed.	ii. Change request 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 must be approved by at least 1 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 all 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 System logging is enabled to record activities that are performed during the migration process. Administrative activities related to migration within vCenter are recorded in vCenter logs. Additional logging is can be viewed in the Site Recovery Manager (SRM) Add-on for VMware Cloud on AWS. SRM client log files contain information about the client configuration and related messages in the SRM UI.

	VMware has well established controls in place to protect and control access to all production systems and source code. All 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 all components are updated in a timely fashion.
iii. Change risk categories are used to determine approval requirements in accordance with the defined change management process. Appropriate escalation levels and approvals are established and documented in the Change Authority matrix for changes.	iii. VMware's change management process includes change risk review and analysis. Changes are categorized into various categories such as Standard, Normal and Emergency which trigger the relevant approval requirements. Depending on the nature of change, they are approved by CAB and ECAB. Change advisory board (CAB): Governing body that exists to advise the change management team on approvals and to assist the Change Manager in the assessment and prioritization of RFCs. Emergency Change advisory board (ECAB): This is a subset of CAB members who make decisions about emergency changes.
iv. Segregation of environments for development, testing, staging and production is established. UAT data are anonymised. If UAT contains production data, the environment must be subject to appropriate production level controls.	iv. VMware has well established controls in place to maintain segregation of duties and protect and control access to all production systems and source code. All 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 has policies and procedures in place to ensure that test data is not used in production environments. Development, QA, and production all use separate equipment and environments and are managed by separate teams. Customers retain control and ownership of their content. It is the responsibility of each customer to control the movement of their content between their environments and ensure that their production customer content is not replicated to any non-production environment.
v. Source code reviews are conducted for higher risk systems and applications changes to identify security vulnerabilities and deficiencies, coding errors, defects and malicious codes before these changes are implemented.	v. VMware has invested in the Security Development Lifecycle (SDLC) process which is continuously evolving in response to the threat landscape and a security organization that utilizes multiple key resources to ensure that VMware Cloud on AWS implements appropriate operational and security controls. As a part of the VMware Security Development Lifecycle, 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 cloud security teams, manual & automated code analysis and 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

(d) Incident Management

These controls provide reasonable assurance that all system and network processing issues are resolved in a timely and controlled manner.

ABS Control Criteria	VMware Response
1. System and network processing issues are resolved in a timely and controlled manner.	
i. A formal documented incident management process exists. The process is reviewed at least every 12 months, or when there are changes to the process, and updated and approved accordingly.	i. VMware has a documented security incident management policy which is reviewed every 12 months. VMware has Incident response program, plans, and procedures which are documented and implemented.
ii. Roles and responsibilities of staff involved in the incident management process are clearly documented in the procedures, including recording, analysing, remediating and monitoring of problem and incidents.	ii. 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) pertaining to all virtual machines that they have deployed in customer SDDC. Roles and responsibilities of staff involved in incident management processes at VMware are clearly documented 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 vSIRT program manager. The Director, Threat Management, shall approve the development and refinement of the incident response policy, standards, procedures, tools, and capabilities. 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 The Risk Analysis Group contains appropriate management levels from Legal, Human Resources, Finance (if applicable), IT, and any other appropriate business units. The Legal Privacy Counsel leads of the Risk Analysis Group.VMware Legal Privacy Counsel and Public Sector Legal Team work with vSIRT in the event of an incident involving PII, PHI, CDI, or PCI data.
iii. Clear escalation and resolution protocols and timelines are documented. FIs are notified of incidents and the notifications are tracked and reported to the FIs in accordance with the SLA.	iii. 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 endeavors to assist

	customers in mitigating, where possible, the adverse effects of any personal data breach.
iv. Incidents are recorded and tracked with the following information: (a) Severity (b) Client/FI information (c) Description of incident/problem (d) Date and time of incident/problem (e) Incident type (f) Application, systems and / or network component impacted (g) Escalation and approvals (h) Actions taken to resolve the incident or problem, including date and time action was taken (i) Post-mortem on incidents that includes root-cause analysis.	iv. VMware uses ticketing system to record incidents and captures specified fields in the incident tickets.
v. Problems attributing to the incidents are analysed to address root cause and to prevent recurrence. Trend analysis of past incidents is performed to facilitate the identification and prevention of similar problems.	v. VMware conducts root cause analysis and trend analysis for incidents depending on severity. Follow up actions are documented and actions are addressed with respective teams.

(e) **Backup and Disaster Recovery**

These controls provide reasonable assurance that business and information systems recovery and continuity plans are documented, approved, tested, and maintained. Backups are performed and securely stored.

ABS Control Criteria	VMware Response
Backups are performed and securely stored	
i. Backup policies and procedures are documented. The policies and procedures are reviewed and updated at least every 12 months or whenever there are changes impacting backup procedures.	i. VMware has established a backup policy that establishes the requirements for backing up VMware information, software, and systems, collectively referred to as 'Data Backup' Policy. It defines the retention and protection requirements for the organization. The policy is reviewed every 12 months. VMware Cloud on AWS backs up account Information including system configuration settings but does not provide data backup services for customer content. Customer content will not be relocated, replicated, archived, or copied without the explicit actions by the customer administrator. VMware provides each customer a secured/isolated configuration by default which can be customized via self-service tools, as required by the customer administrators, to optionally enable customer content transport outside of the dedicated customer SDDCs to any other AWS facilities, customer dedicated private networks or public internet.
ii. Backup and restoration processes are implemented such that FIs' critical information systems can be recovered. Backup procedures are formally documented based on the data backup and recovery requirements of FIs. These include a data retention policy and procedures designed to meet business, statutory and regulatory requirements as agreed with FIs.	ii. VMware has implemented policies and procedures to guide personnel in performing data backups and data restoration. Procedures document each step of the scheduling, monitoring, quality assurance (QA), and restoration processes, as well as roles and responsibilities. VMware schedules regular backups of the VMware Cloud on AWS application and backend infrastructure meta data to Amazon Simple Storage Services (S3). Customers are responsible for backing up their own data. Administrative access privileges to backup systems and data are restricted to accounts accessible by authorized VMware personnel. VMware operations personnel perform backup media

	restores on a regular basis to verify that VMC on AWS components can be recovered from system backups.
iii. System level backups are securely stored at off-site storage facilities.	iii. VMware schedules regular backups of the VMware Cloud on AWS application and backend infrastructure meta data to Amazon Simple Storage Services (S3). Customers are responsible for backing up their own data.
iv. Backup logs associated with system level backups are generated and remedial action is taken for unsuccessful backups.	iv. The backup system records the results of each backup job as well as the associated date, duration, and size of the data backup. The backup system is configured to automatically send e-mail notifications to IT operations personnel for failed backup jobs via the PagerDuty mobile application. Additionally, request tickets are generated in JIRA to help ensure that issues are resolved, and backups are completed.
v. Data backed up to external media such as tapes are encrypted using industry-standard cryptography.	v. The automated backup systems used by VMware are configured to encrypt backup data. As mentioned above customers are responsible for backing up their content. Customers can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration.
vi. Tape (or other media) tracking/management system is used to manage the physical location of backup tapes. This includes a full inventory of all tapes on and off site, tapes retention periods and tapes due for rotation.	vi. VMware schedules regular backups of the VMware Cloud on AWS application and backend infrastructure meta data to Amazon Simple Storage Services (S3). Customers are responsible for backing up their own data.
vii. Tape (or other media) inventory checks are performed at least every 12 months such that all tapes are accounted for	vii. VMware does not backup customer content. VMware schedules regular backups of the VMware Cloud on AWS application and backend infrastructure meta data to Amazon Simple Storage Services (S3). Backups stored in S3 buckets are periodically checked and verified by VMware SRE engineers.
viii. Backup tapes (or other media) are periodically tested to validate recovery capabilities.	viii. VMware does not backup customer content. VMware schedules regular backups of the VMware Cloud on AWS application and backend infrastructure meta data to Amazon Simple Storage Services (S3). Backups stored in S3 buckets are periodically tested and verified by VMware SRE engineers.
Business and information systems recovery and continuity plans are documented, approved, tested, and maintained.	
Disaster Recovery ("DR") refers to disaster recovery capabilities as a whole for services rendered and not specific to information technology ("IT") disaster recovery only. i. A DR strategy and business continuity plan is established and maintained based on business, operational and information technology needs of FI. Operational considerations include geographical requirements, on-site and off-site redundancy requirements. (a) Different scenarios such as major system outages, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary processing centre are considered in a DR plan (b) DR facilities shall accommodate the capacity for recovery as agreed with FIs (c) OSP should notify the FIs of any substantial changes in the OSPs' BCP plans and of any	i. 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 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 manmade threats based upon a geographically

adverse development that could substantially impact the services provided to the FIs.	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 all 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 have an optional (paid) disaster recovery feature called VMware Site Recovery that greatly simplifies disaster recovery management and operations.
ii. DR strategy and business continuity plan, including activation and escalation process is reviewed, updated and tested at least every 12 months. In consultation with FIs this may be conducted more frequently depending on the changing technology conditions and operational requirements. FIs should also be permitted to participate in DR and BCP tests as appropriate.	ii. VMware has a defined Information Security Program that includes Business Continuity (BC) and Disaster Recovery (DR) strategies and includes regular testing exercises every 12 months.
iii. DR exercise (i.e. testing plans and results) should be documented with action plans to resolve and retest exceptions. The results of BCP and DR exercises should be communicated to the FIs.	iii. VMware has a defined Information Security Program that includes Business Continuity (BC) and Disaster Recovery (DR) strategies for business operations data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises for the hosting VMware operations platform. Audits are performed annually under the VMware information security management system (ISMS) program.
iv. Recovery plans include established procedures to meet recovery time objectives (RTO) and recovery point objectives (RPO) of systems and data. Applied definitions and actual objectives related to RTO and RPO are reviewed on a periodic basis by appropriate OSP management to ensure alignment with FIs' expectations and applicable MAS regulation (e.g. MAS Outsourcing, Business Continuity Management ("BCM") and MAS TRM). Defined RTO, RPO and resumption operating capacities should be validated by management during the annual test of the DR strategy and BCP.	iv. 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.
v. Redundancy plan for single points of failure which can bring down the entire network are developed and implemented.	v. 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 cloud service platform architecture to ensure high availability of the VMware Cloud on AWS service, including regional independence and separation of console availability and SDDC services availability.

	VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as in 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. VMware Cloud on AWS customers can utilize and optional VMware Site Recovery (VSR) service that 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.

(f) Network and Security Management

These controls provide reasonable assurance that the systems and network controls are implemented based on FIs' business needs.

ABS Control Criteria	VMware Response
1. **Systems and network controls are implemented based on clients' business needs.**	
i. Specific security controls for systems and networks are defined to protect the confidentiality, integrity and availability of systems and data. These controls are documented, reviewed and updated at least every 12 months. Security baseline standards (i.e. system security baseline settings and configuration rules) are defined for the various middleware, operating system, databases and network devices to ensure consistent application of security configurations and harden systems to the required level of protection. Regular enforcement checks against baseline standards should be carried out to monitor compliance.	i. As the industry-leading virtualization software company, VMware maintains best-in-class security standards through all facets of our products and cloud services, which also align with the major compliance certifications. This includes well-established programs and practices to identify and remediate security vulnerabilities in our products and to mitigate software security risks to customers. The VMware Platform & Application Security standards are consistent with industry-accepted guidance and standards, such as, but not limited to, NIST, ISO, and CIS. 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. Internal and external audits are performed at annually under the VMware information security management system (ISMS) program. VMware utilizes internal/external audits as a way 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 VMware follows a strict policy of security baseline configuration that includes pre-implementation approvals and alignment with standards set by USGCB, FDCC, DISA, STIGs, and CIS Benchmarks. All security baseline configuration changes are reviewed for approval in a timely manner. The Vulnerability Management team also maintains a central repository of security baseline configurations to satisfy legal/regulatory requirements.
ii. Procedures are implemented to ensure that anti-virus/anti-malware software are installed and updated regularly. Detected threats are quarantined and removed appropriately.	ii. To ensure the security of the VMC on AWS, antivirus software is installed on internal VMware Mac/Windows workstations that support the VMC on AWS system and configured to scan and monitor for updates to virus definitions and update workstations. The antivirus software is also configured to perform on-access scans for any new files installed on monitored workstations. New customer environments are configured to deny all network connections by default unless specifically configured by customers.

	Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry- accepted timeframes.
iii. Patch management procedures are established and include maintaining an up-to-date inventory of hardware and software platforms used (including open source platforms) to facilitate patching and vulnerability monitoring, timely monitoring, reviewing, testing and application of vendor provided patches, and prioritising security patches to address known vulnerabilities. The timeframe for implementing patches on critical system and security vulnerability is agreed with the FIs.	iii. 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 all 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.
iv. Deviations from security policies/standards are documented and mitigating controls are implemented to reduce the risks. Deviations are tracked and remediated appropriately. Outstanding deviations are reviewed at least every 12 months. Deviations which impact the services rendered to the FIs should be reported to the FIs.	iv. VMware's policy exception process evaluates business justification for the non-compliance against the risk. All exception requests must be sponsored by an executive manager. A policy exception is not in place until fully approved. All requests for policy exception are reviewed and dispositioned by the Policy Working Group (PWG). In addition to a resolution date to resolve the non-compliance, the PWG requires appropriate compensating controls are established to mitigate the risk where possible. Exception requests are risk rated and may be approved for a term not longer than 1 year. Exception requests considered *critical* risk, or, as deemed appropriate for executive attention by the PWG, are further escalated to the Policy Executive Committee for approval. A periodic report of open, approved security exceptions is distributed to key stakeholders including both PEC and PWG members, and tracks remediation progress of the non-compliance.
v. File integrity checks are in place to detect unauthorised changes (e.g. databases, files, programmes and system configuration).	v. Operations management security, logging, monitoring and intrusion detection higher levels of assurance are required for the protection, retention, and lifecycle management of 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 behaviors and/or file integrity anomalies; and support forensic investigative capabilities in the event of a security breach. The service continuously collects and monitors the environment logs, which are correlated with both public and private threat feeds to spot suspicious and unusual activities
vi. Network security controls are deployed to protect the internal network. These include firewalls and intrusion detection-prevention devices (including denial-of-service security appliances where appropriate) between internal and external networks as well as between geographically separate sites, if applicable. Network surveillance and security monitoring procedures (e.g. network scanners, intrusion detectors and security alerts) are also established.	vi. 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 all network traffic and defend the console by detecting and preventing web-based attacks.
vii. Rules for network security devices are backed up and reviewed regularly for appropriateness and relevance.	vii. VMware delivers each SDDC with a secure by default (deny-all) configuration. VMware provides each customer a secured/isolated configuration by default which can be customized via self-service tools, as required by the customer's administrators. Customers manage VMware NSX Edge Firewall Rules to allow/block access to the vCenter appliances & other workload VMs in their SDDCs, connect to direct connect networks, and create Virtual Private Networks (VPN) to encrypt traffic between customer networks and the VMC SDDC networks. Each customer must configure & monitor all of the networks they create that connect to their VMs, OS, and applications for malicious threats with tools and operational processes to respond to security risks. Each SDDC is protected by a pair of customer managed VMware NSX firewalls that secure north-south traffic. Additionally, customer managed NSX distributed firewalls may be provisioned to provide east-west traffic security and network segmentation inside the SDDC. VMware Cloud on AWS SDDCs enable customers to manage Firewall Rules to allow/block access to the vCenter appliances & other workload VMs in their SDDCs, connect to Direct Connect circuits, and create Virtual Private Networks (VPN) to encrypt traffic between customer networks and the VMC SDDC networks.
viii. Security system events are logged, retained and monitored	viii. 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. Furthermore, intrusion detection devices such as honeypots are used. 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. They are tested annually by the ISMS and are monitored and reviewed for security events by the VMware Security Operations Center 24 hours a day, 7 days a week. 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 all 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.

Security Incident Response

These controls provide reasonable assurance that appropriate personnel within the OSP are contacted and immediate action is taken in response to a security incident. Requirements in the relevant notices such as the MAS TRM Notice are adhered to.

ABS Control Criteria	VMware Response
1. **Appropriate personnel are contacted and immediate action taken in response to a security incident.**	
i. An Incident Response Plan that establishes and documents specific procedures that govern responses to security incidents (physical or system security) is documented. The roles and responsibilities of staff involved in responding to security incidents are clearly defined.	i. 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) pertaining to all virtual machines that they have deployed in customer SDDC. Roles and responsibilities of staff involved in incident management processes at VMware are clearly documented 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 vSIRT program manager. The Director, Threat Management, shall approve the development and refinement of the incident response policy, standards, procedures, tools, and capabilities 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 The Risk Analysis Group contains appropriate management levels from Legal, Human Resources, Finance (if applicable), IT, and any other appropriate business units. The Legal Privacy Counsel leads of the Risk Analysis Group.VMware Legal Privacy Counsel and Public Sector Legal Team work with vSIRT in the event of an incident involving PII, PHI, CDI, or PCI data.
ii. Security response procedures are reviewed and tested every 12 months and the Incident Response Plan updated where necessary.	ii. Security response procedures are tested annually. Issues identified are documented and follow up actions are created and addressed.
iii. When an incident is detected or reported, the defined incident management process is initiated by authorised personnel. The incident severity level and escalation process are pre-agreed with FIs. FIs should be notified immediately upon discovery and an Incident Report should be provided post-event.	iii. The vSIRT team is notified by the Security Operations Center of any potential incident 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 endeavors to assist customers in mitigating, where possible, the adverse effects of any personal data breach.

(g) System Vulnerability Assessments

These controls provide reasonable assurance that vulnerability assessments and penetration testing are conducted regularly to detect and remediate security vulnerabilities in the IT environment.

ABS Control Criteria	VMware Response
1. Vulnerability Assessments	
i. Vulnerability assessment ("VA") policies and procedures are documented and reviewed at least every 12 months or whenever there are changes.	i. 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.
ii. The OSP continually monitors emergent security exploits, and perform regular VAs of its IT environment against common and emergent internal and external security threats. The frequency of the Vas is agreed with FIs based on the FIs' risk assessments.	ii. VMware assesses vulnerabilities across VMware Cloud on AWS platform information systems and applications on a quarterly 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.
2. Penetration Testing	
i. Penetration testing ("PT") policies and procedures are documented and reviewed at least every 12 months or whenever there are changes.	i. VMware has an established vulnerability management policy and vulnerability management standard that includes the requirement to cover regular penetration tests. The policy and standard are reviewed on an annual basis.

ii. PTs are performed to simulate attacks of the IT systems. PTs of Internet facing systems are performed at least every 12 months.	ii. 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 grey box testing. A grey box approach is a mixture of black box and white box testing. White box testing means that all 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 grey 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 Red Team Information Security staff as well as third party security auditors to periodically perform comprehensive penetration testing of systems and applications. Penetration testing occurs at least annually to support VMware compliance programs.
3. Timely Remediation	
i. Issues identified via the VAs and PTs are remediated promptly and revalidated to ensure that the identified gaps are fully resolved.	i. VMware patches or upgrades all platform systems and applications after analysing 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. 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.
ii. Procedures for fixing issues identified by VAs and PTs are documented and reviewed at least every 12 months or whenever there are changes.	ii. The vulnerability management policy and standards are reviewed every 12 months.

(h) Technology Refreshment Management

These controls provide reasonable assurance that software and hardware components used in the production and disaster recovery environment are refreshed timely.

ABS Control Criteria	VMware Response
1. Production and disaster recovery systems and software are replaced timely.	
i. Technology Refresh Management plan and procedures are documented and reviewed at least every 12 months or whenever there are changes.	i. VMware has an established System Acquisition, Development & Maintenance Policy and Change Management policy that describes the procedures for changes across VMware software and infrastructure. The policies are reviewed every 12 months.
ii. An up-to-date inventory of software and hardware components used in the production and disaster recovery environments supporting FIs is maintained to	ii. VMware has an established Asset Management policy that dictates management of assets at VMware including creation, processing, storage, transmission, deletion, and destruction.

facilitate the tracking of IT resources. The inventory includes all relevant associated warranty and other supporting contracts related to the software and hardware components.	VMware maintains inventories of critical assets including asset ownership and location.
iii. The OSP actively manages its IT systems and software supporting FIs so that outdated and unsupported systems which significantly increase its exposure to security risks are replaced timely. Close attention is paid to the products' end-of-support ("EOS") dates.	iii. Automated processes are in place that handle media sanitization before repurposing of any hardware. Upon the explicit deletion of a production environment by a tenant, a cryptographic wipe of the hard drives is performed via destruction of keys used by the self-encrypting drives. For more detail, 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 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.
iv. The OSP should inform FIs on identification of any systems to be decommissioned or replaced.	iv. 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.
v. When decommissioning IT systems, the OSP should ensure that the FI's information is securely destroyed / purged from the system to prevent data leakage. Evidence of the secure destruction / purge should be provided to the FI.	v. Refer to response at (iii) above.
vi. A risk assessment of systems approaching EOS is conducted to assess the risks of continued usage and establish effective risk mitigation controls where necessary.	vi. VMware Cloud on AWS utilizes AWS data centers. Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their lifecycles. 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.

Service Controls

(a) Setting-up of New Clients/Processes

These controls provide reasonable assurance that client contracting procedures are defined and monitored, and client processes are set up and administered in accordance with client agreements/instructions.

ABS Control Criteria	VMware Response
1. **OSP contracting procedures are defined and monitored.**	
i. In considering, amending, renegotiating or renewing an outsourcing arrangement, the OSP provides accurate and timely information to FIs so that they can perform an appropriate due diligence to assess the risks associated	ii. VMware has made SLAs, Terms of Service, Data Processing Addendums, Privacy notices publicly available. They can be found here:

with the outsourcing arrangements. Information provided includes: (a) Experience and capability to implement and support the outsourcing arrangements over the contracted period (b) Financial strength and resources (c) Corporate governance, business reputation and culture, compliance, and pending or potential litigation (d) Security and internal controls, audit coverage, reporting and monitoring environment (e) Risk management framework and capabilities, including in technology risk management and business continuity management in respect of the outsourcing arrangements (f) Disaster recovery arrangements and disaster recovery track records (g) Reliance on and success in dealing with sub-contractors (h) Insurance coverage (i) External factors (such as the political, economic, social and legal environment of the jurisdiction in which the OSP operates, and other events) that may impact service performance Ability to comply with applicable laws and regulations and track records in relation to its compliance with applicable laws and regulations	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.
ii. Contractual terms and conditions governing relationships, functions, obligations (including minimal insurance coverage of assets), responsibilities, rights and expectations of all contracting parties are set out fully in written agreements, e.g. Outsourcing Agreement with Service Level Agreements ("SLA").	ii. Refer to response at (i) above. Contractual terms and conditions governing relationships, functions, obligations, and rights are set out in the Terms of Service, Service Level Agreement and Data Processing Agreement.
ii. The outsourcing agreements between the OSP and FIs have provisions to address the following: (a) The scope of the outsourcing arrangements (b) The performance, operational, internal control and risk management standards (c) Confidentiality and security (i.e. roles and responsibilities, liability for losses in the event of breach of security/confidentiality and access to and disclosure of), including a written undertaking to protect, isolate and maintain the confidentiality of FIs information and other sensitive data (d) Business resumption and contingency requirements. The OSP is required to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures (e) Processes and procedures to monitor performance, operational, internal control and risk management standards. (f) Notification of adverse developments or breaches of legal and regulatory requirements. The outsourcing agreement should specify the type of events and the circumstances under which the OSPs should report such events to the FIs. (g) Dispute resolution (i.e. protocol for resolving disputes and continuation of contracted service during disputes as well as the jurisdiction and rules under which disputes are to be settled). The	iii. Refer to response at (i) above. The Terms of Service, Service Level Agreement and Data Processing Agreement cover the provisions for scope of outsourcing arrangement, risk management, shared responsibility, confidentiality and security, business continuity and disaster recovery, audits, data processing arrangements, breach management, termination, sub-processors and compliance with applicable laws and regulations.

outsourcing agreement should specify the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties. (h) Default termination and early exit by all parties. *Note: FIs have right to terminate the outsourcing arrangement in the event of default, ownership change, insolvency, breach of security or confidentiality, or serious deterioration of service quality* (i) Sub-contracting (i.e. restrictions on sub-contracting, and clauses governing confidentiality of data) (j) FIs' contractual rights to remove or destroy data stored at the OSP's systems and backups in the event of contract termination (k) Ownership and access (i.e. ownership of assets generated, purchased or acquired during the outsourcing arrangements and access to those assets) (l) Provisions that allow the FIs to conduct audits on the OSP and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the FIs; and to obtain copies of any report and findings made on the OSP and its sub-contractors, in relation to the outsourcing arrangements and to allow such copies of any report or finding to be submitted to the Monetary Authority of Singapore ("MAS") (m) Provisions that allow the MAS, or any agent appointed by the MAS, where necessary or expedient, to exercise the contractual rights of the FIs to access and inspect the OSP and its sub-contractors, to obtain records and documents of transactions, and information given to the OSP, stored at or processed by the OSP and its sub-contractors, and the right to access and obtain any report and finding made on the OSP and its sub-contractors (n) Provisions for the OSP to comply with FIs' security policies, procedures and controls to protect the confidentiality and security of the FIs' sensitive or confidential information, such as customer data, computer files, records, object programs and source codes (o) Provisions for the OSP to implement of security policies, procedures and controls that are at least as stringent as the FIs' (p) Provisions to ensure that audit is completed for any new application/system before implementation that will address FIs' information asset protection interests. The audit should at least cover areas like system development and implementation life cycle, the relevant documentation supporting each cycle phase, business user (including client where applicable) involvement and sign-off obtained on testing and penetration test outcomes for application/ system and compliance with pre-agreed security policies with FIs. (q) Provisions for sub-contracting of material outsourcing arrangements to be subjected to prior approval of the FIs (r) Applicable laws, i.e. choice-of-law provisions, agreement covenants and jurisdictional covenants	

that provide for adjudication of disputes under the laws of a specific jurisdiction.	
iv. In sub-contracting arrangements where the sub-contractors are providing services to support the OSP's outsourcing arrangement with the FI, the contractual terms in the sub-contracting arrangements should align with the OSP's contract with FIs.	iv. VMware has contractual arrangements with its subcontractors. Third Party IT Risk Management Policy applies to VMware's management and oversight of all 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 all third parties to ensure the security of information assets. Identification of risks related to external parties and access controls is performed as part of our Risk Management program and verified as part of our ISO 27001 audit. VMware vendors/suppliers do not have access to customer data.
2. OSP's processes are set up and administered in accordance with FIs agreements/instructions.	
i. Implemented process control activities are agreed with the FIs. The types of these controls are appropriate for the nature and materiality of the outsourcing arrangements.	i. The 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 ISO 27001, ISO 27017, ISO 27018, SOC2 and HIPAA.
i. Operating procedures are documented, reviewed and updated at least every 12 months and made available to appropriate personnel.	ii. VMware has a formal service level agreement that is made available to all customers. SLA is made available on VMware Cloud's website at *https://www.vmware.com/download/eula.html* VMware also provides various documents such as reference architecture and technical documentation to allow customers to understand and run the service. These can be found at *https://cloud.vmware.com/vmc-aws/resources#all-categories* VMware has also documented various technical documentation supporting VMC on AWS. You can find the most up-to-date technical documentation on the VMware website at: *https://docs.vmware.com/* Additionally, VMware also maintains various internal documentation/run books supporting key processes such as BC/DR, Incident Management, Security and Change Management. VMware's policies, standards, SLA, and Terms of Service are reviewed annually.

(b) Authorising and Processing Transactions

These controls provide reasonable assurance that services of the OSP are authorised, recorded and subjected to internal checks to ensure completeness, accuracy and validity on a timely basis. Services are processed in stages by independent parties such that there is segregation of duties from inception to completion.

.

ABS Control Criteria	VMware Response
i. Services and related processes are authorised and recorded completely, accurately and on a timely basis.	
i. Services provided to the FIs and related automated and manual processes, including controls, are set up and administered in accordance with mutually agreed instructions between OSP and FI. Such agreement might include standard operating procedures ("SOP") or other types of instructions.	Not Applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions/data on behalf of customers.

ii. Service procedures are documented, kept current and made available to appropriate personnel.	Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.
2. Services are subjected to internal checks to reduce the likelihood of errors.	
i. All services are recorded and checked against the FIs' specifications as defined in documented procedures. Errors or omissions are rectified promptly. All breaches and incidents (IT and non-IT) are tracked and escalated as per the SLA. Root cause analysis is conducted and, where appropriate, remedial actions are implemented to prevent recurrence. Error prevention and detection controls, e.g. reconciliations and "maker-checker" reviews, and error correction mechanisms are in place for key processes. ii. Management Information reports are generated as per the agreed procedure to report on the status of tasks performed. Key performance indicators ("KPIs") are monitored as per the agreed procedure.	Not applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions on behalf of customers. Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.
3. Services are processed in stages by independent parties such that there is segregation of duties from inception to completion.	
i. Appropriate segregation of duties is implemented for transaction processing through logical and/or physical access controls. ii. Access to record, authority to post and authorise transactions or services is restricted. Only authorised users have access to update customer service records.	Not applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions on behalf of customers. Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.
4. Sample controls for Data Entry Services **Data entry procedures are performed in an accurate and timely manner.**	
i. Input forms are stamped with the date/time of receipt ii. Input forms are batched and batch totals, e.g. number of forms are calculated and logged. iii. Batch totals are re-calculated upon data entry and reconciled with the log. Discrepancies are investigated and remediated. iv. Processed input forms are clearly marked to prevent re-input. v. Keyed data are verified against the original input forms to verify accuracy of data entry. vi. The identities of the maker and checker are recorded for accountability.	Not applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions on behalf of customers. Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.
5. Sample controls for Debt Collection Services **Collections and monies received are posted to customer accounts in an accurate and timely manner.**	
i. Documented collection procedures are documented to guide personnel in the debt collection process. ii. Debt collection instructions are scanned into a document imaging application for archiving and retrieval. iii. The outstanding amounts in debt collection instructions are recorded and reconciled to the collected amounts before posting to the FIs' accounts. iv. The debt collection report is reviewed by the checker before the posting is approved.	Not applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions on behalf of customers. Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.

v. The identities of the maker and checker are recorded for accountability.	
6. Sample controls for Physical and Electronic Statement Printing Services **Customer Statements are printed accurately and sent timely to FIs' customers.**	
i. Statement printing procedures are documented to guide personnel in the statement printing process. ii. A statement schedule outlines when statements are required to be printed and mailed for each customer. iii. System reports with batch and hash totals are reconciled to ensure the completeness and accuracy of printed statements. iv. The identities of the checker and verifier of system reconciliation reports are recorded for accountability.	Not applicable. VMware Cloud on AWS provides infrastructure for customers to host their workloads. VMware Cloud on AWS does not process any transactions on behalf of customers. Customers are responsible for managing their content, including maintaining completeness and accuracy of their content.

(c) Maintaining Records

These controls provide reasonable assurance that the OSP classifies data according to sensitivity, which determines protection requirements, access rights and restrictions, and retention and destruction requirements.

ABS Control Criteria	VMware Response
1. Data are classified according to sensitivity, which determines protection requirements, access rights and restrictions, and the retention and destruction requirements.	
i. Policies for data classification, retention and destruction are implemented. Retention is as required by local law (governing the FIs) or as required by the FIs.	VMware has a data classification policy that describes the controls over data lifecycle, from creation of the data to its destruction, and covers all forms of media while in use, in transit or archived. The policy is reviewed annually.
ii. Data held with the OSP (both in physical and electronic forms) are to be stored in appropriate media where the level of backups are determined based on the classification of data. For information/ records held in electronic storage media (including cloud based storage services), the OSP should ensure that appropriate levels of data/ record segregation exist to prevent co-mingling of data. Logical segregation is an acceptable form of control to segregate customer information held electronically.	i. VMware Cloud on AWS does not create image snapshots for customers. VMware Cloud on AWS backs up account information including system configuration settings, but does not provide data backup or archive services for customer content. VMware will not relocate, replicate, archive or copy customer content. VMware Cloud on AWS does not provide customer SDDC administration services, but provides customers self-service administrative tools to manage and/or isolate their virtual machines, physical hosts and/or SDDCs as required to secure their customer content. VMware Cloud on AWS provides customers with isolated environments which will not impact any other customers related to data retention or destruction. Customers have full control over their content, applications, and virtual machines to implement a solution to meet any legal holds requirements for management of their content.
iii. Procedures on retention of Information and Data should be implemented. These procedures should clearly state retention guidelines be based on the classification of information/data, applicable laws and agreed with the FIs.	ii. Administrative activities within VMware Cloud on AWS are recorded in audit logs collected across the VMware infrastructure and supporting SaaS services platforms. Each individual system within the larger VMware cloud platform sends the collected audit logs over SSL to a centralized log storage location with a WORM security storage policy. The audit logs from are then collected by a secured logging pipeline over SSL that sends the audit logs into a SIEM that is managed by the VMware employee managed Security Operations Center (SOC).

	The automated storage policy for all audit logs have a retention period of 3 years and logs are automatically purged when objects exceed the 3-year lifecycle. The storage objects and storage policies monitored by the VMware SOC and alerts are generated if the policy is violated or if there are any attempts to access the secured objects.
iv. Procedures on Destruction of Information and Data by the OSP should be implemented. These procedures should clearly state the secured destruction process based on the classification of information held. The procedures should be agreed with the FIs.	iii. Automated processes are in place that handle media sanitization before repurposing of any hardware. Upon the explicit deletion of a production environment by a tenant, a cryptographic wipe of the hard drives is performed via destruction of keys used by the self-encrypting drives. For more detail, 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* 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.
v. For terminated arrangements, the OSP should provide the FIs with the relevant evidence that demonstrates that all forms of data/records/information (both electronic and physical) the OSP have been promptly removed or deleted, destroyed or rendered unusable	i. Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their lifecycles. 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.

(d) Safeguarding Assets

These controls provide reasonable assurance that physical assets held by the OSP are safeguarded from loss, misappropriation and unauthorised access.

ABS Control Criteria	VMware Response
Physically assets are safeguarded from loss, misappropriation and unauthorised access.	
i. Physical access to the operational OSP’s office/facilities is restricted to authorised personnel at all times. The entry to office/ facilities is through an automated proximity access card entry control system.	i. 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. All 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 all access is logged and audited.
i. Access to offices/facilities after normal business hours is pre-approved. Access is monitored 24 hours a day, 365 days a year.	ii. VMware Cloud on AWS leverages AWS datacenters. AWS manages physical access to datacenters. Physical Access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, two-factor authentication s to access data center floors and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. For more information on AWS controls, please visit: https://cloudsecurityalliance.org/star-registrant/amazon-aws/ and

	data centers *https://aws.amazon.com/compliance/data-center/data-centers/*
i. Physical assets (e.g. office equipment, storage media) are tagged and are assigned to custodians. Fixed assets counts are performed every 12 months and movements of assets are tracked and recorded.	ii. VMware Cloud on AWS uses AWS datacenters. AWS manages equipment identification in alignment with the ISO 27001 standard. For more information, please see the AWS CAIQ *https://cloudsecurityalliance.org/star/registry/amazon/*

Service Reporting and Monitoring.

These controls provide reasonable assurance that OSP's engagement with FIs and sub-contractors handling material outsourcing and FIs' customer information are properly managed.

ABS Control Criteria	VMware Response
Outsourced activities are properly managed and monitored.	
i. A governance framework supported by policies, procedures, guidelines and standards is established to manage and deliver its services.	i. VMware has an established Third Party IT Risk Management Policy that applies to VMware's management and oversight of all 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 all third parties to ensure the security of information assets. Identification of risks related to external parties and access controls is performed as part of our Risk Management program and verified as part of our ISO 27001 audit. VMware vendors/suppliers do not have access to customer data.
ii. Due diligence and risk assessments of sub-contractors providing sub-contracted services are performed every 12 months. The due diligence includes the review of independent audit/expert assessment reports. The frequency of independent audit/expert assessment is agreed with the FIs..	ii. VMware conducts a 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 address 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.
iii. The governance procedures include regular training for employees and sub-contractors to ensure that employees and sub-contractors are aware of relevant regulatory requirements, e.g. anti-bribery and banking secrecy.	iii. In alignment with the ISO 27001 standard, all 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. Compliance audits are periodically performed to validate that employees understand and follow the established policies.

	Upon hire, personnel are required to read and accept the Acceptable Use Policy and the VMware Business Conduct Guidelines. Personnel who have access to our production environment receive additional training as they assume job roles and responsibilities within their specific department; training is completed before authorizing access to production systems. AWS maintains employee training programs to promote awareness of AWS information security requirements, including periodic Information Security training and compliance audits to validate that employees understand and follow the established policies.
iv. SLAs with FIs and sub-contractors clearly define performance monitoring (e.g. performance measures and indicators such as system uptime and turnaround time for document processing) and reporting requirements. Achievements of agreed key performance indicators (KPIs) and key risk indicators (KRIs) are tracked and monitored.	iv. VMware has made SLAs, Terms of Service, Data Processing Addendums, Privacy notices publicly available. They can be found here: VMware Universal End User License Agreement (EULA): *https://www.vmware.com/download/eula.html* Service Level Agreement *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf* 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. The real-time status of the VMware Cloud on AWS services along with past incidents is publicly available on https://status.vmware-services.io/. Availability reports are available to customers upon request within 45 days after a validated SLA event. VMware conducts risk assessments of vendors at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity, and availability of sensitive information.
v. Procedures are established for service recovery and reporting of lapses relating to the agreed service standards, including processes ensuring regular exchange of information and communication of critical issues.	v. As indicated above, the real-time status of the VMware Cloud on AWS services along with past incidents is publicly available on https://status.vmware-services.io/. Availability reports are available to customers upon request within 45 days after a validated SLA event
vi. The OSP arranges regular meetings with FI clients and sub-contractors to discuss performance and service delivery outcomes. Corrective actions and plans are prepared and agreed with FI clients and sub subcontractors to address performance and service delivery gaps.	vi. VMware monitors supplier performance and has a process to escalate issues to management as necessary. VMware has dedicated account management teams who are responsible for regular liaison with customers. Regular meetings are held with customers to discuss any performance issues and service delivery to ensure alignment with agreed level of service delivery in line with the terms of service.

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