Germany Cloud Computing Compliance Criteria Catalogue (C5) Whitepaper

VMware Cloud on AWS

vmware®

Executive Summary

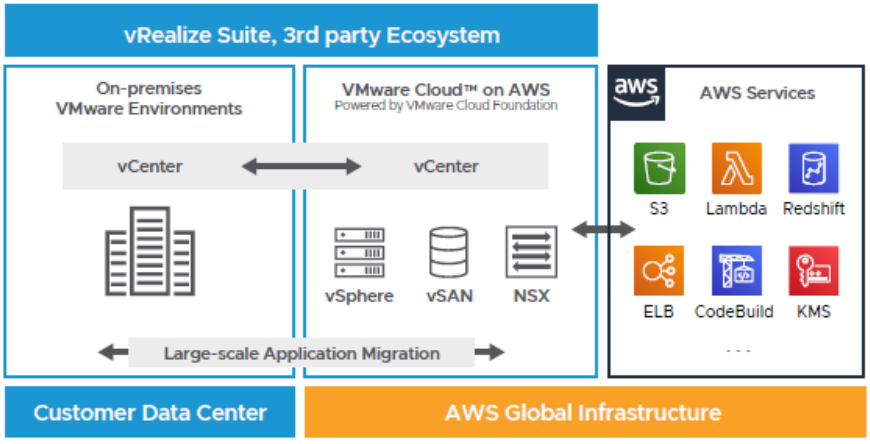
The Cloud Computing Compliance Controls Catalogue (C5) is a cloud security certification prescribed by the German Federal Office of Information Security (BSI). The certification describes the security controls and processes implemented by cloud service providers to secure customer workloads and the infrastructure supporting the cloud platform. The control requirements in C5 are based on some of the leading international standards such as ISO27001/17/18, SOC2, Cloud Security Alliance ANSSI Référentiel Secure Cloud 2.0, IDW and BSI IT-Grundschutz Catalogues.

VMware Cloud on AWS has achieved a number of globally recognized compliance certifications such as ISO 27001, ISO 27017, ISO 27018, SOC2, PCI-DSS, Cloud Security Alliance – Level 1 and Cyber Essentials Plus. While VMware Cloud on AWS is yet to undergo the certification for C5, in this whitepaper intend to show the controls and processes VMware Cloud on AWS has in place to address the control requirements in C5 certification.

To complement this whitepaper, customers can also utilize the mapping document published by BSI which shows how C5 standard maps to various international compliance certifications. The mapping document is available at *Referencing Cloud Computing Compliance Criteria Catalogue (C5) to International Standards*.

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 them 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.



Structure of C5 Framework

The below table shows the key control areas and objectives prescribed in the C5 framework:

No.	Area	Objective
1	Organisation of Information Security (OIS)	Plan, implement, maintain and continuously improve the information security framework within the organization.
2	Security Policies and Instructions (SP)	Provide policies and instructions regarding security requirements and to support business requirements.
3	Personnel (HR)	Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.
4	Asset Management (AM)	Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.
5	Physical Security (PS)	Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.
6	Operations (OPS)	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.
7	Identity and Access Management (IDM)	Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.
8	Cryptography and Key Management (CRY)	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.
9	Communication Security (COS)	Ensure the protection of information in networks and the corresponding information processing systems.
10	Portability and Interoperability (PI)	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.
11	Procurement, Development and Modification of Information Systems (DEV)	Ensure information security in the development cycle of cloud service system components.
12	Control and Monitoring of Service Providers and Suppliers (SSO)	Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.
13	Security Incident Management (SIM)	Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.

14	Business Continuity Management (BCM)	Plan, implement, maintain and test procedures and measures for business continuity and emergency management.
15	Compliance (COM)	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.
16	Dealing with investigation requests from government agencies (INQ)	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.
17	Product Safety and Security (PSS)	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.

VMware response to C5 requirements

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
1	Organisation of Information Security (OIS)	Plan, implement, maintain and continuously improve the information security framework within the organization.	VMware Cloud on AWS has established an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. Internal and external audits are performed annually under the VMware information security management system (ISMS) program and VMware has been audited by external auditors for the ISO 27001 certification. VMware has established information security policies in line with 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 operates a shared responsibility model for delivery of services. The shared responsibility model that outlines the responsibilities of VMware, AWS and the customer. For information see *Shared Responsibility Model Whitepaper* VMware has considered significant interactions between itself and relevant external parties and risks that could affect the company's ability to provide reliable service to its user entities. Risks identified during the risk assessment process are ranked and formally documented along with mitigation strategies. A formal process is documented to guide personnel when performing a risk assessment. VMware maintains an ISMS framework to manage information security risks. VMware performs annual risk assessments as part of the VMware ISMS program to support security and compliance programs. The framework security requirements have been designed and implemented to address industry standards around security and privacy. This requires the identification of applicable regulatory and contractual requirements, technical compliance with information security policies, protection of records, protection of information systems audit tools, and audit controls and reporting. This policy also requires VMware to adhere to the applicable legal, statutory, regulatory, or contractual obligations related to information security and security requirements. VMware has a dedicated Security, Governance, Risk and Compliance team that oversees risk management and compliance across the organization. Where needed, the team liaises with relevant regulatory authority to address specific regulatory concerns.	A.6.1 Internal Organisation
2	Security Policies and Instructions (SP)	Provide policies and instructions regarding security requirements and to support business requirements.	VMware has documented policies, standards and system and network diagrams supporting VMware Cloud on AWS. VMware documents, updates, and maintains baseline configurations for software and hardware installed in the production environment; changes are governed by a defined change management policy and baseline configurations are securely managed.. Security baselines are documented to guide personnel to ensure appropriate configurations are in place to protect sensitive information. VMware utilizes various internal tools for communication of VMware policies. These policies are published on intranet, version controlled, reviewed, and updated on an annual basis.	A.5 Information security policies
3	Personnel (HR)	Ensure that employees understand	VMware has organizational charts in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and	A.7 Human resource security

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
		their responsibilities, are aware of their responsibilities regarding information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.	monitoring of the system. These charts are communicated to employees via the company intranet and updated as needed. VMware has established screening procedures, where allowed by local laws VMware performs background checks for new hires. The results are evaluated to determine employment eligibility. New hires are required to attend orientation meetings to review corporate security policies and obligations. In alignment with the ISO 27001 standard, VMware personnel are required to complete annual security awareness training. Personnel supporting VMware managed services receive additional role-based security training to perform their job functions in a secure manner. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Formal procedures are in place for access granting and revocation for starters and leavers, these are validated by external auditors as part of compliance audits. VMware has also documented terms and conditions for maintaining confidentiality as part of the VMware Cloud on AWS Terms of Service.	
4	Asset Management (AM)	Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.	VMware has an established Asset Management policy that dictates management of assets at VMware including creation, processing, storage, transmission, deletion, and destruction. VMware maintains inventories of critical assets including asset ownership and location. VMware also maintains an acceptable use policy that dictates employee responsibility towards protecting and managing company's assets. VMware Corporate Human Resources has an established policy for employee termination processes and provides procedures for management to ensure that company owned assets are returned within the specified timeframe. Controls over asset management processes are audited by external auditors as part of the ISO 27001 audits. It is important to note that VMware Cloud on AWS utilizes AWS data centers to support backend infrastructure. Media storage devices used to store customer data are classified by AWS as critical and treated accordingly, as high impact, throughout their lifecycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.	A.8 Asset Management
5	Physical Security (PS)	Prevent unauthorized physical access and protect against theft, damage, loss	VMware Cloud on AWS uses AWS datacenters. AWS security management standards follow the industry standards such as the ISO/IEC 27001:2013. AWS manages physical access to datacenters as defined in the AWS Data Center Physical Security Policy. Physical access is strictly controlled both at the perimeter and at building ingress/egress points and includes, but is not limited to fencing, walls, video surveillance, intrusion detection systems, and other electronic biometric access	A.11 Physical and environmental security

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
		and outage of operations.	controls and alarm monitoring systems managed by a 24x7x365 professional security staff. For more information on AWS controls, please visit: *https://cloudsecurityalliance.org/star/registry/amazon/* *https://aws.amazon.com/compliance/data-center/data-centers/* AWS performs regular audits of their physical infrastructure. For more information on AWS data center security controls and compliance reports, please visit *https://aws.amazon.com/compliance/* AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS 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. Critical system components are backed up across multiple, isolated locations known as 'availability zones'. Each availability zone is engineered to operate independently with high reliability. Availability zones are connected to enable you to easily architect applications that automatically fail-over between availability zones without interruption. Highly resilient systems, and therefore service availability is a function of the system design. Through the use of availability zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. AWS monitors and performs preventive maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. Preventive maintenance is performed to maintain the continued operability of equipment.	
6	Operations (OPS)	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities,	VMware has a defined Information Security Program that includes Business Continuity and Disaster Recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. This program implements appropriate security controls to protect its employees and assets against natural and manmade disasters. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and made available to appropriate individuals. VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify dependencies, critical products, and services. The real-time status of the VMware Cloud on AWS along with past incidents is publicly available at *https://status.vmware-services.io/* . Customers have the ability to architect their VMware Cloud on AWS implementations in various ways to reduce impact of an availability zone or regional disaster using VMware products. For example, an SDDC may be deployed as a "stretched cluster" that provisions hosts in 2 distinct availability zones. Customers retain control and ownership of their customer content and have the ability utilize their own backup and recovery mechanisms. VMware Cloud on AWS SDDC also have an optional (paid) disaster recovery feature	A.12 Operations Security

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
		malfunctions and failures.	called Site Recovery Manager and VMware Cloud Disaster Recovery that greatly simplifies disaster recovery management and operations. VMware Cloud on AWS backs up account information including system configuration settings but does not provide data backup services for customer content. Customer content will not be relocated, replicated, archived, or copied without the explicit actions by the customer administrator. VMware provides each customer a secured and isolated configuration by default which can be customized via self-service tools, as required by the customer administrators, to optionally enable customer content transport outside of the dedicated customer SDDCs to any other AWS facilities, customer dedicated private networks or public internet VMware patches or upgrades platform systems and applications after analysing the severity and impact of potential vulnerabilities. VMware has subscriptions to pertinent vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical and high vulnerability patches are installed in a timely manner. Non-critical patches are included in the pre-defined patch schedule and applied within commercially reasonable timeframes. Patch testing and rollback procedures are completed by the QA department to ensure compatibility with and minimal impact to the production environment. VMware continuously collects and monitors services operation logs using SIEM technologies. The 24x7x365 VMware Security Operations Center uses the SIEM to correlate information with public and private threat feeds to identify suspicious and unusual activities. The VMware Security Operations Center (SOC) team takes reported security events and escalates to the VMware Security Incident Response Team (vSIRT) for security incident management as appropriate based on defined criteria.	
7	Identity and Access Management (IDM)	Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.	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. Access privileges to VMware systems are controlled based on the principle of least privilege – only the minimum level of access required shall be granted. Access is based on an individual's "need to know" as determined by job functions and requirements. Access privileges to computers and information systems is authorized by the appropriate level of management and documented within the ticket lifecycle, and such access is monitored (in use) and revoked when no longer required. Managing access to information systems is implemented and controlled through centralized identity stores and directory services. A periodic review is performed to ensure service access is still appropriate. Controls are in place ensuring timely removal of systems access that is no longer required for business purposes. Entitlement actions are recorded via the systems used to grant/revoke access and provide evidence to support compliance programs. Remediation actions related to access violations will follow user access policies and standard procedures. To support troubleshooting on VMware Cloud on AWS platform, a "Delegated Access" process is in place that enables only VMware engineers with the appropriate permissions to authenticate (using MFA) to a system to generate one-time use certificates and credentials that are user-specific with limited time-	A.5 Information security policies A.9 Access Control

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
			bound access to troubleshoot and remediate issues on the physical hosts, hypervisors, and service management appliances. Access must be tied to a support ticket and access is logged & monitored and any suspicious activity is investigated by VMware's Security Operations Center (SOC).	
8	Cryptography and Key Management (CRY)	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.	VMware has an encryption policy that provides guidelines on use of cryptographic controls and key management. The policy is reviewed on an annual basis. VMware Cloud on AWS leverages encryption to protect data during transport across and between networks and hypervisor instances. For VMware Cloud on AWS offerings that enable transport from on-premises environments to the VMware Cloud on AWS environment, information is sent over a VPN connection. One of these offerings is VMware HCX, which facilitates the bulk migration of data. This service uses AES-256 encryption to encapsulate in-transit workloads. vSphere features including VMware vSphere vMotion, VMware vSphere Distributed Resource Scheduler (DRS), VMware vSphere High Availability (HA), and VMware vSphere Replication are supported with vSAN Encryption. For in-cloud VMware HCX vMotion activities, a dedicated, secure and encrypted network is used. VMware vSAN provides storage array level encryption in addition to the existing VMware Cloud on AWS physical disk encryption found on NVMe self-encrypting drives. Encryption is implemented using XTS AES 256 cipher with Intel AES-NI. As part of the shared responsibility model, customers are responsible for securing their sensitive data with in-guest encryption and application encryption software using options for alternative key management systems to enable full control of the key management lifecycle.	A.5 Information Security Policies A.10 Cryptography
9	Communication Security (COS)	Ensure the protection of information in networks and the corresponding information processing systems.	VMware Cloud on AWS have logically separated networks that restrict the customer's access to their own private networks. The services' system and network environments are protected by a firewall or virtual firewall to ensure business and customer security requirements, as well as to ensure protection and isolation of sensitive data. Firewalls act as critical components of the VMware network and information security architecture and are used to restrict and control network traffic and access to systems, data, and applications. 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 customer datacenter, office, or colocation environment. Encrypted vMotion is available at VMware Cloud on AWS between hosts inside the Cloud SDDC. To maintain ongoing VMware Cloud on AWS compliance programs, audits are performed at least annually that include network penetration testing. The results from evidence compiled by 3rd party assessors are published in	A.13 Communications security

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
			customer available SOC 2 and ISO 27001 compliance reports. The purpose of these reports is to help customers and their auditors understand the controls and evidence gathered by 3rd party assessors evaluating support operations, security and compliance programs.	
10	Portability and Interoperability (PI)	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.	VMware Cloud on AWS has three independent and comprehensive isolation layers in place to segregate customers' environments: A Software Defined Data Center (SDDC) is deployed in a dedicated AWS Virtual Private Cloud (VPC) that is owned by an AWS account created exclusively for each customer. Amazon accounts and Amazon VPCs are the mechanisms implemented by AWS to logically isolate sections of the AWS Cloud for each customer. Each SDDC is deployed on dedicated bare metal hardware - providing physical isolation between customers' environments. Dedicated hardware means that customers do not share the physical processor, memory or storage with anyone else. VMware vSphere is deployed in each SDDC which allows customers to logically isolate their Content by creating Resource Pools and configuring vSphere permissions to control who has access to content within their own organization Customers are responsible for backing up content and migrating all workloads to their target environment, and deleting their SDDCs, prior to termination of their Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service). Customers can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration. For further information, contact a VMware sales specialist. Termination of service offering instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations pursuant to VMware practices. For further details see *VMware Cloud on AWS. Service Description* and *Terms of Service*	A12.3 Backup A 8.3 Media handling
11	Procurement, Development and Modification of Information Systems (DEV)	Ensure information security in the development cycle of cloud service system components.	VMware has a security development lifecycle process and a VMware Cloud on AWS Security organization that focuses on ensuring that VMware Cloud on AWS implements robust 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 & 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 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.	A12.1.2 Change Management A.14 System acquisition, development and maintenance

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
			VMware security development lifecycle 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.	
12	Control and Monitoring of Service Providers and Suppliers (SSO)	Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.	VMware has an established Third-Party IT Risk Management policy. The policy applies to VMware's management and oversight of third parties (vendor /supplier) accessing or processing company data facilities, information, and/or information systems. It defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. Sourcing and business teams collaborate with the information security risk team to ensure a risk-based approach is taken with respect to third parties to ensure the security of information assets. VMware also maintains a list of third-party vendors and 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. 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 Supplier relationships
13	Security Incident Management (SIM)	Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.	VMware has a documented security incident management policy which is reviewed every 12 months. VMware has incident response program, plans, and procedures which are documented and implemented. VMware maintains an incident response plan, which includes evidence preservation and customer notification processes. VMware provides incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to availability of the service offering. Customers are responsible for incident and problem management (e.g., detection, severity, classification, recording, escalation, and return to service) pertaining to all virtual machines that they have deployed in customer SDDC. The VMware Security Operations Center (SOC) uses log capture and SIEM tools, security monitoring technologies and intrusion detection tools in real-time to identify unauthorized access attempts, any behaviors that would indicate abnormal activity or by any VMware personal accessing customer data.	A.16 Information Security Incident Management

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
			The vSIRT team is notified by the Security Operations Center of any potential breach and participates in any investigation. If VMware becomes aware of a security incident on VMware Cloud on AWS that leads to the unauthorized disclosure or access to personal information provided to VMware as a processor, we will notify customers without undue delay, and will provide information relating to a data breach as reasonably requested by our customers. VMware will use reasonable endeavors to assist customers in mitigating, where possible, the adverse effects of any personal data breach.	
14	Business Continuity Management (BCM)	Plan, implement, maintain and test procedures and measures for business continuity and emergency management.	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. VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training. VMware follows 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. VMware is adequately prepared 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 stakeholders, thus 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. The VMware business continuity plans and documentation are reviewed annually as part of the enterprise independent attestation in 3rd party compliance audits, including ISO 27001 and SOC 2. VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify dependencies, critical products, and services. The real-time status of the VMware Cloud on AWS along with past incidents is publicly available at *https://status.vmware-services.io/* . VMware Cloud on AWS 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	A17 Information security aspects of business continuity management

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
			their workloads in multiple regions are effectively operating across multiple providers. Customers also have the ability to architect their VMC implementations in various ways to reduce impact of an availability zone or regional disaster by implementing stretched clusters, or Add-on solutions like Site Recovery Manager (DRaaS). 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 VMware partners that run vSphere.	
15	Compliance (COM)	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.	VMware has a compliance program in place that is designed after several industry standards and frameworks including ISO27001 and SOC2. 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 visit: *https://www.vmware.com/security.html*	A.18 Compliance
16	Dealing with investigation requests from government agencies (INQ)	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.	VMware handles government requests in line with the Section 1.9 ("Required Disclosures") of the Terms of Service. For further details see *vmware-cloud-services-universal-tos.pdf*.	A.18 Compliance
17	Product Safety and Security (PSS)	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers,	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, manual & automated code analysis, vulnerability scans, and additional reviews necessary to meet industry leading security standards. VMware security personnel approve	A.14.2 Security in development and support processes

No.	Area (Identifier)	Objective	VMware Response	Applicable ISO 27001 reference
		appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.	releases to validate internal processes and mitigate software security risks to customers. 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. 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 for vulnerabilities prior to full release or version update. For further information, please visit: *VMware Product Security Whitepaper*	

Conclusion

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

VMware Cloud on AWS has undergone independent third-party audits on a regular basis to provide assurance to our customers that VMware has implemented 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.

VMware Cloud on AWS helps to meet their security and privacy compliance obligations with an enterprise ready SDDC that leverages both on-premises and cloud resources for rapid application portability and operational consistency across the environment.

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