VMware vCloud Air IaaS CAIQ SEPT 2016 - CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle	The VMware Security Development Lifecycle (SDL) team helps guide product teams to identify and correct security issues during the development lifecycle.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	As a part of the VMware Security Development Lifecycle, VMware identifies security defects using multiple methods which can include automated and manual source-code analysis.
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	As a part of the VMware Security Development Lifecycle, VMware identifies security defects using multiple methods which can include automated and manual source-code analysis.
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	N/A - vCloud Air does not utilize third party software suppliers.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	N/A for vCloud Air IaaS
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Yes. Prior to granting access to the vCloud Air service, Customers are required to review and agree to a Terms of Service. The vCloud Air Terms of Service are made publicly available to prospects and customers at: http://vcloud.vmware.com/legal
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	Yes. The vCloud Air User's Guide contains detailed information pertaining to the setup and administration of account users including specialized privileges based on user role. The vCloud Air User's Guide is made publicly available to prospects and customers at: http://pubs.vmware.com/vca/index.jsp#com.vmware.ICbase/Welcome/welcome.html
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	The VMware Security Development Lifecycle (SDL) team helps guide product teams to identify and correct security issues during the development lifecycle based on the assessment of risks.
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	The International Organization for Standardization (ISO) has developed the ISO 27001 standard which defines an information security management system ("ISMS") as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization's people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's Air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. For more information concerning vCloud Air's ISO 27001 certificate and other security and compliance information, please visit: http://vcloud.vmware.com/service-offering/cloud-compliance
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	vCloud Air has a robust compliance program using ISO 27001 as our framework. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud Air controls against multiple industry standards which include ISO 27001, SOC 1, SOC 2, HIPAA. vCloud Air utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also identify areas of improvement. Audits are essential to vCloud Air's continuous improvement program. For more information concerning vCloud Air's ISO 27001 certificate and other security and compliance information, please visit: http://vcloud.vmware.com/service-offering/cloud-compliance

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes. vCloud Air engages independent third party auditors to perform reviews against industry standards. For more information concerning vCloud Air's available compliance reports and other security and compliance information, please visit: http://vcloud.vmware.com/service-offering/cloud-compliance
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes. vCloud Air has a comprehensive vulnerability management program. As a part of the vulnerability management program, network penetration tests are performed at least annually. Results are reviewed by the VMware security team(s) and remediation is performed based on the security team's guidance.
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes. vCloud Air has a comprehensive vulnerability management program. As a part of the vulnerability management program, application penetration tests are performed at least annually. Results are reviewed by the VMware security team(s) and remediation is performed based on the security team's guidance.
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes. Internal audits are performed at least annually under the guidance of our ISO 27001 ISMS program. vCloud Air utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also identify areas of improvement. Audits are essential to vCloud Air's continuous improvement program. Annual external audits are performed for the majority of our compliance programs (such as HIPAA, SOC 1, SOC 2, ISO, etc.)
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes. External audits are performed at least annually. vCloud Air utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also identify areas of improvement. Audits are essential to the vCloud Air continuous improvement program. Annual external audits are performed for the majority of our compliance programs (such as HIPAA, SOC 1, SOC 2, ISO, etc.)
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	vCloud Air is subject to regular internal and external reviews and security assessments. As a part of the vCloud Air vulnerability management program, vCloud Air engages third party independent auditors to review the results of the penetration tests.
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	External audit reports are provided to tenants under NDA. Internal audit reports are classified as VMware confidential and are not provided to tenants. Internal audit reports are reviewed by independent third party auditors as a part of vCloud Air's annual ISO 27001 review.
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	VMware has an internal audit program which reviews the vCloud Air controls on an annual basis to identify nonconformities and opportunities for improvement.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes. Core separation is via the underlying vSphere technology, an assured component. vCloud Air has three primary service offerings: Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery. The Dedicated Cloud is a single-tenant, physically isolated platform. Customers get their own physical servers and a dedicated management stack, isolated from other tenants. Virtual Private Cloud and Disaster Recovery are based on a multi-tenant platform. Each customer is logically isolated from others through vSphere and vCloud Director software, limiting each customer's access to only
		AAC-03.2		Do you have capability to recover data for a specific customer in the case of a failure or data loss?	Yes. The customer must be subscribed to our Data Protection Service and the data backed up prior to the failure or data loss.
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes. Customers choose the physical data center where they want their data deployed. Data is not moved away from that physical data center unless data migration is performed by the customer or the customer purchases an offline data transfer offering.
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes. VMware monitors changes to regulatory requirements and notifies vCloud Air of these changes. Adjustments to the vCloud Air Information Security Management System are made as necessary to ensure compliance.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them	Do you provide tenants with geographically resilient hosting options?	Yes. Customers explicitly choose which vCloud Air location best suits their needs, and customer data does not traverse locations without the explicit actions of the tenant administrator. A customer must subscribe to services within multiple locations, and initiate transport/migration operations using on-premises tools such as vCloud Connector. VMware delivers vCloud Air services through locations listed at the following public URL: http://vcloud.vmware.com/explore-vcloud-air/vcloud-air-location
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?	Yes. The vCloud Air Disaster Recovery service offering allows customers to replicate virtual machines and failover into vCloud Air from non-vCloud Air data centers.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes. Business continuity plan exercises are scheduled annually as a part of the VMware Business continuity programs. Business continuity exercises are reviewed as a part of the independent third party audits for vCloud Air (ISO 27001, SOC2).
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	A high-level architecture diagram detailing the layers of interconnected networks for tenants and for the provider is provided during the onboarding process.
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?	Yes. Customers explicitly choose which vCloud Air location best suits their needs, and customer data does not traverse locations without the explicit actions of the tenant administrator. To transport data between vCloud Air locations, a customer must subscribe to services within multiple locations and initiate transport/migration operations using available tools.
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes. Information system documentation is made available to authorized personnel to ensure configuration, installation and operation of the information system. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Yes. VMware performs an assessment on each data center selected to ensure each site has appropriate countermeasures in place. Data centers selected must meet a minimum set of criteria before final selection by VMware.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.2	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Yes. The vCloud Air data center located in Santa Clara, CA, is near an earthquake fault line. However, the facility has been physically hardened to withstand a 7.5 magnitude earthquake. All other data centers are located in areas that do not have a high probability/occurrence of high-impact environmental risks.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	At the vCloud Air management layer, functionality is enabled in the vSphere hypervisor and underlying hardware to deliver highly available compute resources. This includes automated hardware restart and workload migration and recovery in the event of hardware failure with an automated workload restart on new host.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	Yes. Customers are able to leverage two technologies to achieve this. Customers may take a single point-in-time snapshot leveraging the vCloud Director control functions, or may leverage a more robust feature set by using vCloud Air Data Protection. Data Protection is an optional data backup and recovery feature for VMware vCloud Air that enables self-service, policy-based protection of business-critical data. Policies can be defined around when data will be backed up and for how long backups are retained. These backups can be restored to replace the source workload, or can be duplicated to restore as a new
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	Yes. vCloud Air natively supports the Open Virtualization Format (OVF), making it simple to download, clone, migrate, copy, port or transfer workloads between environments. We also support vCloud Connector for moving workloads to other vSphere- or vCloud Director-based clouds.
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Yes. There are multiple ways to achieve this. vCloud Connector can be used to copy workloads to another vSphere- or vCloud Director-based environment and also to synchronize templates between locations. Additionally, vCloud Air Disaster Recovery allows for replication of on-premises vSphere workloads to vCloud Air. Customers may also use various third party replication appliances to replicate to offsite storage, including vCloud Air Object Storage, another cloud storage destination, or their own storage hardware within vCloud Air locations. VMware, for example, has a partnership with RackWare for appliance-based replication.
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	Yes. Customers may elect to use third party tools for restore and recovery. VMware, for example, works with third party providers for appliance-based replication. Please see the Solutions Exchange here: https://solutionexchange.vmware.com/store/category_groups/vcloud-air?q=vcloud+air
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes. Risk analysis is completed on a regular basis to identify natural and man-made threats. Reviews are triggered through change management, new projects, and critical process reviews. The resulting security mechanisms and redundancies are reviewed through regular audits.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Availability reports are available to customers upon request within 45 days after a validated SLA event or up to once per year.
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Security metric data, such as activity and audit logging, can be obtained through the portal and from the underlying vCloud Director control panel.
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	Availability reports are available to customers upon request within 45 days after a validated SLA event or up to once per year.
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes. As a part of the Information Security Management System for vCloud Air, a document management system is in place to ensure policies and procedures are reviewed and made available to appropriate individuals.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?	Yes. The VMware Record Retention Standard outlines the retention schedule for various types of records. Security logs, for example, are currently maintained for 3 months onsite and 1 year in offsite storage. Customers may additionally choose to set workload lease times based on their policy requirements. This can be defined within the Portal, or through integrated product offerings such as vRealize Automation. Lease policy can be defined at the blueprint layer and exposed to consumers/users via the self-serve portal. Further, backups using Data Protection can be granularly configured to retain data for extended periods, exceeding 3 years. Customers can also leverage third party tools to backup workloads to archival storage using vCloud Air Object Storage.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	VMware has processes in place to identify and escalate third party requests to the proper parties.
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes. vCloud Air has implemented all necessary mechanisms to ensure compliance with regulatory, statutory and contractual obligations. This includes retaining standard security logs for 3 months onsite and 1 year in offsite storage and retaining HIPAA-related documentation for 6 years.
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	Yes. Annual exercises are required as a part of the vCloud Air Business Continuity plan. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	vCloud Air teams work together 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. This is reviewed as a part the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
		CCC-01.2		Is documentation available that describes the installation, configuration and use of products/services/features?	vCloud Air teams document build documentation to ensure proper installation and configuration of new services and features. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Change Control & Configuration Management *Outsourced*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization	Do you have controls in place to ensure that standards of quality are being met for all software development?	VMware follows standardized testing and quality assurance processes during the software development lifecycle
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?	N/A - vCloud Air does not outsource software development activities.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?	VMware follows standardized testing and quality assurance processes during the software development lifecycle and maintains strict control for managing the introduction of change into production systems. The quality of our service is contractually commited to our customers via our publicly-available Service Level Agreements. These Service Level Agreements include coverage for the core components of vCloud Air such as networking, compute, storage, backup, and user interfaces.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	Yes. Known issues are provided publicly in our vCloud Air release notes.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes. Product bugs follow a standardized process for capture, investigation, development, testing, change approval, and implementation. Vulnerabilities are handled through our vulnerability management procedures which follow a similar methodology as product bugs but additionally embodies our risk treatment process.
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Configuration management and change management are validated by an independent third party at least annually as part of the vCloud Air ISO 27001 certification.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	VMware's Acceptable Use Policy prohibits the use of unauthorized software.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	vCloud Air defines the roles/rights/responsibilities for customers through a few documents including our Service Description, Terms of Service, and Service Level Agreement.
Data Security & Information Lifecycle	DSI-01	DSI-01.1		Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting	Yes. Customers can add metadata to a virtual machine through vCloud Director which can be leveraged through API's.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Management *Classification*		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	VMware has asset tags for each device.
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?	Ability to use system geographic location as an authentication factor is not available. Since authentication can be delegated to an external identity provider, any enforcement by the external provider would carry over to vCloud Director.
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes. Customers choose the physical data center where they want their data deployed. Data is not moved away from that physical data center unless data migration is performed by the customer or the customer purchases an offline data transfer offering.
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes. Customers choose the physical data center where they want their data deployed. Data is not moved away from that physical data center unless data migration is performed by the customer or the customer purchases an offline data transfer offering.
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	vCloud Air follows a data-labeling standard in addition to data classification guidelines.
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	Customers explicitly choose which vCloud Air location is used for resource instantiation, and customer data does not traverse locations without the explicit actions of the tenant administrator. Customers can install private lines (MPLS/VPLS) through Direct Connect to control where data is routed.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	vCloud Air documents data flows for the vCloud Air service. Network diagrams are reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	Customers explicitly choose which vCloud Air location best suits their needs, and customer data does not traverse locations without the explicit actions of the tenant administrator.
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	vCloud Air provides customers with the ability to create IPsec and SSL VPN tunnels from their environments which support the most common encryption methods including 128-byte and 256-byte AES.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Communication that transports sensitive information (authentications, administrative access, customer information, etc.) is encrypted with standard encryption mechanisms (i.e. SSH, TLS & Secure RDP).
Data Security & Information Lifecycle Management *Handling / Labeling / Security*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain	vCloud Air follows a data-labeling standard in addition to data classification guidelines.
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	VMware has a data handling and protection standard in place to guide employees on appropriate labeling and handling for each classification level. Handling procedures include the secure processing, storage, transmission, declassification and destruction of data.
Data Security & Information Lifecycle Management *Nonproductio n Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes. vCloud Air has procedures in place to ensure only test data is utilized. This is reviewed as a part the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	Yes. data stewardship and ownership is outlined in the Risk Assessment Policy for vCloud Air. This is reviewed as a part of the annual independent third party ISO 27001 assessment for vCloud Air.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	VMware does not utilize customer data in non-production environments. VMware has a Data Handling and Protection Standard in place to guide employees on appropriate labeling and handling for each classification level. Handling procedures include the secure processing, storage, transmission, declassification and destruction of data. Media disposal controls are validated by an independent third party at least annually as part of the vCloud Air ISO 27001 certification.
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Exiting of the vCloud Air service is highlighted in the vCloud Air Service Description. VMware will delete the tenant environment as a part of termination of service. It is the tenant's responsibility to perform any special delete procedures (triple writing, 7x writing / zeroization, etc.) as a part of sanitization of any sensitive information within the tenant environment prior to exiting of the service.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	VMware maintains inventories of critical assets including ownership as a part of the risk assessment process for vCloud Air.
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	VMware maintains an inventory of critical supplier relationships in support of the business continuity plan for vCloud Air.
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes. Data Center locations are assessed by vCloud Air management to ensure appropriate physical security safeguards are in place.
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Not at this time. vCloud Air has physical safeguards in place to help reduce risks of unauthorized connection of technologies.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	Customer data does not traverse locations without the explicit actions of the tenant administrator. Documentation exists describing the use of supporting migration and replication technologies such as vCloud Connector and vSphere Replication for vCloud Air Disaster Recovery. vCloud Connector also supports Offline Data Transfer using a physical device containing customer data, shipped to a vCloud Air location and imported into the customer's cloud environment. Customers have complete control over when and how their data migrates between environments; VMware does not move
Datacenter Security *Offsite equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	Policies and procedures are in place to guide personnel on media sanitization once drives are no longer in use. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air. Audit reports are available upon request and an executed NDA.
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Policies and procedures are in place to establish a secure working environment. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	Business Conduct Guidelines and Security awareness training is required upon hire and at least annually. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	Yes. Customers choose the physical data center where they want their data deployed. Data is not moved away from that physical data center unless data migration is performed by the customer or the customer purchases an offline data transfer offering.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Ingress and egress points are monitored by vCloud Air data center providers.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	vCloud Air restricts physical access to authorized personnel. Audits are performed on a regular basis to confirm appropriateness.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	Key management policies and procedures are in place to guide personnel on proper encryption key management.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used	Do you have a capability to allow creation of unique encryption keys per tenant?	vCloud Air has key management controls in place. vCloud Air does not manage customer keys.
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	vCloud Air has key management controls in place. vCloud Air does not manage customer keys.
		EKM-02.3		Do you maintain key management procedures?	Key management policies and procedures are in place to guide personnel on proper encryption key management.
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
		EKM-02.5	protocol design and algorithms used; access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	VMware vCloud Air strongly recommends the use of in-guest encryption tools to protect customer data at rest within our service. Customers can use partner solutions like HyTrust DataControl for encryption. See our partner solutions here: https://solutionexchange.vmware.com/store/category_groups/vcloud-air Learn more about HyTrust DataControl here: https://solutionexchange.vmware.com/store/products/hytrust-
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	VMware vCloud Air strongly recommends the use of in-guest encryption tools to protect customer data at rest within our service. Customers can use partner solutions like HyTrust DataControl for encryption.
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes. During transport from on-premises environments to vCloud Air, vCloud Connector uses AES-256 encryption to encapsulate in-transit workloads. For in-cloud vMotion activities, a dedicated, secure and encrypted network is used exclusively for this purpose. Further, customers may leverage in-guest encryption technology from a range of supported partners to protect data within the virtual machine.
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	Customers may use a variety of preferred partner solutions for delivering in-guest-based encryption controls. When using tools like HyTrust DataControl, VMware does not manage customer encryption keys. Supported partner technologies are listed in the vCloud Air Solution Exchange. See our partner solutions here: https://solutionexchange.vmware.com/store/category_groups/vcloud-air Learn more about HyTrust DataControl here: https://solutionexchange.vmware.com/store/products/hytrust-
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Key management policies and procedures are in place to guide personnel on proper encryption key management.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Customers are responsible for encrypting their own data, and the management of cryptographic keys is solely the responsibility of the customer. VMware has trusted partners that offer vCloud Air compatible solutions for encrypting data at rest, but VMware does not directly manage customer encryption keys.
		EKM-04.3		Do you store encryption keys in the cloud?	Customers are responsible for encrypting their own data, and the management of cryptographic keys is solely the responsibility of the customer. VMware has trusted partners that offer vCloud Air compatible solutions for encrypting data at rest, but VMware does not directly manage customer encryption keys.
		EKM-04.4		Do you have separate key management and key usage duties?	Yes. vCloud Air uses OpenSSL and minimum 2K key lengths
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Security baselines are documented to guide personnel to ensure appropriate configurations are in place to protect sensitive information.
		GRM-01.2		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	vCloud Air has the ability to monitor certain aspects of the information security baseline.
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	Yes. Customers can import their own virtual machines and virtual machine templates into vCloud Air. vCloud Air supports the Open Virtualization Format (OVF) and customers can import their own trusted OVF images. vCloud Air templates can also be synched with on-premises catalogs to ensure consistent conformance with a customer's IT standards.
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	Customers can send network traffic data logs, including traffic coming to and from the customer's environment, to a syslog server for continuous monitoring. Additionally, customers can access more than 50 metrics around the service performance (across compute, memory, storage, and networking) through APIs and integrate this data to their preferred solution. These allow customers to have continual validation of their physical and logical control status.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	vCloud Air conducts risk assessments at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity, and availability of sensitive information.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	The compliance department along with management are responsible for maintaining awareness and complying with security policies. Business Conduct Guidelines and Security awareness training is required upon hire and annually. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCoud Air.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	vCloud Air has an Information Security Management System in place that is ISO 27001 certified. Please see the vCloud Air Security and Compliance page for more information http://vcloud.vmware.com/service-offering/cloud-compliance
		GRM-04.2		Do you review your Information Security Management Program (ISMP) least once a year?	Yes. vCloud Air performs a formal review of the vCloud Air Information Security Management System at least annually.
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	Yes. The vCloud Air ISMS committee includes leadership representation from all major functions of the business. Furthermore, all members of the business are required to complete annual security and awareness training. Applicable security provisions are added to ensure providers are contractually obligated to maintain appropriate security provisions.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	Yes. The vCloud Air Information Security Management System is based on the ISO 27001 framework and has been certified.
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Applicable security provisions are added to ensure providers are contractually obligated to maintain appropriate security provisions.
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	The vCloud Air Information Security Management System is based on the ISO 27001 framework and has been certified. The vCloud Air ISO certificate is available for tenants to view at the following site: http://vcloud.vmware.com/service-offering/cloud-compliance
		GRM-06.4		Do you disclose which controls, standards, certifications and/or regulations you comply with?	Yes. Under NDA, customers may be provided with the attestation reports from our third party audits which typically contain the controls that are in scope and complied with for that program.
Governance and Risk Management *Policy*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes. vCloud Air follows the VMware corporate disciplinary process for violations of security policies and procedures.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes. vCloud Air follows the VMware corporate disciplinary process for violations of security policies and procedures.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Relevant updates to security policies and procedures are made once identified as a part of the risk assessment or corrective action.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Security controls are documented and reviewed as a part of the annual independent third party ISO 27001, SOC1, and SOC2 assessments for vCloud Air. Any material changes are documented as a part of the audit reports.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	Privacy and security policies are reviewed at least annually.
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	vCloud Air conducts risk assessments at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity, and availability of sensitive information.
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability	The vCloud Air risk assessment independently assesses likelihood and impact associated considering all risk categories.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.	Do you have a documented, organization-wide program in place to manage risk?	VMware has an organization-wide program to manage risk.
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	The vCloud Air Information Security Management System is based on the ISO 27001 framework and has been certified. For more information, please see: http://vcloud.vmware.com/service-offering/cloud-compliance
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	VMware's Security Operations Center and vCloud Air Network Operations Center monitor the environment for events that may impact the privacy or security of sensitive data.
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	Yes. VMware manages the privacy policy in line with industry standards.
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	Background checks are performed on all VMware personnel and all personnel who have access to vCloud Air infrastructure.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their role versus the tenant's role in providing information security controls?	Business Conduct Guidelines and Security awareness training is required upon hire and annually. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	Yes. An enterprise Learning Management System is used to facilitate the delivery of VMware training programs. The tools used record the successful completion of required training and completion reports are reviewed during ISMS committee meetings.
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	All VMware personnel must sign employment agreements to ensure all customer/tenant information is kept confidential.
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	All personnel who have access to the vCloud Air infrastructure must undergo annual security awareness training. Management is notified if training is overdue, and it is management responsibility to ensure that personnel are trained.
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	HR systems, policies, and procedures are in place to help guide management during termination or change of employment status.
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	Termination processes are in place to guide timely revocation of access and return of assets.
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	VMware has Mobile Device, Remote Access, and Acceptable Use policies that define the requirements for access to sensitive data. These policies are reviewed annually as part of our regular certification process.
Human Resources *Nondisclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Applicable agreements are reviewed at planned intervals by VMware.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Yes. The vCloud Air Terms of Service, Service Description, and service documentation outline the line of demarcation between the customer's responsibilities and those of VMware.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems	Do you provide documentation regarding how you may or access tenant data and metadata?	Yes. The vCloud Air Terms of Service, Service Description, and service documentation outline the line of demarcation between the customer's responsibilities and those of VMware.
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	The VMware Data Privacy Addendum to VMware vCloud Air Terms of Service discloses to customers what type of usage data is collected during their use of the service. This includes data such as information on the amount of computing and storage resources purchased or consumed, named user counts, and third party licenses consumed.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
		HRS-08.3	infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	No. The type of data we collect is outlined in our Data Privacy agreement and the methods by which we use the data is clearly stated and available publicly on our website. This collection of the types of data specified are necessary in order for us to delivery the services outlined by our Service Description.
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive	Do you provide a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons	A formal security awareness training program is in place to guide personnel on maintaining appropriate security for the vCloud Air service.
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	A formal security awareness training program is in place to guide personnel on maintaining appropriate security for the vCloud Air service.
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory	A formal security awareness training program is in place to guide personnel on maintaining appropriate security for the vCloud Air service.
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	A formal security awareness training program is in place to guide personnel on maintaining appropriate security for the vCloud Air service.
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	A formal security awareness training program is in place to guide personnel on maintaining appropriate security for the vCloud Air service.
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	The VMware Information Security Governance Policy is in place to guide employees on the protection of customer data.
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Access control, separation of duty, and other policies define which individuals are allowed to have access to vCloud Air management systems. Furthermore, the vCloud Air management network is isolated from the VMware corporate network to further restrict access. Log capture, security monitoring, and intrusion detection tools are in place to safeguard the management systems.
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Access control, separation of duty, and other policies define which individuals are allowed to have access to vCloud Air management systems. Furthermore, the vCloud Air management network is isolated from the VMware corporate network to further restrict access. Log capture, security monitoring, and intrusion detection tools are in place to safeguard the management systems.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Access control, separation of duty, and other policies define which individuals are allowed to have access to vCloud Air management systems. Furthermore, the vCloud Air management network is isolated from the VMware corporate network to further restrict access. Log capture, security monitoring, and intrusion detection tools are in place to safeguard the management systems.
		IAM-01.2		Do you monitor and log privileged access (administrator level) to information security management systems?	Privileged access is logged and captured in a centralized log server.
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Procedures are in place to ensure timely removal of system access that is no longer required for business purpose.
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	Procedures are in place to ensure timely removal of system access that is no longer required for business purpose. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Yes. Authorized personnel have access to provide management access to the vCloud Air environment.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Identity and access management controls are in place within the vCloud Air environment to ensure appropriate personnel have access.
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	Identity and access management controls are in place within the vCloud Air environment to ensure appropriate personnel have the appropriate level of access.
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes. The vCloud Air Terms of Service, Service Description, and documentation outline the line of demarcation between the customer's responsibilities and that of VMware.
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Identity and access management controls are in place within the vCloud Air environment to ensure appropriate personnel have the appropriate level of access.
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Identity and access management controls are in place within the vCloud Air environment to ensure appropriate personnel have the appropriate level of access. Audits are performed at regular intervals to ensure appropriateness.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	Yes. vCloud Air has several ways to recover from disasters. vCloud Air infrastructure leverages vSphere High Availability to automatically restart a workload from any failure in a specific host. Data Protection backs up workloads to a separate storage environment. vCloud Air Disaster Recovery allows for the replication of workloads from vSphere to vCloud Air. Customers are able to implement additional redundancy via in-guest replication with third party solutions and/or manual synchronization via import/export/migration tools.
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	VMware vCloud Air operates a network operations center. In the event of an upstream event, vCloud Air works with those vendors to develop a preventative action plan.
		IAM-07.3		Do you have more than one provider for each service you depend on?	VMware utilizes multiple providers for service dependencies to minimize the risk of service disruptions.
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	As a part of the Business Impact Analysis for vCloud Air, dependencies on third parties are documented to ensure appropriate business continuity measures are in place. This is reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air.
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	Yes. Customers may declare a disaster via self-service through a number of interfaces (portal, vSphere client), or they may call our Global Support team.
		IAM-07.6		Do you provided a tenant-triggered failover option?	Yes. Workloads can be failed over as per a pre-defined policy or through manual event triggering.
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	VMware shares high level business continuity documentation upon request and with an executed NDA.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	Yes. Customers are provided a secure URL to create their first account. Afterward, customers may elect to invite other users within their organization. For these users the process is the same: a secure URL is provided, and upon visiting this URL the new users are required to create a unique, secure password. All of the details for performing these actions are documented in the vCloud Air user guides. Additionally, vCloud Air provides support for identity federation via SAML 2 authentication.
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes. Within vCloud Air, customers may assign unique roles and responsibilities to specific users within the account. Roles are delineated by function and privilege, such as Network Administrator who can only manage network-related settings, or End User who can only consume a workload but not alter its configuration in any way. Additionally, vCloud Air provides support for identity federation via SAML 2 authentication.
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and	Processes and procedures are in place to ensure management and security team authorization is in place prior to provisioning of access.
		IAM-09.2		Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	User access reviews and appropriateness is audited and reviewed as a part of the annual independent third party ISO 27001, SOC1, and SOC 2 assessments for vCloud Air. Audit reports are available upon request and an executed NDA.
Identity & Access Management *User Access*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Access audits are performed to validate appropriateness of access.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Reviews		IAM-10.2	business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Termination of inappropriate access is recorded in a ticketing system.
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	User access reviews and appropriateness is audited and reviewed as a part of the annual independent third party ISO 27001, SOC1, and SOC 2 assessments for vCloud Air. Audit reports are available upon request and receipt an executed NDA.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Yes. User access reviews and appropriateness is audited and reviewed as a part of the annual independent third party ISO 27001, SOC1, and SOC 2 assessments for vCloud Air. Audit reports are available upon request and receipt of an executed NDA.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes. User access reviews and appropriateness is audited and reviewed as a part of the annual independent third party ISO 27001, SOC1, and SOC 2 assessments for vCloud Air. Audit reports are available upon request and an executed NDA.
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Support of external identity & access management federation with customer directories is availble with the Dedicated Cloud Service.
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	vCloud Air supports Identity Federation using SAML v2 standards for authenticating with the customer's Identity Provider solutions. Support of identity federation with customer directories is currently available with the Dedicated Cloud Service.
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	Yes. The vCloud Air Portal uses multiple methods for ensuring password policy enforcement, including minimum password length, password expiration, complexity and lockout after more than 5 failed login attempts. With support for Identity Federation, this can be defined by the customer's Identity Provider solution
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	Identity Federationsupport uses SAML v2 standards for authentication with customer's Identity Provider solutions. Support of identity federation with customer directories is currently available as a Beta with full release within the second half of 2016
		IAM-12.10		Do you support the ability to force password changes upon first logon?	Yes. This is the default behavior of new accounts or users within an account using the vCloud Air portal.
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes. Accounts may be unlocked by Administrators with the appropriate level of privilege governing user accounts, or by an authorized individual contacting Global Support Services
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted	Yes. vCloud Air has multiple levels of access roles
		IAM-13.2		Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	Yes. vCloud Air has the capability to detect these types of attacks.
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	Yes. vCloud Air has logically separated networks that restrict Tenant access to their own private networks.
Infrastructure & Virtualization Security *Audit Logging / Intrusion*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Network IDS is implemented. A file integrity monitoring solution has been architected.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	Yes. Security personnel have access to the definitive central log servers.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Detection		IVS-01.3	accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	Regulatory requirements and applicability is assessed as a part of the vCloud Air annual risk assessment.
		IVS-01.4		Are audit logs centrally stored and retained?	Yes. Audit logs are centrally stored.
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	The Security Operations Center monitors logs for security events.
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or	Yes. All infrastructure actions are logged in the service.
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	Yes. When VMware updates public catalog items, changes are automatically propagated to public tenant catalogs. This affects only templates within the public catalog, as VMware does not control workloads that are already deployed and active, or the contents of a customer's private catalog. It is the customer's responsibility to ensure security and to update policy governing their own private template catalogs, as well as running workloads. Using tools such as vCloud Connector, changes to customer templates can be automatically propagated to all of their
Infrastructure & Virtualization Security *Clock Synchronizati*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes. NTP is in place to ensure time is synchronized.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Customers using Dedicated Cloud are able to control their own oversubscription settings for Memory and Compute resources. Users may also choose between a variety of storage options with different performance characteristics on a per-workload basis.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	In the Dedicated Cloud service, customers are able to control their own oversubscription settings for Memory and Compute resources. With the Virtual Private Cloud service, this control is disabled as the oversubscription is carefully managed by VMware to ensure guaranteed performance in the multi-tenant environment.
		IVS-04.3		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	Yes. Capacity reports are monitored at least daily to ensure appropriate capacity is maintained.
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	VMware will use commercially reasonable efforts to ensure that each class of service purchased for an identified user of an instance of a Service Offering is “Available” during a given calendar month equal to the “Availability Commitment” provided in the documented SLA.
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Yes, the VMware vulnerability scanning technology provider fully supports virtualized networks and hosts.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Customers have access to documentation and user guides as well as technical support, a knowledge base, and other technical assets providing guidance. Additionally, professional services are available for purchase. Customers may also reference white papers and other information that VMware has produced over the years regarding how to properly secure a virtual environment.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes. Diagrams are updated regularly.
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes. Audits are performed on a on a regular basis.
		IVS-06.4		Are all firewall access control lists documented with business justification?	Yes. A formal firewall access control approval process is in place to document access justification and authorization.
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	Yes. Security hardening standards are in place to include file integrity monitoring, antivirus and logging.
Infrastructure &	IVS-08	IVS-08.1	Production and non-production environments shall be separated to	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	N/A

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Virtualization Security *Production / Nonproduction Environments*		IVS-08.2	prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Customers have access to documentation and user guides as well as technical support, a knowledge base, and other technical assets providing guidance. Additionally, professional services are available for purchase. Customers may also reference white papers and other information that VMware has produced on how to designing production ready environments
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	Yes. Production and non-production environments are logically and physically segregated. Communication that transports sensitive vCloud Air information (authentications, administrative access, customer information, etc.) is encrypted with standard encryption mechanisms
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures	Are system and network environments logically separated to ensure business and customer security requirements?	Yes. vCloud Air has logically separated networks that restrict Tenant access to their own private networks
		IVS-09.2		Are system and network environments logically separated to ensure compliance with legislative, regulatory and contractual requirements?	The vCloud Air Terms of Service and Data Privacy Addendums establish the line of demarcation between the responsibility of VMware and those of the customer as it pertains to data protection. In addition, security briefs are available to customers to o establish transparency regarding the separation of responsibility between VMware and the customer for compliance programs such as HIPAA or data privacy rules
		IVS-09.3		Are system and network environments logically separated to ensure separation of production and non-production	Yes. Production and non-production environments are logically and physically segregated.
		IVS-09.4		Are system and network environments logically separated to ensure protection and isolation of sensitive data?	Yes. Production and non-production environments are logically and physically segregated.
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	Communication that transports sensitive information (authentications, administrative access, customer information, etc.) is encrypted with standard encryption mechanisms.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	VMware does not migrate data internally.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Identity and access management controls are in place within the vCloud Air environment to ensure appropriate personnel have the appropriate level of access and is based on the principle of least privilege.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless	N/A. Wireless networks are not used to connect directly to the vCloud Air production environment.
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys	N/A - Wireless networks are not used to connect directly to the vCloud Air production environment.
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Processes are in place to detect rogue wireless access points within the vCloud Air environment.
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Network diagrams are in place which identify high-risk environments and systems. The vCloud Air environment is assessed against compliance requirements at least annually.
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	vCloud Air has security controls in place to reduce the risk to sensitive information in the production environment.
Interoperability & Portability *APIs*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes. Our published API documentation can be found here: http://pubs.vmware.com/vca/index.jsp#com.vmware.ICbase/Welcome/welcome.html
Interoperability & Portability *Data Request*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	vCloud Air does not directly manage customer data. Customers can have access to unstructured data through their own systems and applications which they deploy.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	vCloud Air service leval agreements govern all aspects of the service, and can be found here: http://vcloud.vmware.com/legal
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Migration of data to and from vCloud Air is fully managed by the customer. Acceptable use for those options are defined by the Terms of Service and Service Legal Agreements.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes. Migration of data to and from vCloud Air is fully managed by the customer and they include using vCloud Connector and/or Offline Data Transfer which both leverage SSL encyrption methods.
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes. Customers have access to a set of documentation which covers various aspects of the cloud architecture which are relevant to the customer/tenant, including networking protocols and capabilities.
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	Yes. vCloud Air natively supports the Open Virtualization Format (OVF), making it simple to download, clone, migrate, copy, port or transfer workloads between environments.
		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	VMware does document custom changes made to hypervisors in use. VMware does not provide this information to tenants.
Mobile Security *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	VMware has a Mobile Device Policy in place to guide employees on proper security guidelines pertaining to mobile devices. Security of mobile devices are discussed in the annual security awareness training.
Mobile Security *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Device Inventory*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Device Management*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Encryption*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Jailbreaking*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
and Rooting		MOS-12.2	(e.g. jailbreaking or rooting) and is enforced through detective and preventative controls on the device or	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Lockout Screen*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Operating Systems*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	N/A – Mobile devices do not connect directly to the vCloud Air production environment. VMware does have a Mobile Device Policy in place.
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes. vCloud Air maintains liaisons and points of contacts with local authorities as a part of incident response plans.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	Yes. vCloud Air leverages the VMware Security Incident Response Policy to manage the incident response process.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	This is not standard practice for vCloud Air except for remote situations where modifications have been made contractual agreements.
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The vCloud Air Terms of Service, Service Description, and web content outline the line of demarcation between the customer's responsibilities and that of VMware.
		SEF-02.4		Have you tested your security incident response plans in the last year?	The incident response plan is tested at least annually if a security incident did not occur.
Security Incident Management, E-Discovery	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and	Yes. The vCloud Air SIEM merges data sources.
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	No. vCloud Air does not monitor tenant traffic or behavior.
Security Incident Management, E-Discovery	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes. vCloud Air has a formal Incident Response group that facilitates all Incident Response activities.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis	Yes. vCloud Air has a formal Incident Response group that facilitates all Incident Response activities.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
& Cloud Forensics *Incident Response Legal*		SEF-04.3	information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes. each Tenant organization is independent
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes. vCloud Air has a comprehensive program to monitor information security incidents.
Security Incident Management, E-Discovery & Cloud	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Information pertaining to security breaches will only be shared with tenants where VMware is contractually or legally obligated to do so .
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	Information pertaining to security breaches will only be shared with tenants where VMware is contractually or legally obligated to do so .
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Yes. This is completed as a part of the annual risk management process for vCloud Air.
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Yes. This is completed as a part of the annual risk mitigation process for vCloud Air.
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	Information pertaining to security breaches will only be shared with tenants where VMware is contractually or legally obligated to do so .
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	The VMware Data Privacy Addendum to VMware vCloud Air Terms of Service discloses to customers what type of usage data is collected during the customer's use of the service. This includes data such as information on the amount of computing and storage resources purchased or consumed, named user counts, and third party licenses consumed.
		STA-03.2		Do you provide tenants with capacity planning and use reports?	Yes. During the sales process, a customer may elect to leverage tools such as vRealize Operations (formerly vCenter Operations Manager) to attain a baseline of on-premises capacity utilization for the purpose of properly allocating capacity for workloads to be migrated to the cloud. Further, customers may integrate vRealize Operations into vCloud Air via a free Management Pack. Customers can then import capacity, availability and performance metrics into their local instance of vRealize Operations. Finally, metrics data including resource utilization metrics are exposed via APIs to feed into a customer's preferred capacity planning solution.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes. Internal audits are completed at least annually of the Information Security Management System for vCloud Air.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Providers are monitored for compliance with applicable requirements.
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	VMware has a sourcing program in place to select providers that meet VMware requirements which include compliance with applicable laws.
		STA-05.3		Does legal counsel review all third-party agreements?	VMware has a program in place to select providers that meet VMware requirements which include legal review of agreements.
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	VMware has a program in place to select providers that meet VMware requirements which include security provisions.
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Sub processing agreements are reviewed as a part of the vCloud Air annual independent third party ISO 27001, SOC1 and SOC 2 assessments. Audit reports are available upon request and execution of an NDA.
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	vCloud Air monitors provider audit reports and certifications to ensure effectiveness of applicable controls.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	vCloud Air IaaS Responses
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	SLAs, Terms of Service, Privacy addendums, etc, can be found here: http://vcloud.vmware.com/legal
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	vCloud Air has a formal process to document and track non-conformance as a part of our ISMS.
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes. vCloud Air monitors supplier performance and escalates issues as necessary.
		STA-07.4		Do you review all agreements, policies and processes at least annually?	vCloud Air monitors provider agreements and audit reports and certifications at least annually.
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	vCloud Air conducts risk assessments at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity, and availability of sensitive information.
		STA-8.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	vCloud Air conducts risk assessments at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity, and availability of sensitive information. This includes risks associated with providers.
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?	vCloud Air has a comprehensive vulnerability management program in place which includes vulnerability scanning and penetration testing of vCloud Air shared infrastructure. Tenants are permitted to perform vulnerability assessments against their allocated service objects with approval from vCloud Air operations. Tenants are not permitted to perform vulnerability assessments against shared VMware assets.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes. vCloud Air has a comprehensive vulnerability management program which includes vulnerability scans and penetration testing.
Threat and Vulnerability Management *Antivirus / Malicious*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your	Yes. Anti-malware programs are installed on components that are typically vulnerable to malware.
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time	Network IDS and anti-malware systems are configured and updated based on industry accepted time frames.
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes. Vulnerability scans are performed regularly as a part of the vulnerability management program for vCloud Air.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes. Vulnerability scans are performed regularly as a part of the vulnerability management program for vCloud Air.
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes. Vulnerability scans are performed regularly as a part of the vulnerability management program for vCloud Air.
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	Vulnerability scans are reviewed as a part of the annual independent third party ISO 27001 and SOC 2 assessments for vCloud Air. Audit reports are available upon request and under NDA.
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	vCloud Air provides ready-to-use operating systems and packaged applications within vCloud Air via the public template catalog. vCloud Air will patch and update operating systems and applications provided in the public template catalog. Only public catalog templates will be patched and updated by vCloud Air. A customer is responsible for any patches and updates within their tenant environment. vCloud Air management layer system security patches are evaluated upon release. Patches that remediate a critical vulnerability will be applied no later than 30 days from the date the patch was released.
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?	The vCloud Air patch timeframes are in line with industry standards and meet PCI standards.
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security	N/A – Mobile devices do not connect directly to the vCloud Air production environment.
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	N/A – Mobile devices do not connect directly to the vCloud Air production environment.