# Hong Kong Monetary Authority – TM-G-1 General principles for technology risk management

VMware Cloud on AWS

vmware

## Executive Summary

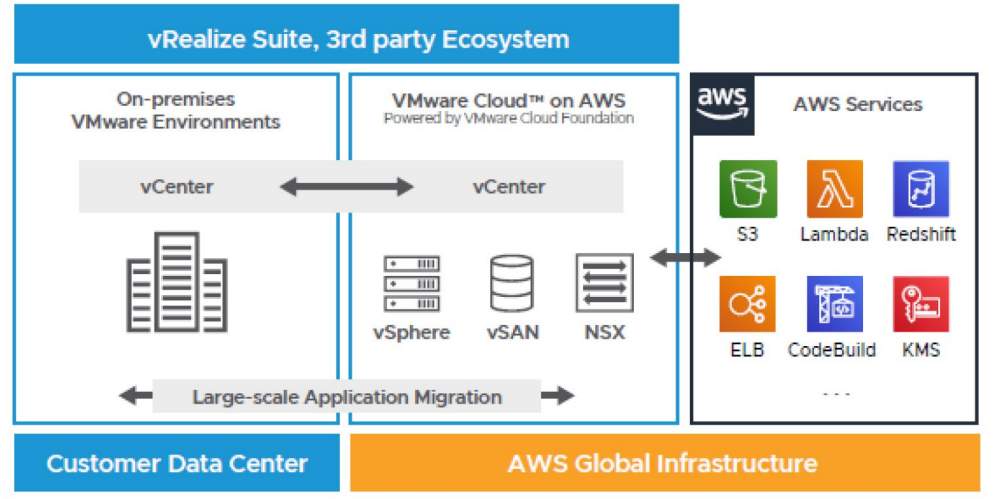
The Hong Kong Monetary Authority (HKMA) General Principles for Technology Risk Management provides a set of guidelines that HKMA expects authorized financial institutions to consider in their technology risk management processes, strengthen the security posture of their system, and implement measures to prevent and manage cyber security risks.

In this whitepaper, we map out the security controls and processes of VMware Cloud on AWS against the applicable guidelines of HKMA TM-G-1 General Principles for Technology Risk Management. 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 has implemented a wide range of security controls to help ensure we deliver a secure and reliable environment for financial services organizations to manage their IT infrastructure needs and manage data in line with leading industry standards and regulatory guidelines. You can view existing compliance and certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance*

## VMware Cloud on AWS

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



## HKMA TM-G-1 General Principles on Technology Risk Management.

The table below maps out VMware Cloud on AWS security controls and processes to the applicable principles of the HKMA TM G-1 General Principles on Technology Risk Management. An important reminder in reviewing the table below is that VMware Cloud on AWS operates on a Shared Responsibility Model with responsibilities shared between VMware, AWS and Customer. For further information see *Shared Responsibility Model*

| Control Principle # | Control Principle Requirements | VMware Responsibility | Customer Responsibility |
|---|---|---|---|
| **2. IT Governance** | | | |
| **2.1 IT control policies** | | | |
| 2.1.1 | Achieving a consistent standard of sound practices for IT controls across an AI requires clear direction and commitment from the Board and senior management. In this connection, senior management, who may be assisted by a delegated sub-committee, is responsible for developing a set of IT control policies which establish the ground rules for IT controls. These policies should be formally approved by the Board or its designated committee and properly implemented among IT functions and business units | 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. The policies are reviewed annually and approved by the designated committee. | Each VMware Cloud on AWS customer is responsible for developing, implementing, and monitoring policies and IT controls over their environment |
| 2.1.2 | IT control policies normally cover, at a minimum, the five aspects of IT controls mentioned in sections 3 to 7 of this module. They should be reviewed regularly, and where necessary updated to accommodate changing operating environments and technologies | VMware IT policies are reviewed annually. The policies cover wide range of areas such as Access Control, Governance, Incident Management, Third party risk management and Change Management. To support the policies VMware also maintains underlying process and procedure documents that enable teams to implement and maintain consistent processes. These documents are updated to accommodate any major change in environment or technologies. | Each VMware Cloud on AWS customer is responsible for developing, implementing, and monitoring policies and IT controls over their environment. |
| 2.1.3 | Senior management should ensure that processes used to verify compliance with IT control policies and the process for seeking appropriate approval for dispensation from IT control policies are specified clearly. Senior management should also define the consequences associated with any failure to adhere to this process. In general, the responsibility for ensuring compliance with IT | 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.<br><br>VMware management believes that establishing a relevant organizational structure includes considering key areas of authority and that serve both external customers, as well as | Each VMware Cloud on AWS customer is responsible for developing, implementing, and monitoring policies and IT controls over their environment |

| | | | |
|---|---|---|---|
| | control policies and the process for seeking dispensation rests with individual business units and IT functions, with the assistance of the technology risk management function (see subsection 2.3 below). | other business units within the company.<br><br>VMware Cloud on AWS undergoes regular external and internal audits where compliance with controls and policies are verified by the auditors. Any findings from the audits are followed up through to resolution. | |
| 2.1.4 | Senior management may put in place mechanisms (e.g. periodic reminders for relevant staff and policy orientation for new recruits) to promote awareness of IT control policies among relevant personnel on a regular basis. | VMware personnel are required to complete annual security awareness training. VMC support staff receive additional role-based security training to perform their job functions in a secure manner. Compliance audits are periodically performed to validate employees understand and follow the established policies. | Each VMware Cloud on AWS customer is responsible for conducting security awareness training for their staff on a regular basis. |
| **2.2 Oversight of organization and IT function** | | | |
| 2.2.1 | Senior management should establish an effective organisation of IT functions to deliver technology services and to provide day-to-day technology support to business units. A clear IT organisation structure and related job descriptions of individual IT functions should be documented and approved by senior management. | 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.<br><br>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. The VMware organizational structure provides the framework within which its activities for achieving the entity-wide objectives are planned, executed, controlled, and monitored.<br><br>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.<br><br>VMware also maintains documented position descriptions to define the skills, responsibilities, and knowledge levels required for specific jobs. | Each VMware Cloud on AWS customer is responsible for developing, implementing, and monitoring policies and IT controls over their environment |

| | | | |
|---|---|---|---|
| 2.2.2 | Proper segregation of duties within and among various IT functions is crucial for ensuring an effective IT control environment. In the event that an AI finds it difficult to segregate certain IT control responsibilities, it should put in place adequate compensating controls (e.g. peer reviews) to mitigate the associated risk | 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 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 AWS.<br><br>**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.<br><br>**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.<br><br>**AWS responsibility "Security of the Infrastructure"** – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.<br><br>See VMware Cloud on AWS Shared Responsibility Model whitepaper at *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmc-aws/vmware-shared-responsibility-model-overview-vmware-cloud-on-aws.pdf* | See response on the left |

| | | | |
|---|---|---|---|
| 2.2.3 | It is recommended that AIs establish an IT planning or steering committee which oversees whether IT resources are used effectively to support business strategies. This committee should normally consist of representatives of senior management, key business units and IT functions.<br>It should meet regularly and report to senior management, and where appropriate to the Board or its designated committee on the status of major technology-related initiatives and any material IT-related issues. | 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.<br><br>Senior management meets with the BOD quarterly to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments<br><br>Internal audit communicates with the Board of Directors on at least an annual basis to provide updates on information security. | Each VMware Cloud on AWS customer is responsible for implementing governance committees to oversee their IT environment. |
| 2.2.4 | In general, the IT planning or steering committee should also be responsible for developing an IT strategy to cover longer and short-term technology-related initiatives, taking into account new business initiatives, organisational changes, technological evolution, regulatory requirements, staffing and control related issues. The IT strategy should be formally documented, endorsed by the Board or its designated committee and senior management, as well as reviewed and updated at least on an annual basis. | VMware management meets on a regular basis to develop and discuss the IT strategy for organization as well as product strategy for VMware Cloud on AWS. Planning meetings are conducted quarterly to decide the product direction and features required in the future releases. | Each VMware Cloud on AWS customer is responsible for developing their own internal IT strategy and implement processes to monitor the IT strategy. |
| **2.3 Technology risk management function** | | | |
| 2.3.1 | IC-1 “General Risk Management Controls” specifies that AIs should have in place effective risk management systems and that new products and services should be subject to careful evaluation (including a detailed risk assessment) as well as a post-launch review. The same risk management controls apply to the technology risk management of AIs. | VMware has a dedicated Security teams for risk management to manage GRC for VMware Cloud on AWS. VMware employs third-party auditors to perform reviews against industry standards, including ISO 27001 which typically contain the controls that are in scope. In alignment with the ISO 27001 standard, VMware maintains a Risk Management program to mitigate and manage risk companywide. Risk assessments are performed at least annually to ensure appropriate controls are in place to reduce the risk related to security and availability of VMware Cloud on AWS | Each VMware Cloud on AWS customer is responsible for maintaining risk management systems to manage risk over their environment. |

| | | | |
|---|---|---|---|
| 2.3.2 | Senior management should establish clearly which function in the AI is responsible for implementing and managing the technology risk management process (the TRM function). Depending on the business and operational needs of individual AIs, the TRM function may refer to a dedicated department of an AI, or a group of departments or support units collectively performing the roles defined for this function. | VMware has dedicated teams for compliance and risk management for VMware Cloud on AWS. Executive and senior leadership, led by the VMware Chief Information Security Officer, play important roles in establishing the company's tone and values as it relates to information security. The Governance, Risk and Compliance teams, together with management, are responsible for managing technology risk. | Each VMware Cloud on AWS customer is responsible for maintaining risk management systems to manage risk over their environment. |
| 2.3.3 | The TRM function has a role to assist business units and IT functions in performing the technology risk management process which identifies, measures, monitors and controls technology-related risks. In addition, this function helps to ensure awareness of, and compliance with, the AI's IT control policies, and to provide support for investigation of any technology-related frauds and incidents. | VMware has a dedicated Security teams for risk management. VMware employs third-party auditors to perform reviews against industry standards, including ISO 27001 which typically contain the controls that are in scope. In alignment with the ISO 27001 standard, VMware maintains a Risk Management program to mitigate and manage risk companywide. Risk assessments are performed at least annually to ensure appropriate controls are in place to reduce the risk related security and availability of VMware Cloud on AWS | Each VMware Cloud on AWS customer is responsible for maintaining risk management systems to manage risk over their environment. |
| 2.3.4 | The TRM function should formulate a formal technology risk acknowledgement and acceptance process for reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. Typical reasons for such non-compliance are technology limitations (e.g. certain proprietary operating systems are only able to provide primitive password controls), business constraints (e.g. undesirable impact on customer services) and the costs outweighing the associated benefits. The process includes:<br>• a description of the risk being considered for acknowledgement by the owner of the risk and an assessment of the risk that is being accepted;<br>• identification of mitigating | VMware has dedicated teams to evaluate the effectiveness of the controls and risk management. The team evaluates findings identified from internal assessments and monitoring activities to identify improvement opportunities. The findings are documented in the nonconformity tracker. Appropriate personnel are assigned the responsibility for correcting the nonconformity and developing a corrective action plan, overseeing the implementation of the plan, providing updates to management, and closing the nonconformity. The nonconformities are discussed with respective business units as part of the interlock meetings. | Each VMware Cloud on AWS customer is responsible for developing their own internal technology risk management processes over their environment. |

| | | | |
|---|---|---|---|
| | controls;<br>• formulation of a remedial plan to reduce the risk; and<br>• approval of the risk acknowledgement from the owner of the risk and senior management. | | |
| **2.4 Technology audits** | | | |
| 2.4.1 | IC-1 "General Risk Management Controls" sets out the general objective and the importance of independence and expertise of AIs' internal audit function. As regards technology audits, AIs are expected to assess periodically their technology risk management process and IT controls. To ensure adequate coverage of the IT control environment and critical computer systems, an annual technology audit plan should be developed. AIs should also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified | VMware Cloud on AWS undergoes independent third-party audits on an annual basis to provide assurance to our customers that VMware has implemented robust security 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.<br><br>VMware utilizes internal/external audits to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and to identify areas of improvement. Audits are essential to the VMware continuous improvement programs. | Each VMware Cloud on AWS customer is responsible for conducting audits over their environment. |
| 2.4.2 | It is recognised that the internal audit function of some AIs may find it difficult to build up in-house technology audit expertise. In these circumstances, technology audit support may be supplemented by external specialists or internal technology auditors of other offices of the same<br>banking group. | Internal and external audits are performed at annually under the VMware information security management system (ISMS) program. VMware utilizes internal/external audits to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and to identify areas of improvement. Audits are essential to the VMware continuous improvement programs. | Each VMware Cloud on AWS customer is responsible for conducting audits over their environment. |
| **2.5 Staff competence and training** | | | |
| 2.5.1 | Given the rapid pace of technological development, senior management needs to ensure that staff of IT functions, the TRM function and internal technology auditors are competent and able to meet required levels of expertise and experience on an ongoing basis. It is also important to ensure that staffing levels are sufficient to handle present and expected work | 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. VMware also maintains documented position descriptions to define the skills, responsibilities, and knowledge levels required for specific jobs. | Each VMware Cloud on AWS customer is responsible for conducting training and awareness programs for their staff. |

| | | | |
|---|---|---|---|
| | demands, and to cater reasonably for staff turnover. | | |
| 2.5.2 | To ensure that an adequate training programme is in place for IT personnel, it is essential to establish a process to identify any material skill gaps of staff of technology-related functions. AIs may encourage and, where appropriate, facilitate their staff to acquire relevant professional qualifications, such as for those who are responsible for security management, technology risk management and technology audits. | Personnel supporting VMware Cloud on AWS role-based security training to perform their job functions in a secure manner. | Each VMware Cloud on AWS customer is responsible for conducting training and awareness programs for their staff. |
| **2.6 IT support provided by overseas offices** | | | |
| 2.6.1 | Some AIs may rely upon or work with their overseas offices (e.g. parent banks, subsidiaries, head offices or other regional offices of the same banking group) with regard to certain IT controls or support activities. Senior management should ensure that the respective responsibilities of the local and overseas offices in these areas are clearly set out in the relevant documents (e.g. policies, procedures or service agreements). | VMware's compliance team monitors compliance against VMware policies across regions it operates in. VMware Cloud on AWS implements controls and policies across the global instances of the product to enforce compliance with VMware's global and regional compliance requirements. | Each VMware Cloud on AWS customer is responsible for monitoring compliance over their environment against any of their own regional or global compliance requirements. |
| **3. Security Management** | | | |
| **3.1 Information classification and protection** | | | |
| 3.1.1 | For each application system, AIs should preferably assign an individual as the information owner. The information owner normally needs to work with the TRM and IT functions to ensure confidentiality and integrity of information, and to protect the information in accordance with the level of risk present and envisaged. | VMware has an established Asset Management policy that dictates management of assets at VMware including creation, processing, storage, transmission, deletion, and destruction. VMware maintains inventories of critical assets including asset ownership and location. | Each VMware Cloud on AWS customer is responsible for implementing policies and processes for information ownership and maintaining confidentiality and integrity of their customer data. |

| | | | |
|---|---|---|---|
| 3.1.2 | Information can be classified into different categories according to the degree of sensitivity (e.g. highly sensitive, sensitive, internal and public) to indicate the extent of protection required. To aid the classification process, AIs should ideally develop guidelines and definitions for each classification and define an appropriate set of procedures for information protection in accordance with the classification scheme. The level of detail of the information classification scheme adopted should be practicable and appropriate to AIs' circumstances. | 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. | Each VMware Cloud on AWS customer is responsible for implementing policies and processes over classification of their data. |
| 3.1.3 | Protection of information confidentiality should be in place regardless of the media (including paper and electronic media) in which the information is maintained. AIs should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media. | 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. | Each VMware Cloud on AWS customer is responsible for implementing policies and processes over classification of their data. |
| 3.1.4 | If cryptographic technology is used to protect the confidentiality and integrity of AIs' information, AIs should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include:<br>• provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure.<br>In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and | VMware has cryptographic key management policies in place to guide personnel on proper encryption key management.<br><br>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.<br>b. VMware Cloud on AWS SDDCs implement VMware NSX network security that enable customers to create IPsec VPN encrypted connectivity between sites.<br>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.<br>d. Connectivity to all management interfaces | Each VMware Cloud on AWS customer retains control and ownership of their customer data, and it is the customer's responsibility to ensure that all in-guest encryption keys and application data encryption keys are stored securely |

| | | | |
|---|---|---|---|
| | • adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys. | provided in VMware Cloud on AWS is performed via encrypted channels using TLS security. | |
| **3.2 Authentication and access control** | | | |
| 3.2.1 | Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine what application functions, system resources and data a user can access. For each application system, all users should be identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to ensure accountability for their activities. | VMware has established data, systems access policy, and associated access control standards designed to ensure achievement of account management, access enforcement, and separation of duties, role-based, least privilege, and appropriate remote, mobile, and wireless access. Key elements of this policy include system access authorization (role-based); user management (registration and deregistration, reviews, provisioning); inactive accounts; privilege access accounts; and monitoring. The policies and processes ensure data/assets access management is in adherence to legal, statutory, and regulatory compliance requirements.<br><br>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.<br><br>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. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for developing access control policy and procedures for access governance and authentication over their environment. |
| 3.2.2 | AIs should implement effective password rules to ensure that easy-to-guess passwords are avoided, and passwords are changed on a periodic basis. Stronger authentication methods should be adopted for transactions/activities of higher risk (e.g. payment transactions, financial messages and mobile computing). These usually entail multiple factors for | 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.<br><br>A break-glass access process is in place that enables only VMware engineers with the appropriate permissions to authenticate (using | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for developing access control policy and procedures for access governance and authentication over their environment. |

| | | | |
|---|---|---|---|
| | user authentication which combine something one knows (e.g. passwords) and something one has (e.g. a smart card or hardware security tokens). | 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 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). | |
| 3.2.3 | Extra care should be exercised when controlling the use of and access to privileged and emergency IDs.<br>The necessary control procedures include:<br>• granting of authorities that are strictly necessary to privileged and emergency IDs; • formal approval by appropriate personnel prior to being released for usage;<br>• monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);<br>• proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data centre); and<br>• change of privileged and emergency IDs' passwords immediately upon return by the requesters. | 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.<br><br>Managing access to information systems is implemented and controlled through centralized identity stores and directory services. A break glass 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 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). VMware Cloud on AWS does not create emergency or back-door IDs for VMware engineers, access is controlled via the break glass procedure described above. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for developing access control policy and procedures for access governance and authentication over their environment. |
| **3.3 Security administration and monitoring** | | | |

| | | | |
|---|---|---|---|
| 3.3.1 | A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. In particular, the function should cover the following areas:<br>• granting, changing and removing user access rights subject to proper approval of the information owners. In particular, proper procedures should be in place to ensure that a user's relevant access rights are removed when he leaves the AI or when his job responsibilities no longer require such rights;<br>• ensuring the performance of periodic user access re-certification (e.g. on an annual basis) that confirms whether user access rights remain appropriate and obsolete user accounts have been removed from the systems;<br>• reviewing security logs and violation reports in a timely manner; and<br>• performing incident analysis, reporting and investigation. | A break glass 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. 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). Privileged access is logged and captured in a centralized log server. VMware continuously collects and monitors services operation logs using SIEM technologies. The 24x7x365 VMware Security Operations Center uses the SIEM to correlate security monitoring information with public and private threat feeds to identify suspicious and unusual activities. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for developing access control policy and procedures for access governance and authentication over their environment. |

| | | | |
|---|---|---|---|
| 3.3.2 | Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function. | VMware has established data, systems access policy, and associated access control standards designed to ensure achievement of account management, access enforcement, separation of duties, role-based, least privilege, appropriate remote, mobile, and wireless access. Key elements of this policy include system access authorization (role-based); user management (registration and deregistration, reviews, provisioning); inactive accounts; privilege access accounts; and monitoring.<br><br>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 are 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. VMware does not require any user accounts that would provide VMware employees access to any customer Content. Access to customer content is controlled by each customer's use of authentication and authorization mechanisms to VMs, applications, and filesystems that hold their data. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for developing access control policy and procedures for access governance and authentication over their environment. |

| | | | |
|---|---|---|---|
| 3.3.3 | AIs should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours. The incident response and reporting procedures should include timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches. | VMware has a documented security incident management policy which is reviewed annually. VMware has Incident response program, plans, and procedures which are documented and implemented. 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.<br><br>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:<br><br>Chief Security Officer: The Chief Security Officer (CSO) provides executive sponsorship of the VMware security incident response policy, procedures, program, and team.<br><br>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.<br><br>The VMware Security Incident Response Team (vSIRT) is responsible for developing breach handling procedures, forensics, and they handle incident management across VMware.<br><br>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. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for implementing processes and procedure to monitor their IT infrastructure. |

| | | | |
|---|---|---|---|
| **3.4 System Security** | | | |
| 3.4.1 | Control procedures and baseline security requirements should be developed to safeguard application programs, operating systems, system software and databases. For example:<br>• access to data and programs should be controlled by appropriate methods of identification and authentication of users together with proper authorization;<br>• integrity of static data (e.g. system parameters) should be periodically checked to detect unauthorized changes;<br>• operating systems, system software, databases and servers should be securely configured to meet the intended uses with all unnecessary services and programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers;<br>• clear responsibilities should be established to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified, assessed, tested and applied to the systems in a timely manner;<br>• all configurations and settings of operating systems, system software, databases and servers should be adequately documented. Periodic certifications of the security settings should be performed (e.g. by the TRM function or the technology audit function); and • adequate logging and monitoring of system and user activities should be in place to detect anomalies, and the logs should be securely protected from manipulation | VMware has documented policies, standards and system and network diagrams supporting VMware Cloud on AWS. VMware documents, updates, and maintains baseline configurations for software and hardware installed in the production environment; changes are governed by a defined change management policy and baseline configurations are securely managed. Security baselines are documented to guide personnel to ensure appropriate configurations are in place to protect sensitive information.<br><br>VMware follows a strict policy of security baseline configuration that includes pre-implementation approvals and alignment with standards such as USGCB, FDCC, DISA, STIGs, and CIS Benchmarks. 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. | Each VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for implementing processes and procedure to monitor their IT infrastructure. |

| | | | |
|---|---|---|---|
| **3.5 End user and mobile computing** | | | |
| 3.5.1 | While end-user computing may offer advantages (e.g. higher productivity) to an AI, it may also increase the difficulty in controlling the quality of, and access to, the system. AIs should where necessary, therefore, establish control practices and responsibilities with respect to end user computing to cover areas such as data security, documentation, data/file storage and back-up, system recovery, audit responsibilities and training. | VMware Cloud on AWS uses HTTPS connections to connect to the service. Connections are encrypted to prevent any unauthorised access.<br><br>VMware support staff accessing the service for troubleshooting purposes use a break-glass access procedure. Access is time bound, 2 factor authenticated and any activity performed is logged. | VMware Cloud on AWS does not back up customer data. As part of shared responsibility model, each VMware Cloud on AWS customer is responsible managing security of their environment, including any end-user computing, data security, storage, backup, recovery, audit and training. |
| 3.5.2 | Controls over mobile computing are required to manage the risks of working in an unprotected environment. In protecting AIs' information, AIs should establish control procedures covering:<br>• an approval process for user requests for mobile computing;<br>• authentication controls for remote access to networks, host data and/or systems;<br>• protection (e.g. against theft and malicious software) of equipment and devices for mobile computing;<br>• use of data encryption software to protect sensitive information and business transactions in the mobile environment and when being transmitted; and<br>• back-up of data and/or systems in the mobile computing devices. | VMware has Mobile Device, Remote Access, and Acceptable Use policies that define the requirements for access to sensitive data. These policies are reviewed annually by the VMware Information Security team and validated as part of our audit process. VMware Cloud on AWS uses HTTPS connections to connect to the service and hence can be safely accessed via laptops. Connections are encrypted to prevent any unauthorised access.<br><br>VMware support staff accessing the service for troubleshooting purposes use a break-glass access procedure. Access is time bound, 2 factor authenticated and any activity performed is logged. | As part of shared responsibility model, customers are responsible for implementing policy and processes over mobile computing over their environment. |

| | | | |
|---|---|---|---|
| 3.5.3 | Software and information processing facilities are vulnerable to attacks by computer viruses and other malicious software. Procedures and responsibilities should be established to detect and prevent attacks. AIs should put in place adequate controls such as:• prohibiting the download and use of unauthorized files and software, and the access to doubtful web sites;<br>• installation and timely update of anti-virus software provided by reputable vendors;<br>• disallowing the download of executable files, and mobile codes, especially those with known vulnerabilities (e.g. through the use of corporate firewalls and proper configuration of the browser software); and<br>• prompt and regular virus scanning of all computing devices and mobile users' computers, and procedures for recovering from virus infections. | Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry- accepted timeframes. 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.<br><br>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 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 VMware Cloud on AWS customer retains responsibility for customer data. Customers are responsible for implementing processes and procedure to monitor their IT infrastructure. |
| **3.6 Physical and personnel security** | | | |
| 3.6.1 | Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centres and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities. | VMware Cloud on AWS uses AWS data centers. For details on AWS data center controls see *https://aws.amazon.com/compliance/data-center/controls/*<br><br>For details on how AWS addresses the HKMA requirements please visit *Hong Kong (SAR) (amazon.com)* | Customers are responsible for managing physical security over their local environment. |

| | | | |
|---|---|---|---|
| 3.6.2 | AIs should consider fully the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of their data centres. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could affect adversely the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator. | VMware Cloud on AWS uses AWS data centers. For details on AWS data center controls see *https://aws.amazon.com/compliance/data-center/controls/*<br><br>For details on how AWS addresses the HKMA requirements please visit *Hong Kong (SAR) (amazon.com)* | Customers are responsible for managing security over their local environment. |
| 3.6.3 | In controlling access by third-party personnel (e.g. service providers) to secure areas, proper approval of access should be required and their activities should be closely monitored. It is also important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for recruitment of permanent and temporary technology staff, and contractors. | There are no third parties that have access to the VMware Cloud on AWS environment. | As part of shared responsibility model, customers are responsible for conducting risk assessment over their third-parties. Customers are responsible for access governance and authentication of users over their environment |
| **4. System development and change management** | | | |
| **4.1 Project management** | | | |
| 4.1.1 | AIs should establish a general framework for management of major technology-related projects. This framework should, among other things, specify the project management methodology to be adopted and applied to these projects. The methodology should cover, at a minimum, allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, check points, key | VMware Cloud on AWS has a formal release management process for it's SDDC releases. The VMC Project Management Office (PMO) team manages this process and oversees the aspects of planning, scheduling, budgeting, milestones and release approvals. The release cycle involves Product Management team presenting the key feature requirements to wider teams and VMC management which are reviewed for feasibility. Once approved by management these are incorporated into the VMC release process which involves architectural reviews, technical analysis, | Each VMware Cloud on AWS Customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |

| | | | |
|---|---|---|---|
| | dependencies, quality assurance, risk assessment and approvals. | development, testing, quality assurance, risk assessments and security testing. Senior management from VMC product and engineering teams oversee the release process to ensure features are developed in line with product strategy and objectives. | |
| **4.2 Project life cycle** | | | |
| 4.2.1 | AIs should adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this should involve phases of project initiation, feasibility study, requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance. | In addition to the release process described above, VMware has a formal change management process for the changes involved in the feature releases. Change request must be documented in the change request tracking system and the required change management fields are completed.<br><br>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.<br><br>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.<br><br>VMware has also established emergency change management procedures to manage any urgent change requests or response to incidents.<br><br>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 to what | Each VMware Cloud on AWS Customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |

| | | | |
|---|---|---|---|
| | | they were prior to implementation of changes<br><br>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. | |
| 4.2.2 | The project life cycle methodology should define clearly the roles and responsibilities for the project team and the deliverables from each phase. It also needs to contain a process to ensure that appropriate security requirements are identified when formulating business requirements,<br>built during program development, tested and implemented. | See response above at 4.2.1 | Each VMware Cloud on AWS Customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |
| 4.2.3 | An independent party (e.g. the quality assurance function, the TRM function or the technology audit team), which is not involved in the project development, should conduct a quality assurance review of major technology-related projects, with the assistance of the legal and compliance functions if necessary. This review is to ensure compliance with the project life cycle methodology, other internal policies, control requirements, regulations and applicable laws. | The VMC Project Management Office (PMO) is involved in overseeing the VMC release process. The PMO team ensures that all required steps are completed in line with the release process and appropriate approvals are in place prior to the release. | Each VMware Cloud on AWS Customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |
| 4.2.4 | A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separated from the production environment.<br>Production data should not be used in development or acceptance testing unless the data has been desensitised (i.e. not disclosing personal or sensitive information) | 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 annually.<br><br>VMware has well established controls in place to protect and control access to all production | Each VMware Cloud on AWS Customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |

| | | | |
|---|---|---|---|
| | and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are promoted to the production environment. | 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.<br><br>VMware does not have access to customer data. Access to customer data is governed by customer's authentication and authorization mechanisms. VMware support staff does not need access to customer data for troubleshooting purposes. | |
| 4.2.5 | Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. As inappropriate handling of software licences may expose AIs to a significant risk of patent infringement, and financial and reputation losses, AIs should establish a formal software package acquisition process. In particular, the process should involve detailed evaluation of the software package (e.g. in terms of software licence, functionality, system performance and security requirements) and its supplier (e.g. its financial condition, reputation and technical capabilities). | VMware Cloud on AWS product is developed in-house. Software development is not outsourced to third parties. | Each VMware Cloud on AWS customer is responsible for their own software package acquisition and software license management in their environment |
| 4.2.6 | AIs should ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts. For mission-critical software packages, AIs may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of the software packages under certain circumstances, such as when the software vendors cease their business. | VMware has an established third-Party IT Risk Management Policy. 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. | Each VMware Cloud on AWS customer is responsible for developing and implementing policies to manage any third-party suppliers engaged in managing their environment |

| 4.3 Change management | | | |
|---|---|---|---|
| 4.3.1 | Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. An effective change management process helps to ensure the integrity and reliability of the production environment. AIs should develop a formal change management process that includes:<br>• classification and prioritisation of changes and determination of the impact of changes;<br>• roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;<br>• program version controls and audit trails;<br>• scheduling, tracking, monitoring and implementation of changes to minimise business disruption;<br>• a process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and<br>• a post implementation verification of the changes made (e.g. by checking the versions of major amendments). | 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 annually-. Change request must be documented in the change request tracking system and the required change management fields are completed.<br><br>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 has also established emergency change management procedures to manage any urgent change requests or response to incidents. 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.<br><br>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.<br><br>Emergency Change advisory board (ECAB): This is a subset of CAB members who make decisions about emergency changes. | Each VMware Cloud on AWS customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |

| | | | |
|---|---|---|---|
| 4.3.2 | To enable unforeseen problems to be addressed in a timely and controlled manner, AIs should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day). | VMware has established emergency change management procedures to manage any urgent change requests or response to incidents.<br><br>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 to what they were prior to implementation of changes | Each VMware Cloud on AWS customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |
| 4.3.3 | Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures. | VMware has also established emergency change management procedures to manage any urgent change requests or response to incidents.<br><br>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 to what they were prior to implementation of changes<br><br>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 can be viewed in the Site Recovery Manager (SRM) Add-on for VMware Cloud on AWS. | Each VMware Cloud on AWS customer is responsible for developing and implementing change control policy and processes to manage system changes over their environment. |

| | | | |
|---|---|---|---|
| **5. Information processing** | | | |
| **5.1 IT operations management and support** | | | |
| 5.1.1 | Management of IT functions should ideally formulate a service level agreement with business units to cover system availability and performance requirements, capacity for growth, and the level of support provided to users. The responsible IT functions should ensure that adequate procedures are in place for managing the delivery of the agreed technology support and services. | VMware Cloud on AWS has a Service Level Agreement and Service Description that describes the roles and responsibilities of VMware as a service provider and the obligations and rights of our customers.<br><br>These documents can be found at:<br>*https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf*<br><br>*https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf*<br><br>VMware also has central functions such as HR, Finance, Compliance and Information Security who provide services to the VMware Cloud Business Unit. Formal processes are in place internally to work together with these central functions. | Each VMware Cloud on AWS customer is responsible for reviewing the VMC on AWS SLA and Service Description to ensure that the commitments meet their requirements. |
| 5.1.2 | Detailed operational instructions such as computer operator tasks, and job scheduling and execution (e.g. instructions for processing information, scheduling requirements and system housekeeping activities) should be documented in an IT operations manual. The IT operations manual should also cover the procedures and requirements for on-site and off-site back-up of data and software in both the production and development environments (e.g. the frequency, scope and retention periods of back-up). | 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 regarding appropriate configurations to protect sensitive information. | Each VMware Cloud on AWS customer is responsible for developing operating processes and standards to manage their environment. |

| | | | |
|---|---|---|---|
| 5.1.3 | AIs should have in place a problem management system to respond promptly to IT operational incidents, to escalate reported incidents to relevant IT management staff and to record, analyse and keep track of all these incidents until rectification of the incidents. A helpdesk function can be set up to provide front-line support to users on all technology-related problems and to relay the problems to relevant IT functions for investigation and resolution. | 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.<br><br>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:<br><br>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.<br><br>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.<br><br>The VMware Security Incident Response Team (vSIRT) is responsible for developing breach handling procedures, forensics, and they handle incident management across VMware.<br><br>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 | Each VMware Cloud on AWS customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to all virtual machines that customer has deployed in their environment. |

| | | | |
|---|---|---|---|
| **5.2 Performance monitoring and capacity monitoring** | | | |
| 5.2.1 | AIs should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable problems to be identified and corrected before they affect system performance. This process should help the preparation of workload forecasts to identify trends and to provide information needed for the capacity plan, taking into account planned business initiatives. | VMware Cloud on AWS is architected to be highly available. In the event of a hardware failure, this unique cloud service is configured to automatically migrate to, or restart workloads on another host machine in the cluster and automatically restart the failed host. If the host machine fails to restart, or the performance of the restarted host is degraded, the service is capable of automatically replacing the failed host in a cluster with an entirely new host within minutes.<br><br>For details on these unique capabilities, please see the VMware Cloud on AWS service description *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf* | Each VMware Cloud on AWS customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to all virtual machines that customer has deployed in their environment. |
| 5.2.2 | Capacity planning should be extended to cover back-up systems and related facilities in addition to the production environment. | The VMware Cloud on AWS interface provides customers with information about capacity utilization to enable them to do capacity planning. Metrics data including resource utilization metrics are exposed via APIs as an option to feed into a customer's preferred capacity planning solution.<br><br>VMware Cloud on AWS also enables customers to increase capacity by adding hosts to a cluster on demand. These hosts are charged on an hourly basis and can be used to address spikes in demand for computing resources.<br><br>VMware Cloud on AWS continuously monitors consumption rates to ensure sufficient capacity for customers in each data center. | Each VMware Cloud on AWS customer is responsible for monitoring their utilization of services |
| **5.3 IT facilities and equipment maintenance** | | | |
| 5.3.1 | To ensure the continued availability of AIs' technology related services, AIs should maintain and service IT facilities and equipment (e.g. computer hardware, network devices, electrical power distribution, UPS and air conditioning units) in accordance with the industry practice, and suppliers' recommended service intervals and specifications. Proper | 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 deployments in multiple availability zones and separation of console availability and SDDC services availability.<br><br>VMware Cloud on AWS leverages AWS's | Each VMware Cloud on AWS customer is responsible for developing plans and processes to manage the business continuity and disaster recovery over their environment. |

| | | | |
|---|---|---|---|
| | record keeping (including suspected or actual faults, and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance. A hardware and facility inventory should be kept to control and track all hardware and software purchased and leased. These records can also be used for regular inventory taking. | 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.<br><br>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. | |
| **5.4 Disaster recovery planning** | | | |
| 5.4.1 | AIs should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. Please refer to TM-G-2 “Business Continuity Planning” on how to develop detailed recovery procedures of application systems and technology services, and ensure adequate insurance coverage of IT resources. | 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.<br><br>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.<br><br>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. | Each VMware Cloud on AWS customer is responsible for developing plans and processes to manage the business continuity and disaster recovery over their environment. |

| | | | |
|---|---|---|---|
| **6. Communications networks** | | | |
| **6.1 Network management** | | | |
| 6.1.1 | Communications networks convey information and provide a channel of access to application systems and systems resources. Given their technical complexity, communications networks can be highly vulnerable to disruption and abuse. Safeguarding communications networks requires robust network design, well-defined network services and sound discipline to be observed in managing networks. | VMware utilizes private networks and network security solutions, including firewalls and intrusion detection systems. VMware infrastructure is designed to provide 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.<br><br>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.<br><br>VMware Cloud on AWS provides 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. | Each VMware Cloud on AWS customer is responsible for configuring the network connections for inbound and outbound traffic on any customer instances deployed on VMware Cloud on AWS |
| 6.1.2 | Overall responsibility for network management should be clearly assigned to individuals who are equipped with the know-how, skills and resources to fulfil their duties. Network standards, design, diagrams and operating procedures should be formally documented, kept up-todate, communicated to all relevant network staff and reviewed periodically. | The default network configuration provided to each customer is set to deny all connections into the SDDC. | Each VMware Cloud on AWS customer is 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 user. |
| 6.1.3 | Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimised by automatic re-routing of communications through alternate routes should critical nodes or links fail (e.g. routing critical links to more than one external exchange or switching centre, and prearranging services with alternate telecommunications service providers). | VMware Cloud on AWS has multiple disaster recovery mechanisms in place to recover from multiple concurrent failures.<br>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.<br><br>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.<br><br>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. | Each VMware Cloud on AWS customer is responsible for developing plans and processes to manage the business continuity and disaster recovery over their environment. |
| 6.1.4 | The network should be monitored on a continuous basis. This would reduce the likelihood of network traffic overload and detect network intrusions. Monitoring activities include:<br>• monitoring network services and performance against pre-defined targets;<br>• reviewing volumes of network traffic, utilisation of network facilities and any potential | VMware monitoring process 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.<br>VMware monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate | Each VMware Cloud on AWS customer is responsible for monitoring their local infrastructure for security threats and vulnerabilities. |

| | | | |
|---|---|---|---|
| | bottlenecks or overloads; and<br>• detection of unusual network activities based on common attack characteristics. | problems or highlight areas in need of improvement.<br><br>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.<br><br>Communications from external parties and customers corroborate internally generated information or indicate problems.<br>Organizational structure and supervisory activities provide oversight of internal control functions and identification of deficiencies.<br>Operations management monitors delegated access to systems providing approval and temporary access to critical systems for system administration functions.<br><br>Results of VMware infrastructure backup jobs are monitored by VMware personnel to help confirm that backup jobs are completed successfully.<br><br>VMware utilizes network monitoring applications to analyse network device logs and report possible or actual network security breaches and monitor the central logging.<br><br>VMware performs vulnerability assessment on a quarterly basis and performs a penetration test annually to identify and monitor systems for potential security vulnerabilities.<br><br>Information security personnel perform monitoring of authentication and authorization systems, system audit log collection and analysis, security event management and security incident investigations 24x7x365. | |

| | | | |
|---|---|---|---|
| 6.1.5 | Powerful network analysis and monitoring tools, such as protocol analysers, network scanning and sniffer tools, are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage (e.g. viewing of unencrypted sensitive information). The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures. | VMware utilizes network monitoring applications to analyse network device logs and report possible or actual network security breaches and monitor the central logging. 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. | Each VMware Cloud on AWS customer is responsible for monitoring their local infrastructure for security threats and vulnerabilities. |
| **6.2 Network security and certification** | | | |
| 6.2.1 | To prevent insecure connections to an AI's network, procedures concerning the use of networks and network services need to be established and enforced. These should cover:<br>• the available networks and network services;<br>• authorization procedures for determining who is allowed to access particular networks and network services; and<br>• controls and procedures to protect access to network access points, network connections and network services. | VMware utilizes private networks and network security solutions, including firewalls and intrusion detection systems. VMware infrastructure is designed to provide 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 | Each VMware Cloud on AWS customer is responsible for monitoring their infrastructure for security threats and vulnerabilities. |

| | | | |
|---|---|---|---|
| 6.2.2 | AIs should consider segregating internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. For instance, the production systems should be located in dedicated network segments separated from other segments so that production network traffic is segregated from other traffic (e.g. connections to the internet, extranet connections to external parties and market data feeds). Sensitive data traffic between different network segments should be properly controlled and protected from being tampered with. | The VMware Cloud on AWS SDDC includes vSphere, vSAN and NSX and offers an additional layer of logical isolation.<br><br>VMware vSphere provides a third layer of separation via logical isolation using Virtual Machines and Resource Pools. vSphere also provides security features including Encryption, Access Management, and permissions, as well as comprehensive logging capabilities that allow customers to monitor access and changes to the virtual environment – including changes at the hypervisor level.<br><br>VMware Cloud on AWS cloud platform networks and systems are protected by segmentation and firewalls. Customer tenant networks and systems are also protected by dedicated firewalls. VMware utilizes AWS VPCs and AWS security services along with Cloud Trail logs and VPC Flow Logs to manage the security of the cloud platform. VMware continuously collects and monitors services operation logs using SIEM technologies. The 24x7x365 VMware Security Operations Center uses the SIEM to correlate security monitoring information with public and private threat feeds to identify suspicious and unusual activities. | Each VMware Cloud on AWS Customer is 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 user |
| 6.2.3 | Regular reviews of the security parameter settings of network devices such as routers, firewalls and network servers are required to ensure that they remain current. Audit trails of daily activities in critical network devices should be maintained and reviewed regularly. Network operational personnel should be alerted on a real-time basis to potential security breaches. | 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 VMware has formal processes in place to monitor the systems for security threats and vulnerabilities. These include processes such as SOC monitoring, threat detection, vulnerability assessments, penetration testing and security architecture reviews. Internal and external audits are conducted regularly to identify weakness and process improvement opportunities. | Each VMware Cloud on AWS customer is responsible for developing processes and standards to configure and monitor their network for security threats and vulnerabilities. Customers are responsible for managing their local LAN/WAN network and associated connections. |
| 6.2.4 | Network certification should be conducted when requesting local area network (LAN)/wide area network (WAN) additions or changes to AIs' corporate network. The additions or changes cover dial-in/out ports, switches, terminal servers, gateways/servers, routers, extranets and the public internet. | | |

| | | | |
|---|---|---|---|
| | The network certification process includes gathering data about the network environment, analysing any points of vulnerability and associated controls, and documenting whether approval is given or what additional controls are required for approval of connectivity. | | |
| 6.3.1 | If wireless local area networks (WLANs) are to be deployed, AIs should develop policies and procedures for approval, installation, operation and administration of WLANs. A risk assessment process for evaluating the sensitivity of information to be accessible via a WLAN should be formulated before a WLAN can be implemented. AIs should also develop a standard security configuration for WLAN products and follow the network certification process to ensure that WLANs are implemented in a secure manner so that they do not expose the corporate network to unmanaged risks. | | |
| 6.3.2 | Additional security measures may be needed between the wireless workstations and the wired network to provide stronger encryption and mutual authentication. WLANs should be segregated from the corporate network (e.g. by firewalls) to prevent any unauthorized access to the corporate network via WLANs | | |

| | | | |
|---|---|---|---|
| **7. Management of technology service providers** | | | |
| **7.1 Management of technology outsourcing** | | | |
| 7.1.1 | While AIs are expected to take into account the general guidance specified in SA-2 "Outsourcing" when managing technology outsourcing12, they should also have regard to the following controls:<br>• technology service providers should have sufficient resources and expertise to comply with the substance of the AIs' IT control policies;<br>• in case of outsourcing of critical technology services (e.g. data centre operations), AIs are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider. The independent assessment report should set out clearly the objectives, scope and results of the assessment and should be provided to the HKMA for reference;<br>• the outsourcing agreement should specify clearly, among other things, the performance standards and other obligations of the technology service provider, and the issue of software and hardware ownership. As technology service providers may further sub-contract their services to other parties, AIs should consider including a notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services;<br>• further to the regular monitoring activities set out in SA-2 "Outsourcing", AIs should conduct | VMware Cloud on AWS does not outsource any software development or technical support. All software development and technical support for VMware Cloud on AWS is performed in-house. | Each VMware Cloud on AWS customer is responsible for evaluating the suppliers in line with their organizational and regulatory policy and procedures |

| | | | |
|---|---|---|---|
| | an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services; • AIs should try to avoid placing excessive reliance on a single outside service provider in providing critical technology services; and<br>• AIs should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include an exit management plan and identification of additional or alternate technology service providers for such support and services | | |
| **7.2 Management of other technology service providers** | | | |
| 7.2.1 | Apart from technology outsourcing, AIs may rely on some outside technology service providers in the provision of technology-related support and services (e.g. telecommunications and network operators). AIs should have in place guidelines on how to manage different kinds of major outside technology service providers. Similar to the general principles set out in SA-2 "Outsourcing" and subsection 7.1 above, the guidelines may need to cover the selection process of service providers, the process for approving material exceptions, and the need to avoid over-reliance upon a single technology service provider in critical technology services. | VMware Cloud on AWS does not outsource any software development or technical support. All software development and technical support for VMware Cloud on AWS is performed in-house. | Each VMware Cloud on AWS customer is responsible for evaluating the suppliers in line with their organizational and regulatory policy and procedures |

## Conclusion

VMware Cloud on AWS and 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 virtual, and cloud environments. VMware has supported a wide range of organizations across the globe to rapidly drive scalability and growth through future ready technology solutions.

VMware Cloud on AWS has undergone independent third-party audits on a regular basis to provide assurance to our customers that VMware has implemented robust controls. VMware Cloud on AWS has been audited for the following industry certifications: ISO 27001, ISO 27017, ISO 27018, SOC2, MTCS, IRAP, OSPAR, ISMAP and PCI-DSS.
VMware Cloud on AWS helps 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.

## Further reading

- *vmware-shared-responsibility-model-overview-vmware-cloud-on-aws.pdf*
- *HKMA STM-G-1 General Principles on Technology Risk Management*
- *HKMA SA-2 Outsourcing*
- *VMware Cloud Trust Center*

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