Response to Japan Financial Industry Information Systems (FISC) Security Guidelines on Computer Systems for Financial Institutions

VMware Cloud on AWS

vmware®

Table of contents

Executive Summary

The Center for Financial Industry Information Systems (FISC) founded by the Minister of Finance and Bank of Japan have established a set of security controls and guidelines to promote information security measures for financial institutions. These are called the FISC Security Guidelines on Computer Systems for Financial Institutions. The FISC guidelines are a comprehensive set of requirements to enable financial institutions to strengthen the security posture of their system and implement measures to prevent and manage cyber security risks.

In this whitepaper we describe the security controls and processes VMware Cloud on AWS has in place to address the FISC Security Guidelines on Computer Systems for Financial Institutions - Ninth Edition. 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.

Structure of the whitepaper

We have structured this whitepaper in line with the FISC guidelines structure. The guidelines are categorized into four areas:

Control Guidelines: Guidelines relating to implementation of internal and external control structures, policies, human resources management, outsourcing management and implementing sound IT governance measures.

Practice Guidelines: Guidelines relating to management of information security and system operations needed to enhance the security and operational reliability of IT systems.

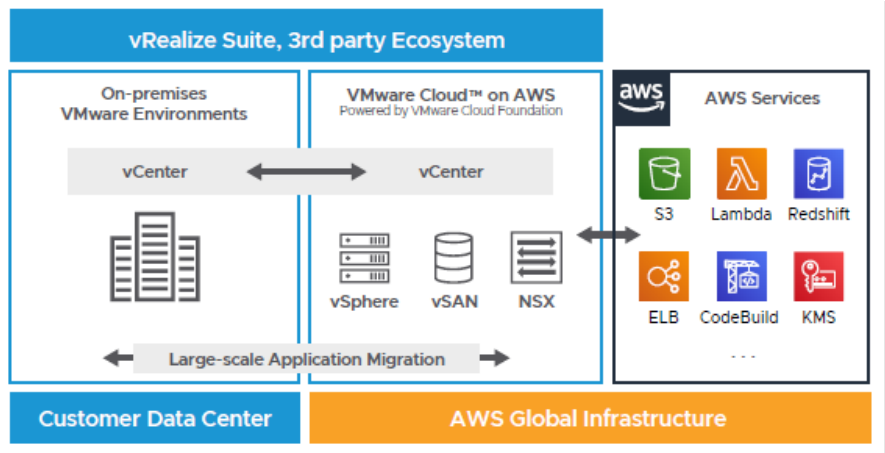
Facilities Guidelines: Guidelines relating to protection of physical infrastructure and computing facilities.

Audit Guidelines: Guidelines relating to implementing audit and compliance controls.

In the sections below, we have demonstrated how VMware Cloud on AWS addresses the guidelines prescribed in the above areas.

VMware Cloud on AWS

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



Managing outsourcing risk and compliance with VMware Cloud on AWS

VMware has implemented a wide range of security controls to help set up a secure and reliable environment for financial institutions to manage workloads and address various compliance requirements, including the FISC guidelines. You can view existing compliance certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance* .

VMware Cloud on AWS also undergoes independent third-party audits on a regular basis to provide assurance to our customers that VMware has implemented industry leading controls. VMware Cloud on AWS has been audited for the following industry certifications: ISO 27001, ISO 27017, ISO 27018, SOC2 and PCI-DSS. A number of other compliance offerings are in our public roadmap at *https://cloud.vmware.com/vmc-aws/roadmap*.

Conclusion

VMware software-defined data center (SDDC) technologies lead the industry in delivering the flexibility, protection, and scalability that financial services organizations need to deliver exceptional customer experiences and new business models across physical, virtual, and cloud environments. VMware has supported a wide range of financial services organizations across the globe to rapidly drive scalability and growth through future ready technology solutions, please visit *https://www.vmware.com/solutions/industry/financial-it-services.html*. VMware Cloud on AWS will help financial institutions to meet their security and privacy compliance obligations with an enterprise ready SDDC that leverages both on-premises and cloud resources for rapid application portability and operational consistency across the environment

FISC - Control Guidelines

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
Internal Control	(1) Policy/Plan	C1	Establish regulations that define important matters pertaining to system security measures.	VMware has an established information security framework and policies which have integrated with the ISO 27001 framework. The policies are published on intranet and name of the person responsible for policy is shown. Policies are reviewed every 12 months. VMware security policies go through a comprehensive review process by multiple teams. Security is of the utmost importance to us. Our programs are continually evolving based on our own experiences, changes in the threat landscape, and our learnings based on industry observation and collaboration. For more information about VMware Security programs: https://www.vmware.com/security.html	A.18 - Compliance
		C2	Formulate system scheme, development, and operation plans based on a medium- to long-term perspective.	Executive and senior leadership, led by the VMware Chief Security Officer, plays important role in establishing the Company's tone and values as they relate to information security. VMware regularly develops and reviews its security strategy to ensure appropriate programs are implemented to protect information assets and to support the organizational IT and business strategy.	A6.1 Internal Organization
		C3	For system development planning, check for proper consistency with medium- and long-term system planning and obtain proper approval.	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 in any authorization of changes applied to the production environment. VMware regularly conducts internal and external audits that include results from security and compliance assessments. The program utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also to identify areas of improvement.	A6.1 Internal Organization A12.1.2 Change Management
	(2) Organizational structure	C4	Establish a security management system.	VMware has an established information security framework and policies which have integrated the ISO 27001 framework. The policies are published on intranet and name of the person responsible for policy is shown. Policies are reviewed every 12 months.	A.18 - Compliance
		C5	Establish a framework that combats cyber-attacks.	VMware has an established information security framework and policies which have integrated the ISO 27001 framework. VMware employs third party auditors to perform reviews against industry standards. VMware Cloud on AWS has been audited for the following industry certifications: ISO 27001, ISO 27017, ISO 27018, SOC2, and PCI-DSS	A.18 - Compliance
		C6	Establish a system management system.	The VMware organizational structure provides the framework within which its activities for achieving the entity-wide objectives are planned, executed, controlled, and monitored. The following key personnel are involved in the design, development, operation, implementation, maintenance and monitoring of VMware Cloud on AWS: • **Executive Management**: Responsible for overseeing companywide activities, establishing, and accomplishing goals and overseeing objectives • **Human resources:** Responsible for HR policies, practices, and processes with a focus on the key HR delivery areas (e.g., talent acquisitions, pre-employment screening, employee retention, compensation, benefits, performance management, employee relations, and training and development)	A6.1 Internal Organization

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				• **VMware Engineering**: Responsible for design, development, documentation, and system test plans • **VMware System Reliability Engineering (SRE) team:** Responsible for automation, upgrades and patch management, monitoring, maintenance, and troubleshooting • **VMware Information Security team**: Responsible for security operations, incident management, compliance certification, security audits, and risk analysis. • **Global Support Services:** Responsible for handling customer support issues and inquiries.	
		C7	Establish a data management system.	In VMware Cloud on AWS, all VMware management appliance VMs and customer Workload VMs reside on the VMware managed storage subsystem (encrypted vSAN), meeting requirements for encrypted data at rest. Customer data is stored within customer managed virtual machines to which only customers control access. In addition, only customers control access to data stored on the associated virtual machine file systems. Virtual machine access is governed by each customer's implementation of an authentication and authorization mechanism, like LDAP services, Microsoft Active Directory services, or local accounts configured within the virtual machine operating system. VMware does not provide services that would require any customer to allow/authorize VMware employees to access their Content (virtual machines, operating systems, applications, file systems, or data).	A9 Access Control
		C8	Establish a network management system.	VMware delivers each SDDC with a secure by default (deny-all) configuration. VMware provides each customer a secured/isolated configuration by default which can be customized via self-service tools, as required by the customer's administrators. Customers manage Firewall Rules to allow/block access to the vCenter appliances & other workload VMs in their SDDCs, connect to direct connect networks, and create Virtual Private Networks (VPN) to encrypt traffic between customer networks and the VMC SDDC networks. Each customer must configure & monitor all of the networks they create that connect to their VMs, OS, and applications for malicious threats with tools and operational processes to respond to security risks. Each SDDC is protected by a pair of customer managed VMware NSX-T firewalls that secure N-S traffic. Additionally, customer managed NSX-T distributed firewalls may be provisioned to provide E-W traffic security and network segmentation.	A9.1.2 Access to networks and network services
		C9	Establish operational organizations.	VMware Cloud on AWS operates a shared security responsibility model between Customers, VMware, and AWS. Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users. VMware responsibility "Security of the Cloud" – VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS. AWS responsibility "Security of the Infrastructure" – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.	A12.1 Operational Procedures and Responsibilities

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				For further details see *VMware Cloud on AWS - Shared Responsibility Model whitepaper*	
		C10	Establish and maintain an organization for disaster prevention.	VMware Cloud on AWS has multiple disaster recovery mechanisms in place to recover from multiple concurrent failures. Redundancy and blast isolation are built into the architecture of the service to ensure high availability of the VMware Cloud on AWS, including regional independence and separation of console availability and customer service availability. VMware Cloud on AWS leverages the specific underlying AWS provider's infrastructure to enable customers to run workloads in multiple areas within a region as well as in multiple geographic regions. VMware monitors the service's infrastructure and receives notifications directly from AWS in the event of a failure. VMware has developed processes with AWS to ensure that that we have defined responses in place if an upstream event occurs. The architecture of AWS provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. However, customers who require redundancy of their workloads on another provider can use VMware DRaaS. As a part of the VMware Business Impact Analysis, dependencies on third parties are documented to ensure appropriate business continuity measures are in place. The VMware business continuity plans and documentation are reviewed annually as part of the enterprise independent attestation process. The VMware Information Security Management System (ISMS) is based on the ISO 27001 framework. Business continuity and redundancy plans are reviewed by VMware third-party auditors who will perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under NDA as they become available. Customers have the ability to architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. Customers retain control and ownership of their Customer Content and have the ability to utilize their own backup and recovery mechanisms including establishing a redundant cloud infrastructure in their own data centers and/or using any one of thousands of VMware partners that run vSphere. Some of these BC/DR options can be automated to reduce changes required to management of customer workloads.	A 17 Information security aspects of business continuity management
		C11	Establish a proper crime prevention organization.	VMware performs annual risk assessments as part of the VMware ISMS program to support security and compliance programs. The framework security requirements have been designed and implemented to address industry best practices around security and privacy. This policy requires the identification of applicable regulatory and contractual requirements, technical compliance with information security policies, protection of records, protection of information systems audit tools, and audit controls and reporting. This policy also requires VMware to adhere to the applicable legal, statutory, regulatory, or contractual obligations related to information security and security requirements. VMware also conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to the service.	A7 Human Resources Security
		C12	Establish regulations for each operation.	VMware performs annual risk assessments as part of the VMware ISMS program to support security and compliance programs. The framework security requirements have been designed and implemented to address industry best practices around security and privacy. This policy requires the identification of applicable regulatory and contractual requirements, technical compliance with information security policies, protection of records, protection of information systems audit tools, and audit controls and reporting. This policy also requires VMware to adhere to the	A18. Compliance

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				applicable legal, statutory, regulatory, or contractual obligations related to information security and security requirements.	
	(3) Evaluation of management status	C13	Confirm the status of security observance.	VMware has an established information security framework and policies which have integrated the ISO 27001 framework. The policies are published on intranet and name of the person responsible for policy is shown. Policies are reviewed every 12 months. Internal and external audits are performed regularly to ensure VMware is compliant with relevant regulations, policies, and processes. In addition, annual information security training is provided to employees to ensure they understand the security responsibilities.	A.18 – Compliance A7.2.2. Information security awareness, education and training
	(4) Personnel (Staffing/Training)	C14	Carry out security training.	All new and existing employees must accept the VMware security policy and complete security training, which describe the responsibilities and expected behavior with regard to information and information system usage, on an annual basis. Additional training and agreements are required for some systems prior to being granted access.	A7.2.2. Information security awareness, education and training
		C15	Carry out education to improve skills of personnel.	All new and existing employees must accept the VMware security policy and complete security training, which describe the responsibilities and expected behavior with regard to information and information system usage, on an annual basis. Additional training and agreements are required for some systems prior to being granted access.	A7.2.2. Information security awareness, education and training
		C16	Provide proper education and training for possible failures and disasters.	All new and existing employees must accept the VMware security policy and complete security training, which describe the responsibilities and expected behavior with regard to information and information system usage, on an annual basis. Additional training and agreements are required for some systems prior to being granted access.	A7.2.2. Information security awareness, education and training
		C17	Implement disaster prevention and crime prevention training.	All new and existing employees must accept the VMware security policy and complete security training, which describe the responsibilities and expected behavior with regard to information and information system usage, on an annual basis. Additional training and agreements are required for some systems prior to being granted access.	A7.2.2. Information security awareness, education and training
		C18	Implement proper personnel management for staff.	In alignment with ISO 27001 VMware has developed a Risk Management program to mitigate and manage risk companywide. VMware has corporate human resource management policy and employee handbook that provide guidelines for expected behavior from staff and various processes in place for personnel management.	A7. Human resources security
		C19	Implement proper health care management for employees.	In alignment with ISO 27001 VMware has developed a Risk Management program to mitigate and manage risk companywide. VMware has corporate human resource management policy and employee handbook that provide guidelines for expected behavior from staff and various processes in place for personnel management. VMware has a number of programs in place to manage employee mental and physical health to ensure we provide a safe working environment for our staff.	A7. Human resources security

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
External Control	(1) Outsourcing management	C20	When outsourcing, identify the purpose and scope beforehand and clearly define the procedures for selecting contractors.	VMware has an established Third-Party IT Risk Management policy. The policy applies to VMware's management and oversight of all third parties (vendor /supplier) accessing or processing company data facilities, information, and/or information systems. It defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. Sourcing and business teams collaborate with the information security risk team to ensure a risk-based approach is taken with respect to all third parties to ensure the security of information assets. VMware also has a defined procurement process for vendors and contractors that involve multiple levels of due diligence and approvals to ensure that any vendors are selected in line with purpose and desired scope.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships
		C21	Conclude proper contracts with the contractor, including provisions on security measures.	VMware has formal contract management processes in place that involve multiple level of reviews from Legal, Compliance, and Information Security teams. Information security and data privacy requirements are agreed with vendors as part of contractual procedures. VMware also monitors vendors on a regular basis to identify any information security risks with vendors.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships
		C22	Ensure that the contractor's staff complies with the rules and check their state of compliance.	VMware has an established Third-Party IT Risk Management policy. The policy applies to VMware's management and oversight of all third parties (vendor /supplier) accessing or processing company data facilities, information, and/or information systems. It defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. Sourcing and business teams collaborate with the information security risk team to ensure a risk-based approach is taken with respect to all third parties to ensure the security of information assets. VMware also has a defined procurement process for vendors and contractors that involve multiple levels of due diligence and approvals to ensure that any vendors are selected in line with purpose and desired scope.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships
		C23	Establish a management structure for outsourcing and check the state of the performance of outsourced tasks.	VMware has an established third party risk management policy that mandates periodic review, monitor, and audit of third party service delivery to ensure alignment with agreed level of information security and service delivery in line with the third party supplier agreement. Based on risk and business impact, changes to the provision of services by the third-party suppliers shall be appropriately managed.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships
	(2) Use of cloud services	C24	When using a cloud service, set up security measures with cloud service-specific risks considered.	VMware's third-party risk management policy covers all kinds of suppliers including cloud services. VMware evaluates the service risk based on the type of service and type of data hosted by the supplier and implements appropriate processes to address specific risks. VMware also maintains a data processing addendum that covers the requirements for managing and processing personal data in line with applicable data processing regulations.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships
	(3) Shared data center	C25	Set up security measures against emergencies at the shared data center.	VMware Cloud on AWS uses AWS geographically resilient data center hosting facilities. Data centers are built in clusters in various global regions. VMware provides customers the flexibility to place VMware Cloud on AWS instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region to minimize risk. AWS has documented policies and procedures for monitoring and performing preventive maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				procedures are carried out by qualified persons and completed according to a documented maintenance schedule. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventive maintenance is performed to maintain the continued operability of equipment. AWS security management standards follow the best practices and comprehensive security controls of ISO/IEC 27001:2013. AWS manages physical access to datacenters as defined in the AWS Data Center Physical Security Policy. For more information on AWS controls, please visit: https://cloudsecurityalliance.org/star/registry/amazon https://aws.amazon.com/compliance/data-center/data-centers/	
	(4) Services on financial institutions' mutual system network	C26	Implement proper risk management upon using services on the financial institutions' mutual system network.	As a cloud provider, the VMware Cloud on AWS is aligned with internationally recognized standards as evidence of our commitment to information security at every level of the organization and the security program is in accordance with industry leading best practices. Platform and application security standards are consistent with industry-accepted guidance and standards, such as, but not limited to, NIST, ISO, and CIS. VMware Cloud on AWS has established an Information Security Management System (ISMS) based on ISO 27001 standards, as well as ongoing compliance programs (SOC, HIPAA, and others), to manage risks relating to confidentiality, integrity, and availability of information. As part of shared security responsibility model, customers are responsible for implementing risk management procedures over their environment.	A: 15.1.1, 15.1.2, 15.1.3 Supplier relationships

FISC - Practice Guidelines

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
Information Security	(1) Data protection	P1	Take measures to prevent others from finding out personal identification numbers and passwords.	VMware's acceptable use policy requires computers and mobile devices to be secured, and access protected with screen locking software controlled by a password/pin, token or similar user authentication mechanism. VMware acceptable use policy applies to all VMware employees, consultants, agents, vendors, and other independent contractors who have access to information systems and assets owned or leased by VMware, connected to a VMware network or residing at a VMware location. The acceptable use policy requires that the use of VMware information and VMware information systems be managed responsibly by users to maintain the appropriate confidentiality, integrity, and availability of data and the infrastructure supporting the enterprise. VMware has established an authentication and password policy, that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC2. Customers are responsible for managing end user access and password configurations for applications and customer resources including developing procedures to safeguard their passwords.	A: 9.3 User responsibilities

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P2	Provide the function of identifying a called terminal.	N/A – Customers are responsible for managing access controls over their terminals	N/A
		P3	Take measures for the protection of stored data against disclosure.	All customer content imported to VMware Cloud on AWS is stored on dedicated physical NVMe storage hardware that is self-encrypting by default. By default, all customer data at rest is also encrypted by vSAN XTS AES-256 cipher data-at-rest encryption, with two levels of keys: KEK (as the master key) and DEK (per-disk data key). In addition, the AWS Key Management Service is used to generate the Customer Master Key (CMK) to work with the two, (KEK & DEK), keys are generated by vSAN. The combination of these keys ensures maximum security and allows for key rotation as required by the customer. As part of shared responsibility model, customers control access to data stored on the associated virtual machine file systems. Virtual machine access is governed by each customer's implementation of an authentication and authorization mechanism, like LDAP services, Microsoft Active Directory services, or local accounts configured within the virtual machine operating system	A.5 Information Security Policies A.9 access control A.9.1 A.9.2 A.9.3 A.9.4 A.10.1 – Cryptographic controls
		P4	Take measures to prevent leakage of transmission data.	Communication networks that transport sensitive information (authentication, administrative access, customer information, etc.) are encrypted with standard encryption mechanisms. VMware provides customers with the ability to create IPSEC and SSL VPN tunnels from their environments which support the most common encryption methods including AES-256. Also available is AWS Direct Connect to provide a private high bandwidth network connection between AWS and your datacenter, office, or colocation environment. Encrypted vMotion is available at VMware Cloud on AWS between hosts inside the Cloud SDDC.	A.5 Policy groups for information security A.5.1.1 A.5.1.2 A.13 Communication security A.13.1 A.13.2
		P5	Provide the function of controlling access to files.	In VMware Cloud on AWS, all VMs reside on the VMware managed storage subsystem (encrypted vSAN). Customer data is stored within customer managed virtual machines to which only customers control access. In addition, only customers control access to data stored on the associated virtual machine file systems. Virtual machine access is governed by each customer's implementation of an authentication and authorization mechanism, like LDAP services, Microsoft Active Directory services, or local accounts configured within the virtual machine operating system. VMware does not provide services that would require any customer to allow/authorize VMware employees to access their virtual machines, operating systems, file systems, applications, or data.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P6	Reinforce the functions of detecting any defective data.	As part of shared security responsibility model, customers are responsible for their data, including maintaining quality and integrity of customer data.	N/A
		P7	Take measures for the detection of tampered transmitting data.	Communication networks that transport sensitive information (authentication, administrative access, customer information, etc.) are encrypted with standard encryption mechanisms. VMware provides customers with the ability to create IPSEC and SSL VPN tunnels from their environments which support the most common encryption methods including AES-256. Also available is AWS Direct Connect to provide a private high bandwidth network connection between AWS and your datacenter, office, or colocation environment. Encrypted vMotion is available at VMware Cloud on AWS between hosts inside the Cloud SDDC.	A.5 Policy groups for information security A.5.1.1 A.5.1.2 A.11 A.12 Operational security

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				As part of shared security responsibility model, customers are responsible for their data, including maintaining quality and integrity of customer data.	A.12.1 A.12.4 A.12.6 A.13 Communication security A.13.1 A.13.2
	(2) Prevention of unauthorized use	P8	Set up functions of personal identification.	VMware has established an authentication and password policy, that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC2. 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 employee access to support the IaaS platform is limited to operations involving physical hosts, hypervisors, and management appliances. VMware does not require any user accounts that would provide VMware employee access to any customer content. Access to customer content is governed by each customer's use of authentication and authorization mechanisms to VMs and filesystems that hold their data.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P9	Provide the function of preventing unauthorized use of IDs.	VMware has established an authentication and password policy, that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC2.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P10	Manage access records.	Audit logs are collected across the VMware infrastructure and supporting SaaS services platforms and are sent to a centralized log storage location with a secure storage policy. The audit logs from are then collected by a secured logging pipeline that sends the audit logs into a SIEM that is managed by the VMware employee managed Security Operations Center (SOC). The lifecycle for all audit logs has a retention period of 3 years. The storage policies applied to audit logs are monitored by the VMware SOC and alerts are generated if the policy is violated or if there are any attempts to change the policy that protects the storage. The VMware Cloud on AWS SDDC logs are made available to all customers: vRealize Log Insight Cloud (vRLIC) delivers unified visibility through robust log aggregation, analytics, and faster root cause determination. The vRealize Log Insight Cloud SaaS service provides near real-time visibility of operations and security relevant logging of the SDDC infrastructure. The logging pipeline from the VMC platform includes SDDC logs from NSX Edge devices and populates within the vRealize Log Insight Cloud Service. This service has retention, archiving, export, and forwarding capabilities to meet	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4 A.12.3 – Logging and monitoring

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				the flexibility requirements of most customers. The recommended option would be to leverage native capabilities of vRealize Log Insight Cloud and also to consider forwarding the VMware Cloud on AWS log files to a customer managed SIEM.	
		P11	Provide the functions of limiting transactions.	Customers are responsible for controlling access to their data and implementing functions to limit transactions.	N/A
		P12	Provide the function of prohibiting transactions when an accident occurs.	Customers are responsible for controlling access to their data and implementing functions to restrict transactions.	N/A
		P13	Provide a function that protects cryptographic keys on devices and media that store electronic encryption keys, or software included with them.	vSAN Encryption on VMware Cloud on AWS uses the AWS KMS service to get the primary key, referred to as Customer Master Key, or CMK. One CMK is generated per cluster. In addition, there are two other keys generated by vSAN. A cryptographically secure key is generated by vSAN for every vSAN disk. This key is referred to as Disk Encryption Key or DEK. A third cryptographically secure intermediate key is generated for every disk, called local key encryption or local KEK for short. The DEK is encrypted using the local KEK and the local KEK is in turn encrypted using the AWS CMK. The AWS generated CMK never leaves the HSM backed AWS KMS and is not accessible to any AWS employees. AWS KMS is designed so that no one, including AWS employees, can retrieve your plaintext master keys from the service. The service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of your keys when you use AWS KMS to create your keys. Customer plaintext keys never leave the HSMs, are never written to disk, and are only ever used in the volatile memory of the HSMs for the time needed to perform requested cryptographic operation. The AWS KMS Key ensures that the encrypt and decrypt functions are done securely and outside of the system that encrypts the data. The AWS KMS CMK does not encrypt the data, it protects the VMware keys that encrypts the data. The KEK and DEK are created by vSAN and stored in secured memory on each ESX host.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4 A.10.1 – Cryptographic controls
	(3) Set up functions for protection against unauthorized access from external network	P14	Take preventive measures against unauthorized access from external networks.	The VMware comprehensive vulnerability management program includes annual vulnerability scanning and penetration testing to maintain compliance requirements. If components typically vulnerable to malware are used within the service, anti-malware programs are installed. The VMware Cloud on AWS services do not use these components. Anti-malware systems are configured and updated based on industry accepted timeframes. Network layer, application, and internal vulnerability scans are performed regularly as a part of the vulnerability management program. Vulnerability scans are reviewed as a part of the annual compliance audit and assessment program. VMware uses firewalls to restrict and control network traffic and access to systems, data, and applications. Firewalls act as critical components of the VMware network and information security architecture; therefore, they shall be designed, implemented and administered appropriately. VMware firewalls are operated in compliance with the Infrastructure Security policy in order to support the protection of VMware information systems.	A.5 Policy groups for information security A.5.1.1 A.5.1.2 A.11 A.12 Operational security A.12.1 A.12.4 A.12.6 A.13 Communication security A.13.1 A.13.2

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P15	Minimize connected devices that can be accessed from external networks.	Communication networks that transport sensitive information (authentication, administrative access, customer information, etc.) are encrypted with standard encryption mechanisms. VMware provides customers with the ability to create IPSEC and SSL VPN tunnels from their environments which support the most common encryption methods including AES-256. Also available is AWS Direct Connect to provide a private high bandwidth network connection between AWS and your datacenter, office, or colocation environment.	A.5 Policy groups for information security A.5.1.1 A.5.1.2 A.11 A.13 Communicatio n security A.13.1 A.13.2
	(4) Measures to detect unauthorized access	P16	Provide the function of monitoring unauthorized access.	To support the VMware Cloud on AWS platform, a tightly controlled "Delegated Access" process is in place that enables only VMware engineers with the appropriate permissions to authenticate (using MFA) to a system to generate one-time use certificates and credentials that are user-specific with limited time-bound access to troubleshoot and remediate issues on the physical hosts, hypervisors, and service management appliances. Access must be tied to a support ticket and all access is logged & monitored and any suspicious activity is investigated by VMware's Security Operations Center (SOC). VMware does not have access to customer content. VMware does not require any user accounts that would provide VMware employee access to any customer content (virtual machines, operating systems, applications, file systems, or data). Access to customer content is solely governed by each customer's use of authentication and authorization mechanisms to secure access to VMs, applications, and filesystems that hold their data.	A.5 Policy groups for information security A.5.1.1 A.5.1.2 A.11 A.12 Operational security A.12.1 A.12.4 A.12.6 A.13 Communicatio n security A.13.1 A.13.2
		P17	Provide the functions of identifying any unusual transactions.	Customers are responsible for implementing procedures for identifying any unusual transactions	N/A
		P18	Provide the functions of monitoring exceptional transactions.	Customers are responsible for implementing procedures for identifying any unusual transactions	N/A
	(5) Response measures for unauthorized access	P19	Take measures for protection against unauthorized access and of recovering.	VMware delivers each SDDC with a secure by default (deny-all) configuration. VMware provides each customer a secured/isolated configuration by default which can be customized via self-service tools, as required by the customer's administrators. Customers manage firewall rules to allow/block access to the vCenter appliances & other workload VMs in their SDDCs, connect to direct connect networks, and create Virtual Private Networks (VPN) to encrypt traffic between customer networks and the VMC SDDC networks. Each customer must configure & monitor all of the networks they create that connect to their VMs, OS, and applications for malicious threats with tools and operational processes to respond to security risks. Access to customer content, is solely governed by each customer's use of authentication and authorization mechanisms to secure access to VMs, applications and filesystems that hold their data as well revoking access to the VMs.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
	(6) Measures against malicious programs	P20	Take preventive measures against malicious programs such as	Anti-malware programs are installed if components typically vulnerable to malware are used within the service. Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry accepted timeframes.	A.5 Information Security Policies A.5.1

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			computer viruses.	The VMware Cloud on AWS service is built on the VMware Photon OS and VMware ESXi. The VMware Cloud on AWS Operations team disables unnecessary ports, protocols, and services to harden the production environment. VMware applies security templates via Group Policy Object and we further harden servers through scripts. All traffic passes through a firewall before reaching proxy servers in our DMZ. Managed interfaces are configured to deny-all communications traffic by default and allow network communications traffic by exception.	A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P21	Take proper precautions to detect any computer viruses and other malicious programs.	Anti-malware programs are installed if components typically vulnerable to malware are used within the service. Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry accepted timeframes. The VMware Cloud on AWS service is built on the VMware Photon OS and VMware ESXi. The VMware Cloud on AWS Operations team disables unnecessary ports, protocols and services to harden the production environment. VMware applies security templates via Group Policy Object and we further harden servers through scripts. All traffic passes through a firewall before reaching proxy servers in our DMZ. Managed interfaces are configured to deny-all communications traffic by default and allow network communications traffic by exception. Customers are responsible for implementing anti - malware/anti-virus applications over their environment.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P22	Take measures for cases involving damage from malicious programs such as computer viruses.	VMware has the capability to rapidly patch vulnerabilities across all of the computing devices, applications, and systems that support the IaaS cloud platform. Remediation efforts and timelines are prioritized and applied using industry best practices. VMware does not provide scans of customer VMs or any customer applications running on the VMs in the SDDC. Patching customer VMs is the sole responsibility of customers. VMware notifies customers of potential changes and events that may impact security or availability of the services through portal notifications, release notes, and email.	A.12 Operational security A.12.1 A.12.2 A.12.3 A .12.4 A.12.5 A.12.6 A.12.7
Common guidelines for system operations	(1) Documentation	P23	Document and maintain manuals for operation in normal times.	VMware maintains comprehensive documentation over key information security management functions such as around network security management procedures, architecture diagrams, incident management, and compliance. Additionally, VMware has developed reference architectures which are designed to provide solution ideas and recommended topologies based on real-world examples, for deploying, configuring, and managing solutions. In these architectures, we have also provided some high-level guidance on how to perform some of the configuration steps. These should be used in conjunction with the service documentation from both VMware and AWS to ensure your deployments are tailored to meet your individual circumstances and are as successful as possible. Customers retain control and ownership of their customer content and remain responsible for controlling access to their content and managing its quality and accuracy.	A.12 Operational security A.12.1 A.12.2 A.12.3 A .12.4 A.12.5 A.12.6 A.12.7
		P24	Prepare manuals used in case of a failure or disaster.	VMware has a defined Information Security Program that includes Business Continuity and Disaster Recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. This program implements appropriate security controls to protect its employees and assets against natural and manmade disasters. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and	A.17 Information security aspects in business continuity management A.17.1

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training. VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. A Risk Assessment is performed on a regular basis to identify natural and manmade threats based upon a geographically specific business impact assessment. Reviews are triggered through change management, new projects, and critical process reviews. The resulting security mechanisms and redundancies are in turn reviewed through regular audits.	A.17.2
	(2) Management of access rights	P25	Definition of access authority to resources and systems.	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. The VMware Cloud on AWS platform utilizes a tightly controlled "Delegated Access" process is in place that enables only VMware engineers with the appropriate permissions to authenticate (using MFA) to a system to generate one-time use certificates and credentials that are support user-specific with limited time-bound access. Customers retain control and ownership of their customer content and remain responsible for controlling access to their content.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P26	Take proper precautions not to make passwords known to anyone other than respective users.	VMware has established an authentication and password policy, that outlines the password requirements for VMware's information assets such as minimum password configurations, password restrictions, secure logon procedures, criteria for strong passwords, and password administration. Password controls have been audited by external third parties as part of the certification process for ISO 27001 and SOC2.	A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
		P27	Define the procedures for authorizing access to various resources and systems and reviewing the access authorization.	VMware has established policies and procedures for granting and revoking terminated access to systems. A user access review audit is performed on a periodic basis to ensure service access is still appropriate. Customers are responsible for managing access to the administrative console and end-user access to customer resources.	A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
	(3) Data management	P28	Clearly explain how to provide, receive, and manage data files.	Customers are responsible for managing access to their data files including receiving, managing, backup, and archival of customers' data	N/A
		P29	Define the procedures for revision control of data files.	Customers are responsible for managing access to their data files including receiving, managing, backup, revision, and archival of customers' data	N/A
		P30	Operational management methods should be defined for the use of	vSAN Encryption on VMware Cloud on AWS uses the AWS KMS service to get the primary key, referred to as Customer Master Key, or CMK. One CMK is generated per cluster. In addition, there are two other keys generated by vSAN. A cryptographically secure key is generated by vSAN for every	A.5 Information Security Policies A.5.1

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			cryptographic keys.	vSAN disk. This key is referred to as Disk Encryption Key or DEK. A third cryptographically secure intermediate key is generated for every disk, called local key encryption or local KEK for short. The DEK is encrypted using the local KEK and the local KEK is in turn encrypted using the AWS CMK. The AWS generated CMK never leaves the HSM backed AWS KMS and is not accessible to any AWS Employees. AWS KMS is designed so that no one, including AWS employees, can retrieve your plaintext master keys from the service. The service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of your keys when you use AWS KMS to create your keys. Customer plaintext keys never leave the HSMs, are never written to disk and are only ever used in the volatile memory of the HSMs for the time needed to perform requested cryptographic operation. The AWS KMS Key ensures that the encrypt and decrypt functions are done securely and outside of the system that encrypts the data. The AWS KMS CMK does not encrypt the data, it protects the VMware keys that encrypts the data. The KEK and DEK are created by vSAN and stored in secured memory on each ESX host.	A.9 access control A.9.1 A.9.2 A.9.3 A.9.4 A.10.1 – Cryptographic controls
	(4) Operation proficiency	P31	Conduct education and training for operational proficiency.	VMware provides security policies and security training to all employees to educate them as to their roles and responsibilities concerning information security. Employees are responsible for completing annual security training.	A: 7.2.2 Human resource security
	(5) Computer Antivirus protection	P32	Take measures against computer viruses.	Anti-malware programs are installed if components typically vulnerable to malware are used within the service. Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry accepted timeframes. The VMware Cloud on AWS service is built on the VMware Photon OS and VMware ESXi. The VMware Cloud on AWS Operations team disables unnecessary ports, protocols, and services to harden the production environment. VMware applies security templates via Group Policy Object and we further harden servers through scripts. All traffic passes through a firewall before reaching proxy servers in our DMZ. Managed interfaces are configured to deny-all communications traffic by default and allow network communications traffic by exception. Customers are responsible for implementing anti-malware/anti-virus applications over their environment.	A.5 Information Security Policies A.5.1 A.9 access control A.9.1 A.9.2 A.9.3 A.9.4
	(6) External connection management	P33	Define the conditions of contract for external connection.	VMware delivers service in line with terms of service. Please see the below links for the relevant documents Service Description https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf Terms of Service https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-cloud-services-universal-tos.pdf	A 13.1.2, 13.2.2 Communications security
		P34	Establish operational management methods for external connections.	VMware Cloud on AWS SDDC network connectivity is configured by each customer to enable IPSEC VPN or AWS Direct Connect. Customer administrator access to VMs can be configured to only allow access from specific networks. VMware has also published an operations management guide that shows how customers can set up and manage connections	A 13.1.2, 13.2.2 Communications security
Operations Management	(1) Management of operations	P35	Verify operator qualifications.	VMware has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods	A: 7.2.2 Human resource security

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				include orientation for new employees, training for employees, and the use of email messages to communicate time sensitive information. Customers are responsible for ensuring that staff handling admin activities over their environment have sufficient understanding of the roles and responsibilities.	
		P36	Define the procedures for assignment and approval of operations.	Customers are responsible for defining the procedures for assignment and approval of operations of their staff handling administrative activities on the platform.	N/A
		P37	Establish and maintain an organization for system operations.	VMware has dedicated teams for information security management, engineering, and development. Customer support and site reliability engineers (SRE) provide troubleshooting support for customers' SDDCs. Customers are responsible for maintaining an organization for system operations over their environment	A6.1 – Internal organization
		P38	Make a record for checking of operations.	VMware management and InfoSec teams monitor the Support ticketing process for SRE and the assignment of tickets with an approval process. All SRE activities are monitored closely and tracked. SRE engineers are assigned Support tickets to troubleshoot platform issues that impact customers' SDDCs but troubleshooting by SREs does not need to access customer data. Activities by both the SRE and customer admins are logged in the Monitor tab in vCenter and vCenter logs are stored in vRealize Log Insight Cloud for customer log management. Customers can monitor for any type of behavior (customer admin or SRE activity) that is not aligned with their security policy by reviewing the SDDC logs.	A6.1 – Internal organization A12.3 – Logging and monitoring
	(2) Data file management	P39	Save backup copies of data files.	VMware Cloud on AWS does not create image snapshots for customers. VMware Cloud on AWS backs up Account Information including system configuration settings but does not provide data backup or archive services for customer data. Customers are responsible for the end-to-end lifecycle for all their data. Customers are responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive and restoration for all customer Content and configurations created by the customer in the SDDC, including Virtual Machines, Content Libraries, Datastores, and Port Groups. Customers have various options to implement data replication and data protection using available VMware provided solutions, 3rd party tools, or VMware partner solutions.	A12.3 - Backup
	(3) Program File management	P40	Define how to manage program files.	VMware has a controlled trusted code build and deployment process using immutable artifacts. VMware has integrated validations that include container signing, certificates and auth token credential processes into the software supply chain to maintain a secure continuous delivery pipeline. VMware uses industry leading code scanning tools to detect potential security issues. VMware identifies security defects using multiple methods which can include automated and manual source-code analysis. Every release of VMware Cloud on AWS goes through a security architectural review, security audits by both the product security teams and the cloud security teams, manual & automated code analysis, vulnerability scans, and additional reviews necessary to meet industry leading security standards. VMware Security personnel must approve each release to validate internal processes and mitigate software security risks to customers. *VMware Product Security Whitepaper* Customers are responsible for managing access to their Virtual machines and customer data.	A.5 Information Security Policies A.5.1 A.14 System acquisition, development and maintenance A.14.1 A.14.2

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P41	Save backup copies of program files.	VMware performs regular backups of the code repositories supporting VMware platform. Customers are responsible for back up of their content and virtual machines	A12.3 - Backup
	(4) Network Configuration management	P42	Manage network configuration information.	VMware follows a strict policy of security baseline configuration that includes pre-implementation approvals and alignment with standards STIGs, and CIS Benchmarks. All security baseline configuration changes are reviewed for approval in a timely manner. The Vulnerability Management team also maintains a central repository of security baseline configurations to satisfy legal/regulatory requirements. VMware has security controls in place to reduce the risk of unauthorized access to sensitive information in the production environment. File integrity of the VMware Cloud on AWS console application is enforced via the container management system and the file integrity of the tenant environment is enforced by the VMware Fleet Management System. VMware Cloud on AWS has several intrusion detection mechanisms in place. The service continuously collects and monitors the environment logs which are correlated with both public and private threat feeds to spot suspicious and unusual activities. Additionally, the service has intrusion detection devices such as honeypots in place.	13.1.1 (Communications security)
		P43	Save backup copies of network configuration information.	VMware Cloud on AWS backs up Account Information including system configuration settings but does not provide data backup or archive services for Customer Content. As part of shared responsibility model, customers are responsible for back up of their content and virtual machines	A12.3 - Backup
	(5) Document management during operation	P44	Define the document storage and management method during system operation.	VMware backs up account information, configuration settings and audit logs in AWS S3 buckets. As part of shared responsibility model, customers are responsible for back up of their content and virtual machines	A12.3 - Backup
		P45	Save backup copies of documents required in preparation for restoring operations in the event of a disaster.	VMware backs up account information, configuration settings and audit logs in AWS S3 buckets. VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as multiple geographic regions. Each Availability Zone is designed as an independent failure zone. In case of failure, customers can configure automated processes to move customer data traffic away from the affected area. The architecture of the AWS infrastructure provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. VMware monitors AWS infrastructure and receives notifications directly from AWS in the event of a provider failure. VMware has developed processes with AWS to ensure that that we have defined disaster recovery mechanisms in place in the event that an upstream event occurs. Customers are responsible for the end-to-end lifecycle for all their data. Customers are responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive, and restoration for all customer Content and configurations created by the customer in the SDDC, including Virtual Machines, Content Libraries, Datastores, and Port Groups. Customers have various options to implement data replication and data protection using available VMware provided solutions, 3rd party tools or VMware partner solutions.	A12.3 – Backup A17 – Information security aspects of business continuity
	(6) Monitoring of operations	P46	Establish a monitoring system to monitor the	Administrative activities within VMware Cloud on AWS are recorded in audit logs collected across the VMware infrastructure and supporting SaaS services platforms and are sent to a centralized log storage location with a WORM security	A12.3 – Logging and Monitoring

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			progress of system operation.	storage policy. The audit logs from are then collected by a secured logging pipeline over SSL that sends the audit logs into a SIEM that is managed by the VMware employee managed Security Operations Center (SOC). The automated storage policy for all audit logs has a retention period of 3 years and logs are automatically purged when objects exceed the 3-year lifecycle. The storage objects and storage policies monitored by the VMware SOC and alerts are generated if the policy is violated or if there are any attempts to access the secured objects.	
Facilities Management	(1) Resource management	P47	Check the capabilities and usage situations of various resources.	VMware Cloud on AWS provides a dedicated environment to customers. VMware Cloud on AWS continuously monitors platform metrics to ensure sufficient capacity for customers in each data center.	A12.1.3 Capacity Management
	(2) Device management	P48	Conduct hardware and software management.	VMware maintains inventories of critical assets including asset ownership. Asset inventory is updated in real-time as assets are connected to the network. Classification of critical assets ensures security and resiliency of critical business operations and service availability. VMware asset management policy provides guidance for asset lifecycle including asset ownership, acceptable use, removal of assets, and secure disposal and reuse. VMware asset management policies and procedures are classified as Confidential. All VMware information Security Policies were validated and updated to internationally recognized ISO27001 standards in our compliance programs. VMware third party auditors perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under NDA.	A8. Asset Management
		P49	Define the device management method.	VMware Cloud on AWS leverages AWS datacenters. AWS manages physical access to datacenters. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, two-factor authentication to access data center floors and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. For more information on AWS controls, please visit: https://cloudsecurityalliance.org/star-registrant/amazon-aws/ and data centers https://aws.amazon.com/compliance/data-center/data-centers/	A11. Physical and Environmental Security
		P50	Take measures to protect network-related devices.	VMware Cloud on AWS leverages AWS datacenters. AWS manages physical access to datacenters. Physical Access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, two-factor authentication to access data center floors and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. For more information on AWS controls, please visit: https://cloudsecurityalliance.org/star-registrant/amazon-aws/ and data centers https://aws.amazon.com/compliance/data-center/data-centers/	A11. Physical and Environmental Security
		P51	Define the device maintenance method.	AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. Regular maintenance and testing are conducted for both the UPS and generators and data centers have contracts for emergency fuel delivery. Facilities personnel monitors all critical electrical systems and components 24x7x365.	A11. Physical and Environmental Security

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P52	Conduct preventive maintenance on devices.	AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. Regular maintenance and testing are conducted for both the UPS and generators and data centers have contracts for emergency fuel delivery. Facilities personnel monitors all critical electrical systems and components 24x7x365.	A11. Physical and Environmental Security
	(3) Maintenance and management of computer-related equipment	P53	Define the method to manage computer-related facilities.	See response at P51	See response at P51
		P54	Define the method through which to maintain computer-related facilities.	See response at P51	See response at P51
		P55	Confirm the capabilities and usage situations of computer-related facilities.	See response at P51	See response at P51
	(4) Physical access control (building and rooms)	P56	Grant entry (rooms) rights and manage keys.	See response at P50	See response at P50
		P57	Execute physical access control.	See response at P50	See response at P50
		P58	Execute room access control.	See response at P50	See response at P50
		P59	Operations conducted after entry into the room should be managed.	See response at P50	See response at P50
	(5) Monitoring	P60	Establish proper monitoring systems for each facility.	See response at P51	See response at P51
Use of systems	(1) Transaction management	P61	Define operational authority for each transaction.	VMware Cloud on AWS provides infrastructure to host, build, manage, and run workloads. Customers are responsible for defining and implementing transaction management and data input/output processes over their applications and environment.	N/A
		P62	Properly control the operator cards.	See response at P61	See response at P61
		P63	Keep a log of transaction operations performed from terminals and inspect the log.	See response at P61	See response at P61
		P64	Establish a reception	See response at P61	See response at

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			system for reports from customers, and implement the management of troubled accounts.		P61
	(2) Input/Output management	P65	Manage data input.	See response at P61	See response at P61
		P66	Take measures to prevent unauthorized action and to protect security in generating and handling output information.	See response at P61	See response at P61
	(3) Forms management	P67	Establish a method for managing unused important forms.	Customers are responsible for implementing procedures to manage unused forms	N/A
		P68	Establish and maintain the procedures for handling of important printed forms.	VMware Cloud on AWS provides infrastructure to host, build, manage, and run workloads. Customers are responsible for defining and implementing processes to manage their content.	N/A
	(4) Protection of customer data	P69	Take measures for the protection of customer data.	See response at P68	See response at P68
Emergency responses	(1) Measures for handling failures and disasters Responsive measures	P70	Define the procedures for communicating with responsible persons in case of failure and disaster.	VMWare maintains defined business continuity and disaster recovery plans and implements appropriate security controls to protect its employees and assets against natural or man-made disasters. VMware Cloud on AWS uses AWS geographically resilient data center hosting facilities. AWS carefully chooses our data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity. Data centers are built in clusters in various global regions. VMware provides customers the flexibility to place VMware Cloud on AWS instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region to minimize risk. For more information, please see the AWS CSA CAIQ submission *https://cloudsecurityalliance.org/star/registry/amazon/* & To access the AWS ISO 27001 report, please see *https://aws.amazon.com/compliance/*	A17. Information security aspects of business continuity
		P71	Establish definite measures against failures and disasters.	VMware follows industry standard frameworks that specify requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. Additionally, VMware follows information security standards in the context of a business continuity program to determine the impact of any disruption by measuring the criticality and establishing priorities across the business. VMware has implemented measures to prepare for a critical business disruption so that its people, processes, systems, facilities, and other assets are able to respond, recover, and resume operations safely and efficiently; and make sure that there is effective communication with all stakeholders, thus	A17. Information security aspects of business continuity

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				minimizing financial, customer, brand, and operational impact to the company. VMware has implemented backup and redundancy mechanisms to ensure compliance with regulatory, statutory, and contractual obligations. VMware has a defined Information Security Program that includes Business Continuity (BC) and Disaster Recovery (DR) strategies that include hardware redundancy, network configuration redundancy, backups, and regular testing exercises for the VMware Cloud on AWS operations platform. Audits are performed to validate plan processes and procedures annually under the VMware information security management system (ISMS) program.	
		P72	Identify and analyze possible causes of any failure.	VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as multiple geographic regions. Each Availability Zone is designed as an independent failure zone. In case of failure, customers can configure automated processes to move customer data traffic away from the affected area. The architecture of the AWS infrastructure provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers. VMware monitors AWS infrastructure and receives notifications directly from AWS in the event of a provider failure. VMware has developed processes with AWS to ensure that that we have defined disaster recovery mechanisms in place in the event that an upstream event occurs. VMware Cloud on AWS has conducted successful DR testing and continues to test annually.	A17. Information security aspects of business continuity
	(2) Formulation of contingency plans	P73	Formulate a contingency plan.	VMWare maintains defined business continuity and disaster recovery plans and implements appropriate security controls to protect its employees and assets against natural or man-made disasters. VMware Cloud on AWS uses AWS geographically resilient data center hosting facilities. AWS carefully chooses our data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity. Data centers are built in clusters in various global regions. VMware provides customers the flexibility to place VMware Cloud on AWS instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region to minimize risk. For more information, please see the AWS CSA CAIQ submission https://cloudsecurityalliance.org/star/registry/amazon/ & To access the AWS ISO 27001 report, please see *https://aws.amazon.com/compliance/* Customers are responsible for implementing contingency plans and back up processes over their content.	A17. Information security aspects of business continuity
	(3) Backup centers	P74	Establish backup centers.	VMware provides the following backup and restore services: Management infrastructure including: vCenter Server, NSX Manager, NSX Controller, and VMware NSX Edge Customers are responsible for all data protection, backup/archive and restoration of the following: All customer Content and configurations created by the customer in the SDDC, including Virtual Machines, Content Libraries, Datastores, and Port Groups.	A12.3 Backup
System development and modification	(1) Management of the development and modification of the system	P75	Define the procedures for developing and modifying systems.	VMware has an industry-leading Security Development Lifecycle process and a VMware Cloud on AWS Security organization that focuses on ensuring that VMware Cloud on AWS implement industry standard operational and security controls. VMware identifies security defects using multiple methods which can include automated and manual source-code analysis. VMware Cloud on AWS releases go through a security architectural review, security audits, by both the product security teams and the cloud security teams, manual &	A12.1.2 Change Management

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				automated code analysis, vulnerability scans, and additional reviews necessary to meet industry leading security standards. VMware Security personnel approve releases to validate internal processes and mitigate software security risks to customers. The development of the VMware Security Development Lifecycle has been heavily influenced by industry best practices and organizations such as SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model). The VMware Product Security and product development groups apply the methodology as an end-to-end set of processes to use at specific times in the development group's software development lifecycle, with the goal of helping teams to remediate security issues early in the lifecycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	
		P76	Establish proper test environments.	The VMware Cloud on AWS team has a comprehensive testing system that covers the entire lifecycle of the release. Testing is conducted 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), FSLite (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 vulnerability scans and system tests at scale for every cycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	A12.1.2 Change Management
		P77	Define procedures for transition to production.	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. Customers are responsible for developing SDLC and change management processes over their content and environment.	A12.1.2 Change Management
	(2) Document management during development and modification	P78	Define the procedures for creating documents during development and modification.	VMware SDLC and change management processes guide personnel 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. Internal audits of these processes are performed under the VMware Information Security Management System (ISMS) program and are essential to the VMware continuous improvement programs. VMware uses various change management tools to document and record change management artifacts and approvals. Respective documentation is retained within these tools throughout the change management cycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	A12.1.2 Change Management
		P79	Define the procedures for storing and managing documents during development and modification.	VMware SDLC and change management processes guide personnel 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. Internal audits of these processes are performed under the VMware Information Security Management System (ISMS) program and are essential to the VMware continuous	A12.1.2 Change Management

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				improvement programs. VMware uses various change management tools to document and record change management artifacts and approvals. Respective documentation is retained within these tools throughout the change management cycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	
	(3) Package installation	P80	Establish a system for evaluating packages.	VMware has invested in the Security Development Lifecycle (SDLC) process which is continuously evolving in response to the threat landscape and a security organization that utilizes multiple key resources to ensure that VMware Cloud on AWS implements appropriate operational and security controls. The SDLC program is designed to identify and mitigate security risk during the development phase of VMware software products so that the development group's software is safe for release to customers. Code undergoes rigorous review for code security and quality. The VMware Product Security and product development groups apply the methodology as an end-to-end set of processes to use at specific times in the development group's software development lifecycle, with the goal of helping teams to remediate any security issues early in the lifecycle. As part of the SDLC, VMware uses both manual and automated source code analysis tools to detect security defects in code as well as security vulnerabilities in applications multiple times prior to production. Vulnerabilities posing a significant risk are addressed prior to deployment. VMware verifies that all software suppliers adhere to industry standards for SDLC security using its comprehensive vendor risk management process that includes review of our vendor's security controls, development processes, privacy controls, business conduct, and third-party audit reports and certifications.	A12.1.2 Change Management
		P81	Define the package application and management system.	VMware SDLC and change management processes guide personnel 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. Internal audits of these processes are performed under the VMware Information Security Management System (ISMS) program and are essential to the VMware continuous improvement programs. Additionally, the VMware Acceptable Use Policy prohibits the use of unauthorized software. Production servers are provisioned and managed programmatically via Infrastructure as Code software. No software can be installed on these systems manually or without several reviews and approvals. Additionally, continuous monitoring by VMware Cloud on AWS system monitoring tools is in place to detect unauthorized changes.	A12.1.2 Change Management
	(4) Disposal of systems	P82	Develop a system disposal plan and define the disposal procedure.	VMware cloud on AWS uses Amazon Data Centers infrastructure. AWS handles all physical equipment lifecycle. AWS uses techniques described in industry-accepted standards to ensure that data is erased when resources leave the service. When a storage device has reached its end of life, and to ensure that no residual data can be exposed, AWS follows the procedures detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"). This includes degaussing and physically destroying all magnetic storage devices.	A 8.3.2 Disposal of media
		P83	Take measures to prevent information leaks during system	See response at P82	See response at P82

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			disposal.		
Measures to improve system reliability	(1) Backup for hardware	P84	Provide a standby for a main unit.	VMware Cloud on AWS is running within Amazon datacenters in multiple locations world-wide. These locations are composed of Regions and Availability Zones. Each Region is a separate geographic area. Each Region has multiple, isolated locations known as Availability Zones. VMware Cloud on AWS has gained new levels of agility, scale and resiliency through a multi-availability zone deployed platform. Every region has at least 2 Availability Zones and most have 3 Availability Zones. https://aws.amazon.com/compliance/data-center/data-centers/	A12.3 Backup
		P85	Provide standbys for peripherals.	VMware Cloud on AWS uses Amazon data centers. All infrastructure components are managed by AWS. AWS manages the infrastructure demands and supports capacity for future demands for information processing, telecommunications and storage. For further information, see *https://aws.amazon.com/compliance/data-center/data-centers/*	A17. Information aspects of business continuity A12.1.3 – Capacity Management
		P86	Provide standbys for communication devices.	See response at P85	See response at P85
		P87	Provide backup lines.	See response at P85	See response at P85
		P88	Provide a standby for a terminal related device.	See response at P85	See response at P85
	(2) Measures to improve the quality of software	P89	Include necessary security functions.	VMware has invested in the Security Development Lifecycle (SDLC) process which is continuously evolving in response to the threat landscape and a security organization that utilizes multiple key resources to ensure that VMware Cloud on AWS implements appropriate operational and security controls. The SDLC program is designed to identify and mitigate security risk during the development phase of VMware software products so that the development group's software is safe for release to customers. Code undergoes rigorous review for code security and quality. The VMware Product Security and product development groups apply the methodology as an end-to-end set of processes to use at specific times in the development group's software development lifecycle, with the goal of helping teams to remediate any security issues early in the lifecycle. As part of the SDLC, VMware uses both manual and automated source code analysis tools to detect security defects in code as well as security vulnerabilities in applications multiple times prior to production. Vulnerabilities posing a significant risk are addressed prior to deployment Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P90	Ensure the quality of software in the design phase.	VMware security programs and practices establish requirements "by design" to evolve methodologies of protection against new "in-the-wild threats." This approach is followed throughout the development process. Products are tested by first-class vulnerability scans and penetration tests prior to any full release or version update. For further information, please visit: *VMware Product Security Whitepaper* Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P91	Ensure the quality of software in the programming phase.	VMware security programs and practices establish requirements "by design" to evolve methodologies of protection against new "in-the-wild threats." This approach is followed throughout the development process. Products are tested by first-class vulnerability scans and penetration tests prior to any full release or version update. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P92	Ensure the quality of software in the testing phase.	The VMware Cloud on AWS team has a comprehensive testing system that covers the entire lifecycle of the release. Testing is conducted 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), FSLite (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, vulnerability scans and System Tests at scale for every cycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P93	Ensure the reliability of software in consideration of program distribution.	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. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P94	Ensure the quality of package software when installed.	VMware Cloud on AWS has a controlled trusted code build and deployment process using immutable artifacts. VMware Cloud on AWS has integrated validations that include container signing, certificates, and auth token credential processes into the software supply chain to maintain a secure continuous delivery pipeline. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P95	Ensure the correctness of routine modification operations.	VMware has in place well-defined operational security policies, standards, practices, and other guidance with which all teams within VMware must comply. These include policies and standards for configuration management and testing, as well as vulnerability detection, assessment, management, and mitigation. The scope of these standards applies and extends to all information systems and applications owned, managed, and/or operated by VMware in both VMware and third-party datacenters and cloud environments, as well as to all business processes associated with the operation of these information systems and applications, and to all VMware employees, consultants, contractors, agents, and vendors who manage or operate VMware information systems and applications and/or business processes. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P96	Ensure that the quality of software is maintained even after changing or adding any functions.	VMware has invested in the Security Development Lifecycle (SDLC) process which is continuously evolving in response to the threat landscape and a security organization that utilizes multiple key resources to ensure that VMware Cloud on AWS implements appropriate operational and security controls. The SDLC program is designed to identify and mitigate security risk during the development phase of VMware software products so that the development group's software is safe for release to customers. Code undergoes rigorous review for code security and quality. The VMware Product Security and product development groups apply the methodology as an end-to-end set of processes to use at specific times in the development group's software development lifecycle, with the goal of helping teams to remediate any security issues early in the lifecycle. Customers are responsible for developing SDLC and change management processes over their content and environment.	A14.2 Security in development and support processes A 14. System acquisition, development and maintenance
		P97	Provide proper exclusive access control functions to files.	VMware has security controls in place to reduce the risk of unauthorized access to sensitive information in the production environment. File integrity of the VMware Cloud on AWS console application is enforced via the container management system and the file integrity of the tenant environment is enforced by the VMware Fleet Management System. Customers are responsible for developing SDLC and change management processes over their content and environment.	A9 Access Control
		P98	Provide the functions of matching files.	VMware has security controls in place to reduce the risk of unauthorized access to sensitive information in the production environment. File integrity of the VMware Cloud on AWS console application is enforced via the container management system and the file integrity of the tenant environment is enforced by the VMware Fleet Management System. Customers are responsible for developing SDLC and change management processes over their content and environment.	A9 Access Control
	(3) Measures to improve operational reliability	P99	Automate and simplify operations.	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. For details on these unique capabilities, please see the VMware Cloud on AWS service description https://www.vmware.com/download/eula/vmware-cloud-on-aws.html Customers have additional options to add additional availability zones and redundancy to their environments to further reduce risk. Customers are responsible for implementing automation over their applications and systems supporting the operational processes.	A17. Information security aspects of business continuity management
		P100	Reinforce the functions of checking operations.	VMware Cloud on AWS offers the optional an add-on for vSphere Site Recovery Manager (SRM) to automatically restart a workload from any failure in a specific host on another host in the cluster. Site Recovery Manager provides an end-to-end disaster recovery solution that can	A17. Information security aspects of business continuity management

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. In the event of a host failure, a new host can be provisioned to a cluster within minutes in order to restore full capacity. The VMware Site Recovery offering provides native hypervisor-based replication using VMware vSphere Replication of workloads between vSphere instances in different regions or customer datacenters. Customers are responsible for implementing automation and checking operations over their applications and systems.	
		P101	Reinforce the functions of monitoring and controlling loaded conditions.	The VMware Cloud on AWS interface provides customer with information about capacity utilization in order to enable them to do capacity planning. Metrics data including resource utilization metrics are exposed via APIs to feed into a customer's preferred capacity planning solution. VMware Cloud on AWS also enables customer 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. VMware Cloud on AWS continuously monitors consumption rates to ensure sufficient capacity for customers in each data center.	A17. Information security aspects of business continuity management
	(4) Functions for early failure detection and recovery	P102	Provide the function of monitoring the operational conditions of a system.	VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify all dependencies, critical products, and services. The near real-time status of the VMware Cloud on AWS along with past incidents is publicly available at *https://status.vmware-services.io/*	A17. Information security aspects of business continuity management
		P103	Provide functions to detect any failures and isolate the points of failure.	VMware Cloud on AWS services are built with a requirement for each service to be deployed in 3 separate Availability Zones for redundancy. Service redundancy includes both stateless components as well as data components. This model covers majority of the availability events on record since each Availability Zone is a separate AWS data center with redundant power and network providers. Service Availability Zone failovers are handled transparently as VMware Cloud on AWS services are built with assumption of that Availability Zone failovers are a relatively frequent events. Customers have the ability to architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. Customers retain control and ownership of their Customer Content and have the ability utilize their own backup and recovery mechanisms including establishing a redundant cloud infrastructure in their own data centers and/or using any one of thousands of VMware partners that run vSphere. Some of these BC/DR options, like VMware Site Recovery Manager can automate recovery processes to reduce changes required to manage customer workloads.	A17. Information security aspects of business continuity management
		P104	Provide the functions for reduction or shutdown and rearrangement of business operations in the event of failure.	VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as in multiple geographic regions. Each Availability Zone is designed as an independent failure zone. In case of failure, customers can configure automated processes to move customer data traffic away from the affected area. VMware Cloud on AWS offers the optional an add-on for vSphere Site Recovery Manager (SRM) to automatically restart a workload from any failure in a specific host on another host in the cluster. Site Recovery Manager	A17. Information security aspects of business continuity management

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
				provides an end-to-end disaster recovery solution that can help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. In the event of a host failure, a new host can be provisioned to a cluster within minutes in order to restore full capacity. The VMware Site Recovery offering provides native hypervisor-based replication using VMware vSphere Replication of workloads between vSphere instances in different regions or customer datacenters. Customers are able to implement additional redundancy via data protection, in-guest replication using third party solutions and/or manual synchronization via import/export/migration tools.	
		P105	Provide functions to limit transactions in the event of failure.	VMware Cloud on AWS gives customers full control over their virtual machines and their content. Customers are responsible for implementing features to restrict transactions over their environment.	A17. Information security aspects of business continuity management
		P106	Provide recovery functions in the event of failure.	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. For details on these unique capabilities, please see the VMware Cloud on AWS service description https://www.vmware.com/download/eula/vmware-cloud-on-aws.html Customers have additional options to add additional availability zones and redundancy to their environments to further reduce risk.	A17. Information security aspects of business continuity management
Individual operations and services	(1) Card transaction service	P107	Establish a method for managing cards.	N/A – Customers are responsible for managing access to their content and implementing controls over card transaction.	N/A
		P108	Alert customers to crimes concerning card transactions, etc.	N/A – Customers are responsible for managing access to their content and implementing controls over card transaction.	N/A
		P109	Ensure the financial transactions by duly authorized customers in the cash transactions through CD/ATM, and other automated machines.	N/A – Customers are responsible for managing access to their content and implementing controls over card transaction.	N/A
		P110	Define the procedures for monitoring transactions by using card in any designated accounts.	N/A – Customers are responsible for managing access to their content and implementing controls over card transaction.	N/A

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P111	Implement technical precautions against counterfeit card.	N/A – Customers are responsible for managing access to their content and implementing controls over card transaction.	N/A
	(2) Internet and mobile services	P112	Prevent illegal use of the Internet and mobile services.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
		P113	Ensure that the user can check the usage status of the Internet and mobile services.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
		P114	Disclose information on security measures for the Internet and mobile services.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
		P115	Make clear the policy for the Internet and mobile services toward customers.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
		P116	Define the operation management method for the Internet and mobile services.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
		P117	Verify the identity of an applicant when he/she opens an account in the Internet and mobile services.	N/A – Customers are responsible for managing access to their content and implementing controls over internet and mobile services.	N/A
	(3) Management of handheld terminals	P118	Establish and maintain proper procedures for operating and managing handheld terminals.	N/A – Customers are responsible for managing access to their content and implementing controls over management of handheld terminals.	N/A
	(4) Management of CD/ATM and unmanned branch	P119	Clarify the operation management method for CD/ATM and unmanned branches and take measures against illegal withdrawal.	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A
		P120	Establish and maintain proper monitoring	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
			systems for unmanned branches.		
		P121	Establish and maintain proper crime prevention systems for unmanned branches.	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A
		P122	Establish and maintain proper preparedness for any failure or disaster in unmanned branches.	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A
		P123	Document and maintain required manuals for unmanned branches.	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A
		P124	Provide CD/ATM with a remote control function.	N/A – Customers are responsible for managing access to their content and implementing controls over management of CD/ATM and unmanned branches.	N/A
	(5) In-store branches	P125	Define guidelines for selecting the locations of in-store branches.	N/A – Customers are responsible for managing access to their content and implementing controls over management instore branches.	N/A
	(6) Convenience store ATMs	P126	Define guidelines for selecting stores for convenience store ATMs.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A
		P127	Take crime-prevention measures associated with cash loading and other maintenance in convenience store ATMs.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A
		P128	Define measures to be taken in response to a failure in a convenience store ATM or a disaster.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A
		P129	Security measures for network-related devices and data transmissions should be implemented in convenience store ATMs.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
		P130	Establish a liaison system with police and security companies in charge of convenience store ATMs.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A
		P131	Raise convenience store ATM customers' awareness about crimes.	N/A – Customers are responsible for managing access to their content and implementing controls over management of convenience store ATMs	N/A
	(7) Debit card services	P132	Security measures should be taken for debit card services.	N/A – Customers are responsible for managing access to their content and implementing controls over management of debit card services.	N/A
		P133	Ensure the security of account numbers, personal identification numbers, etc. of debit cards.	N/A – Customers are responsible for managing access to their content and implementing controls over management of debit card services.	N/A
		P134	Measures should be taken to protect customers when they use debit cards.	N/A – Customers are responsible for managing access to their content and implementing controls over management of debit card services.	N/A
		P135	Steps should be taken to make customers exercise caution on certain points regarding the use of debit cards.	N/A – Customers are responsible for managing access to their content and implementing controls over management of debit card services.	N/A
	(8) Prepaid payment method	P136	State the loss that a user may suffer, and his or her responsibility in conjunction with the theft or damage of equipment or a medium in prepaid payment.	N/A – Customers are responsible for managing access to their content and implementing controls over management of prepaid payment methods.	N/A
		P137	Set up a function to protect electronic value or a mechanism for detecting fraud in prepaid payment methods.	N/A – Customers are responsible for managing access to their content and implementing controls over management of prepaid payment methods.	N/A
		P138	Define email operations policy.	N/A – Customers are responsible for managing access to their content and implementing controls over management of use of emails and internet.	N/A

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
	(9) Use of e-mails and intranet	P139	It is recommended that measures be taken to prevent unauthorized sending/receiving e-mail, or browsing websites, etc., for other than business purposes.	N/A – Customers are responsible for managing access to their content and implementing controls over management of use of emails and internet.	N/A
	(10) Biometric authentication	P140	Implement the security control measures for biometric information handled in the process of biometric authentication.	N/A – Customers are responsible for managing access to their content and implementing controls over management of biometrics.	N/A
		P141	Examine required security measures for biometric authentication in consideration of the characteristics of biometrics.	N/A – Customers are responsible for managing access to their content and implementing controls over management of biometrics.	N/A
	(11) QR code payment	P142	Security measures should be taken for QR code payment.	N/A – Customers are responsible for managing access to their content and implementing controls over management of QR code payments.	N/A
		P143	Measures should be taken to protect customers when they use QR code payment.	N/A – Customers are responsible for managing access to their content and implementing controls over management of QR code payments.	N/A
		P144	Steps should be taken to make customers aware of considerations regarding the use of QR code payment.	N/A – Customers are responsible for managing access to their content and implementing controls over management of QR code payments.	N/A

FISC - Security Guidelines

FISC has published facilities guidelines for management of physical infrastructure and data facilities (***Guidelines F1 to F137 in the FISC Security Guidelines on Computer Systems for Financial Institutions***). It is important to note that VMware Cloud on AWS uses Amazon Web Services (AWS) data centers.

Physical Access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, two-factor authentication to access data center floors and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. Regular maintenance and testing is conducted for both the UPS and generators and data centers have contracts for emergency fuel delivery. Facilities personnel monitors all critical electrical systems and components 24x7x365. AWS' physical protection against environmental risks has been validated by independent auditor and has been certified as being in alignment with ISO requirements.

AWS keeps their data center locations strictly confidential to maintain the security and privacy of customer data. Locations are disclosed only to AWS employees and contractors who have an approved business need to be at the facility. Customers can assess the security and resiliency of the AWS physical infrastructure by considering all of the security controls that AWS has in place for its data centers. To support customers evaluating risks related to AWS data centers, AWS provides the AWS Data Center Controls web page and the AWS SOC 2 report available in AWS Artifact. https://aws.amazon.com/compliance/faq/

For more information please see

- *https://aws.amazon.com/security*
- *https://aws.amazon.com/compliance/data-center/controls/*
- *FISC - Amazon Web Services (AWS)*

FISC – Audit Guidelines

Guideline Category	Guideline Sub-category	Guideline Number	Guidelines Unit	VMware Response	ISO 27001 reference
System Auditing	(1) System auditing	A1	Establish system auditing structures.	VMware has a compliance program in place that is designed after several industry standards and frameworks including ISO27001, SOC2, and PCI-DSS. VMware regularly conducts internal and external audits that include results from security and compliance assessments. The program utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also to identify areas of improvement. Security is of the utmost importance to us. Our programs are continually evolving based on our own experiences, changes in the threat landscape, and our learnings based on industry observation and collaboration. For more information about VMware Security programs: *https://www.vmware.com/security.html* For a list of existing compliance certifications, please visit *VMware Cloud Trust Center*	A18. Compliance

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