VMware vCloud Air SOC 1 Control Objectives/Activities Matrix

VMware vCloud Air goes to great lengths to ensure the security and availability of vCloud Air services. In this effort, we have undergone a variety of industry standard audits, assessments and certification efforts, including Service Organization Controls 1 (SOC1) Type 2.

This document is intended to provide customers with additional context around the SOC 1 control objectives that VMware has designed and implemented for management and delivery of vCloud Air services. An independent third-party audit firm annually assesses these controls, and the details of these audits are available upon request.

The matrix within this document is a tool that can assist your organization in quickly identifying the control activities that vCloud Air has in place to satisfy the control objectives.

****DISCLAIMER** This document only includes the control objectives and related control activities of VMware vCloud Air services and excludes the control objectives and related controls of any data center providers. An independent third-party audit firm assesses vCloud Air services annually.

To request a copy of the most recent vCloud Air SOC 1 report, please contact your VMware salesperson.

COMPUTER OPERATIONS

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that application and data files for the vCloud Air system are backed up in a timely manner and securely stored.

#	VMware vCloud Air Control Activities
1.01	Documented policies and procedures are in place to guide personnel in performing data backups and data restoration.
1.02	An automated backup system is in place to perform scheduled backups of production data and systems.
1.03	The automated backup system is configured to send alert notifications to information technology operations personnel regarding backup job completion status.
1.04	Information technology operations personnel perform backup media restores as a component of normal business operations to verify that system components can be recovered from system backups.
1.05	Administrative access privileges to backup systems and data are restricted to user accounts accessible by authorized personnel.

Computer Operations

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that vCloud Air systems are maintained in a manner that helps ensure system availability.

#	VMware vCloud Air Control Activities
2.01	Documented escalation procedures and a ticketing system are in place to guide employees in identifying, reporting, and responding to system availability issues and related security incidents.
2.02	Documented standard build procedures are utilized for the installation and maintenance of production servers.
	Patch Management
2.03	A patch management methodology is in place to guide personnel in the initiation, testing, and deployment of patches for production infrastructure.
	Monitoring
2.04	Network Operations personnel utilize an automated ticketing system to manage system incidents, response, and resolution.
2.05	Multiple enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.
2.06	The enterprise monitoring applications are configured to forward system events to a central logging system. The central logging system is configured to display on-screen alert notifications when predefined thresholds are exceeded on monitored systems.
2.07	Security and network operations personnel monitor the central logging system for security and availability events 24 hours per day.
2.08	Operational statistics reports are reviewed by management on a quarterly basis.
	Antivirus
2.09	A central antivirus server is configured with antivirus software to protect registered production workstations and servers.
2.10	The antivirus software is configured to scan for updates to antivirus definitions and update registered clients on daily basis.
2.11	The antivirus software is configured to scan registered clients on a weekly basis.

INFORMATION SECURITY

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

#	VMware vCloud Air Control Activities
3.01	Documented policies and procedures are in place to guide personnel regarding information security procedures.
3.02	User access requests to production systems are documented within a ticketing system and require manager approval.
3.03	An employee termination ticket is completed and employee access to production systems is revoked as a component of the employee termination process.
	Network Domain Authentication
3.04	The network domain is configured to enforce the following password requirements: • Minimum password length • Minimum password history • Password expiration intervals • Password complexity • Invalid password account lockout threshold
	Network Domain Access
3.05	Administrative access privileges to the network domain are restricted to user accounts accessible by authorized personnel.
	Network Domain Logging
3.06	The network domain is configured to log the following security events that are reviewed by security administrators on an ad hoc basis: • Account logon events • Account management • Security administration
	Production Environment Authentication
3.07	Users connect to the production environment via a two-factor VPN authentication.
	Production Environment Access
3.08	Administrative access privileges to the VPN systems are restricted to user accounts accessible by authorized personnel.

#	VMware vCloud Air Control Activities
	Operating System Authentication (Windows)
3.09	Users are required to authenticate with a valid user account and password before being granted access to the operating systems.
	Operating System Access (Windows)
3.10	Administrative access privileges to the operating systems are restricted to user accounts accessible by authorized personnel.
	Operating System Logging (Windows)
3.11	The operating systems are configured to log the following security events that are reviewed by security administrators on an ad hoc basis: • Account logon events • Account management • Security administration
	Operating System Authentication (Linux)
3.12	Prior to gaining access to Linux operating systems, operating system users are required to connect and authenticate via a user account and password before being granted access to the operating systems.
	Operating System (Linux)
3.13	Administrative access privileges to the operating systems are restricted to user accounts accessible by authorized personnel.
3.14	Operating system users are authenticated via public/private SSH key pair with passphrase before being granted access to the operating system.
	Operating System Logging (Linux)
3.15	The operating systems are configured to log the following security events that are reviewed by security administrators on an ad hoc basis: • Account logon events • Account management • Security administration
	Application Authentication (vCloud Director)
3.16	Authentication to the application is granted based on the user's network domain credentials.
	Application Access (vCloud Director)
3.17	Administrative access privileges to the application are restricted to user accounts accessible by authorized personnel.
	Application Authentication (vCIM)
3.18	Application users are authenticated via a user account and password before being granted access to the application.

#	VMware vCloud Air Control Activities
	Application Access (vCIM)
3.19	Administrative access privileges to the application are restricted to user accounts accessible by authorized personnel.
	Application Logging (vCloud Director and vCIM)
3.20	The applications are configured to log the following security events that are reviewed by security administrators on an ad hoc basis: • Account logon events • Account management • Security administration

DATA COMMUNICATIONS

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and vCloud Air.

#	VMware vCloud Air Control Activities
4.01	Management maintains documented policies and procedures to govern data communication activities that include, but are not limited to, the following: • Firewall system administration • Remote access
4.02	Documented escalation procedures for reporting security incidents are in place to guide employees in identifying, reporting, and acting upon system security breaches and other incidents.
	Firewall Systems
4.03	High availability firewall systems are in place to filter unauthorized inbound network traffic from the Internet.
4.04	The firewall systems are configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
4.05	Access to modify the firewall system software, configurations or rulesets is restricted to shared and individual user accounts accessible by authorized personnel.
	Remote Access
4.06	Users connect to the production environment via a two-factor VPN authentication.
4.07	Encrypted VPNs are required for remote access to help ensure the security and integrity of the data passing over the public network.
4.08	Administrative access privileges to the VPN systems are restricted to user accounts accessible by authorized personnel.

#	VMware vCloud Air Control Activities
	Network Administration
4.09	Security operations personnel utilize an automated ticketing system to document security violations, responses, and resolution.
4.10	Security operations personnel monitor the central logging system for security events 24 hours per day.
4.11	Web servers utilize SSL encryption for web communication sessions.
4.12	An IDS is in place to analyze network device logs and report possible or actual network security breaches.
4.13	The IDS is configured to forward network events to a central logging system. The central logging system is configured to send e-mail alert notifications to the security operations team when certain network events are detected.
4.14	Information security personnel perform a vulnerability assessment on a monthly basis.
4.15	Management ensures that a penetration test is performed at least annually to identify potential security vulnerabilities.

Application Change Control

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that unauthorized changes are not made to vCloud Air production application systems.

#	VMware vCloud Air Control Activities
5.01	Documented policies and procedures are in place to guide personnel in the requesting, approval, and testing of changes to applications.
	Source Code Repository
5.02	Version control software is utilized to control access to the source code.
5.03	Changes to source code result in the creation of a new version of the application code.
	Application Change Process
5.04	A ticketing system is in place to centrally maintain, manage, and monitor enhancement, development, and maintenance activities.
5.05	QA personnel perform testing of software changes prior to implementation in the production environment.
5.06	Testing efforts are performed in an environment that is physically and logically separate from the production environment.
5.07	A change advisory board (CAB) meeting is held on a weekly basis to discuss ongoing and upcoming projects and to approve software changes.
5.08	CAB members approve software changes prior to implementation.

#	VMware vCloud Air Control Activities
5.09	The ability to implement changes is restricted to user accounts accessible by authorized personnel.
5.10	Release notes and known issues are available to customers on the support center web site.

CHANGE MANAGEMENT

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that changes to vCloud Air infrastructure are logged, authorized, tested, approved, implemented, and documented.

#	VMware vCloud Air Control Activities
6.01	Documented policies and procedures are in place to guide personnel in the requesting, approval, and testing of changes to systems and infrastructure.
	Hosting Infrastructure Changes
6.02	A ticketing system is in place to centrally maintain, manage, and monitor enhancement, development, and maintenance activities.
6.03	Operations support personnel document test plans prior to implementation in the production environment.
6.04	A CAB meeting is held on a weekly basis to discuss ongoing and upcoming projects and to approve infrastructure changes.
6.05	CAB members approve CAB level infrastructure changes prior to implementation.

CUSTOMER SUPPORT AND INCIDENT RESPONSE

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that customer inquiries and issues are responded to in a timely manner.

#	VMware vCloud Air Control Activities
7.01	Documented policies and procedures are in place to guide personnel in regards to customer support and incident response procedures.
7.02	GSS personnel utilize an automated ticketing system to track and manage customer inquiries and issues to resolution.
7.03	vCloud Air Operations personnel meet with GSS personnel on a weekly basis to review open and aged tickets.
7.04	A customer service ticket metrics report is generated on a weekly basis.

MONITORING OF DATA CENTER OPERATIONS

VMware vCloud Air Control Objective: Control activities provide reasonable assurance that controls at Data Center Provider organizations are monitored and additional VMware controls are applied to VMware contracted secured spaces.

#	VMware vCloud Air Control Activities
8.01	Documented policies and procedures are in place to guide VMware authorized personnel in regards to monitoring data center controls.
8.02	Agreements are in place with data center providers to ensure that physical and environmental security controls are being met.
8.03	Data center provider audit reports and or certification documentation, if available, are reviewed to determine effectiveness of data center provider physical and environmental security controls.
8.04	VMware authorized data center operations personnel perform quarterly walkthroughs of the data center providers using a checklist to monitor controls which include the following: • Security guards and/or personnel are in place to monitor the data center ingress points • Assigned badge access devices are in working order • Assigned biometric devices are in working order • Data center temperature is at an acceptable level • Systems are powered appropriately
8.05	Badge access logs for the contracted secured spaces are requested from the data center providers and retained by VMware for at least ninety days.