VMware SDDC Product Applicability Guide for FedRAMP, v 1.0

February, 2014

v1.0

TECHNICAL GUIDE

This is the first document in the Compliance Reference Architecture for FedRAMP. You can find more information on the Framework and download the additional documents from the VMware FedRAMP Compliance Resources on VMware Solution Exchange.

Table of Contents

EXECUTIVE SUMMARY 3

INTRODUCTION 4

OFFICIAL FEDRAMP GUIDANCE AS IT APPLIES TO CLOUD ENVIRONMENTS 6

CLOUD COMPUTING 10

WHERE TO START - CONSIDERATIONS FOR SYSTEM OWNERS, IT AND ASSESSORS 12

VMWARE PRODUCTS AND FEDRAMP 14

VMWARE FEDRAMP REQUIREMENTS MATRIX (OVERVIEW) 16

FEDRAMP REQUIREMENTS MATRIX (BY VMWARE SUITE) 18

vCloud Suite 5.5 18

vCloud Networking and Security Suite 5.5 20

vCenter Operations Management Suite 5.8 22

VMware NSX Suite 6.0 25

Executive Summary

The Federal Risk Authorization and Management Program (FedRAMP) was created to provide a streamlined and standardized process along with a “do once, use many times” approach to the authorization of commercial cloud services. This program enables US Government agencies to take full advantage of the benefits of migrating their IT assets and infrastructure to the cloud, as they work to meet the goals of the *Federal Cloud Computing Strategy* published by the White House in February 2011. FedRAMP, which is governed by a Joint Authorization Board (JAB) that consists of representatives from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD) is also endorsed by the U.S. government’s CIO Council including the Information Security and Identity Management Committee (ISIMC).

The FedRAMP program provides an avenue for Cloud Service Providers (CSPs) to obtain a provisional Authorization To Operate (p-ATO) after undergoing an independent third-party security assessment that has been reviewed by the JAB. By assessing security controls on candidate platforms, and providing P-ATOs on platforms that have acceptable risk, FedRAMP significantly reduces the time and cost to agencies by removing the assessment and authorization requirements of the underlying cloud vendor services on a system-by-system basis. This minimizes the work each Consumer of FedRAMP Cloud resources must undergo to receive an actual ATO for the workloads running applications that process sensitive data and transactions.

VMware, the leader in cloud computing software for enterprises and cloud hosting service providers alike, recognizes the tremendous opportunity that FedRAMP provides customers wishing to leverage VMware vCloud-powered FedRAMP environments for hosting their enterprise applications. For an entity wishing to host applications in a FedRAMP-accredited VMware vCloud hosting provider, or for the vCloud hosting provider itself, it is beneficial to understand which features of the VMware stack may apply in gaining and maintaining FedRAMP compliance. In addition to VMware Products and Suites VMware's Technology Partners' solutions may also be used to provide this goal of ongoing FedRAMP accreditation with the greatest security, agility and cost savings.

For these reasons VMware has enlisted its Audit Partners such as Coalfire, a FedRAMP-approved 3rd Party Assessment Organization (3PAO), to engage in a programmatic approach to evaluate VMware products and solutions for FedRAMP control capabilities and then to document these capabilities into a set of reference architecture documents. The first of these documents in the FedRAMP Reference Architecture set is this document, the Product Applicability Guide, which contains a mapping of the VMware products and features that should be considered for implementing FedRAMP controls. The next two documents in the FedRAMP Reference Architecture set, the Architecture Design Guide and the Validated Reference Architecture, will provide guidance on the key considerations for designing a vCloud environment for FedRAMP, as well as a lab validation exercise analyzing an instance of this reference architecture which utilizes the concepts and approaches outlined therein.

In addition, VMware and Coalfire are engaged with VMware Technology Partners to analyze their products and solutions (available on VMware Solution Exchange) with the goal of providing continuing examples to the industry. In an ongoing effort, VMware and Coalfire will utilize this information to create new "joint" reference architectures based on the VMware Reference Architecture for FedRAMP where partner products and solutions are combined and lab validated to further ease adoption for CIO’s, IT managers, architects, IT auditors and security practitioners involved with a VMware vCloud Suite 5.5 based Cloud Computing Architecture. See Figure 3 in this document for the Compliance Solution Categories.

This study investigated different VMware applications available to organizations that use (or are considering using) virtualization and cloud to support a FedRAMP compliant environment. To that end, Coalfire highlighted the specific FedRAMP requirements these applications (partially) address or should be considered in an evaluation of the initial sourcing of technologies to build a FedRAMP compliant environment. The controls selected for [?] this paper are from the

NIST SP 800-53 Rev3 and the FedRAMP Security Controls Baseline v1.1. It has been reviewed and authored by our staff of FedRAMP auditors in conjunction with VMware.

If you have any comments regarding this whitepaper, we welcome any feedback at vmware@coalfire.com or compliance-solutions@vmware.com.

Introduction

Compliance and security continue to be top concerns for organizations that plan to move any or all of their enterprise-computing environment to the cloud. VMware helps organizations address these challenges by providing bundled solutions (suites) that are designed for specific use cases. These use cases address questions like "How can I be FedRAMP compliant in a VMware supported vCloud hosting environment?" by providing helpful information for VMware architects, the compliance community, and third parties.

The FedRAMP compliant Public Cloud Use Case (See section on Cloud Computing in this document for Cloud Use Cases) is focused on the vCloud Service Provider intending to operate a FedRAMP compliant Public Cloud. Due to the nature of the Public Cloud Use Case this document is primarily concerned with guiding readers in the assembly of VMware components within the 'Provider' layer. This layer is comprised of four VMware Product Suites - vCloud, vCloud Networking and Security (vCNS), vCenter Operations (vCOPs) and NSX. These product suites are described in detail in this paper and in the aforementioned subsequent companion documents. The use case also provides readers with a mapping of the specific FedRAMP controls to VMware's product suite, partner solutions, and organizations involved in FedRAMP compliant cloud services. While every cloud is unique, *VMware and its partners can provide a solution that addresses over 19% of FedRAMP Moderate requirements with 70%?TBD of coverage among technical and operational controls.*

FedRAMP is based on the NIST SP 800-53 Rev3 set of controls (note that Rev4 of these controls is currently available but without corresponding FedRAMP guidance). While this document is intended to provide guidance solely within the Public Cloud Use Case it can also be beneficial to those who seek guidance on building a FISMA Moderate (NIST SP 800-53 Rev3) Private Cloud environment. Another version of the Reference Architecture written specifically for the FISMA Moderate Private Cloud Use Case is expected to be released later in 2014.

Due to the commonalities of the VMware products and features across all of the Cloud Use Cases, understanding their relationship to the seventeen FedRAMP control areas is fundamental and most broadly accommodated in this document with more Use Case specific guidance represented in the Architecture Design Guide. Regardless of the Use Case or operating environment model the FedRAMP control areas represent a broad-based, balanced, information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. The management, operational, and technical controls (i.e., safeguards or countermeasures) are prescribed for an information system in order to protect the confidentiality, integrity, and availability of the system and its information. The operational security controls are implemented and executed primarily by people (as opposed to systems). The management controls focus on the management of risk and the management of information system security. The technical security controls are implemented and executed primarily by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

A comprehensive assessment of the management, operational and technical controls that have been selected for the "information system" is required as part of the authorization process. This assessment must determine the extent to which all selected controls are implemented correctly, operating as intended, and producing desired outcomes with respect to meeting the security requirements for the system. An understanding of both FISMA Moderate and FedRAMP controls as implemented with VMware and its Technology Partners' solutions lends itself to harmonizing the ongoing compliance of the private cloud environment but also the shared responsibility for compliance in the public cloud environment. This common set of well-understood policies and procedures implemented in a common VMware Software Defined Data Center architectures across Private and Public Cloud enables not only the Hybrid Cloud to become reality but opens up tremendous opportunities for tighter control and agility with regard to the principles put forth in the Continuous Diagnostics

and Mitigation program as outlined by Department of Homeland Security and covered in Section # NEED NUMBERED SECTIONS in this document.

Figure 1 FedRAMP Requirements and VMware (need new Graphic with NIST CAPS)

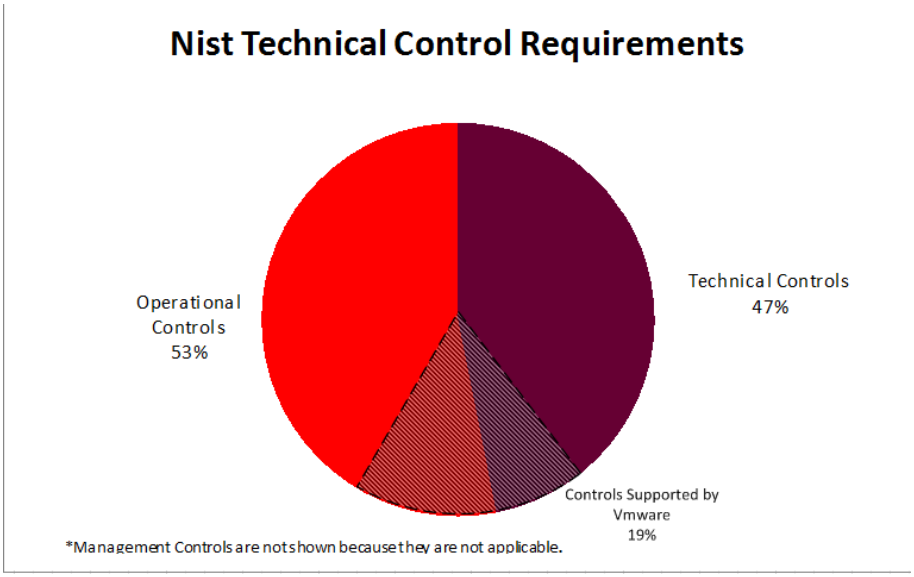


Figure 2: FedRAMP Requirements and Applicable Control Families

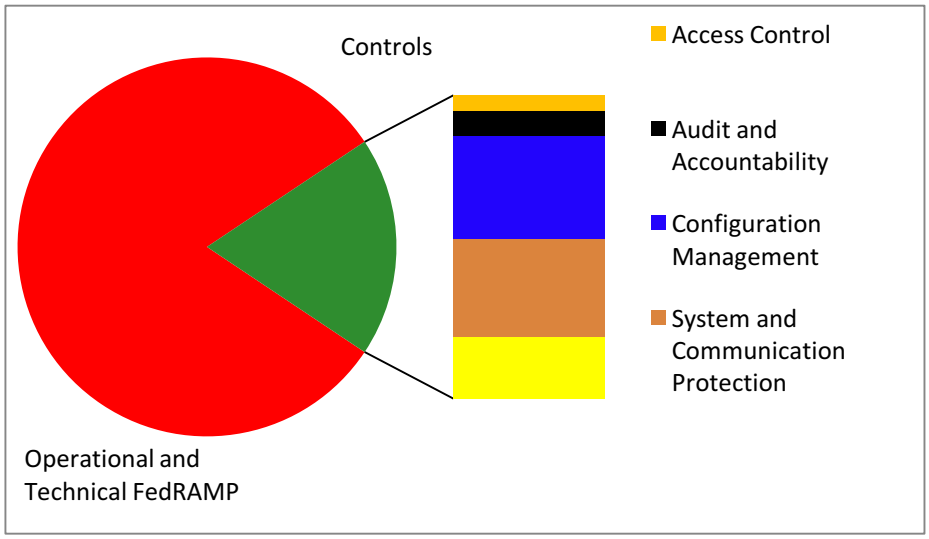
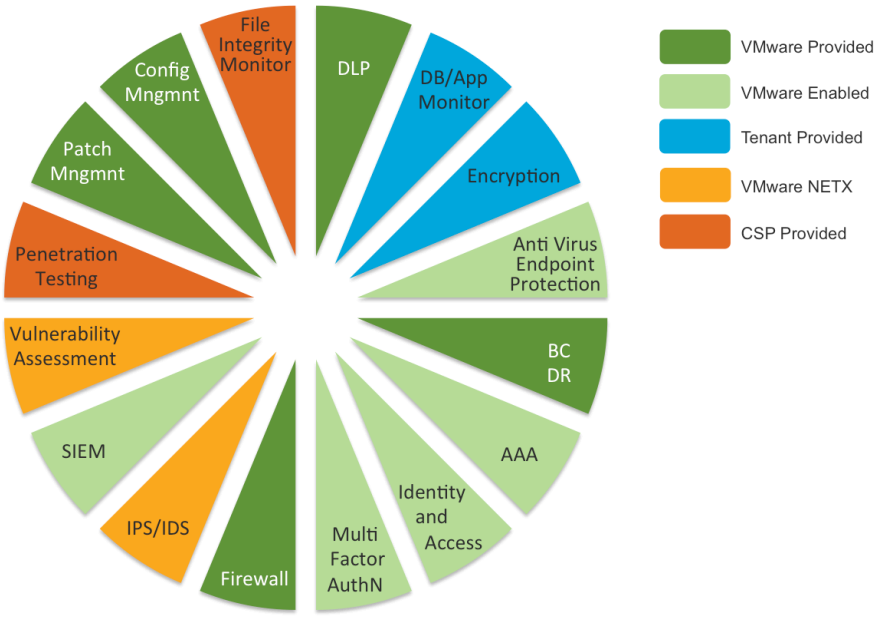


Figure 3: VMware + Partner Product Capabilities for a Trusted Cloud



Official FedRAMP Guidance as it applies to Cloud environments

The Federal Risk Authorization Management Program (FedRAMP) is the result of close collaboration with cybersecurity and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council and its working groups, as well as private industry. The goal is to provide a streamlined process for the security assessment and authorization of commercial cloud services. This process allows a single Provisional Authorization (p-ATO) of the cloud service offering to be leveraged by any federal agency without requiring them to re-assess the hosting infrastructure on a per-system basis.

CSPs must implement the FedRAMP security requirements in their environment and hire a FedRAMP-approved third party assessment organization (3PAO) to perform an independent assessment to audit the cloud system and provide a security assessment package for review. In order to maintain a Provisional Authorization the cloud service provider must implement a continuous monitoring program. This is critical to ensuring the security controls outlined in the NIST SP 800-53 Rev 3 baseline and the additional FedRAMP parameters are effectively implemented.

The FedRAMP security controls baseline is based on the NIST SP 800-53 Rev3 controls that provide detailed Management, Operational and Technical control guidance for meeting the security requirements established by Federal Information System Management Act (FISMA). In addition to the FISMA compliance requirements outlined in the NIST controls baseline, FedRAMP requirements have been written for key controls and control enhancements.

Table 1: FedRAMP Controls Baseline

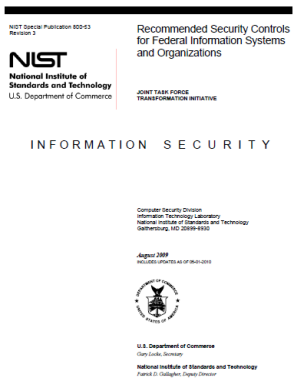
NIST 800-53 rev 3 Control Family Identifiers	NIST 800-53 rev 3 Control Family	Class	FedRAMP Moderate Baseline*
AC	Access Control	Technical	17(24)
AT	Awareness and Training	Operational	4
AU	Audit and Accountability	Technical	12(9)
CA	Certification, Accreditation, and Security Assessment	Management	6(2)
CM	Configuration Management	Operational	9(12)
CP	Contingency Planning	Operational	9(15)
IA	Identification and Authentication	Technical	8(10)
IR	Incident Response	Operational	8(4)
MA	Maintenance	Operational	6(6)
MP	Media Protection	Operational	6(5)
PE	Physical and Environmental Protection	Operational	18(5)
PL	Planning	Management	5
PS	Personnel Security	Operational	8
RA	Risk Assessment	Management	4(5)
SA	System and Services Acquisition	Management	12(7)
SC	System and Communications Protection	Technical	24(16)
SI	System and Information Integrity	Operational	12(9)

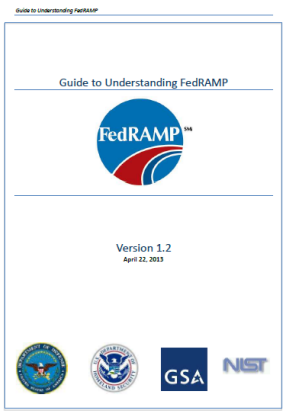
*-The number in parentheses in the last column includes the control enhancements required by the FedRAMP Moderate Baseline

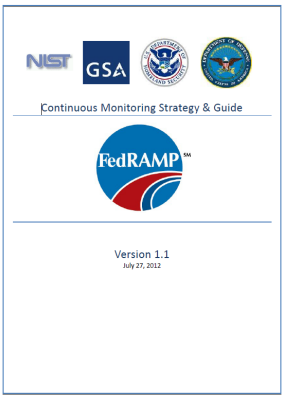
For Cloud Service Providers, deploying and maintaining an infrastructure that meets the requirements established in the NIST and FedRAMP baseline requires centralized management and control of all components including virtual applications, platforms, and network devices.

The Federal Risk Authorization Management Program (FedRAMP) specifically began providing formalized guidance for cloud and virtual environments in June, 2012. These guidelines were based on industry feedback, rapid adoption of virtualization technology, and the move to cloud.

Figure 4: Official guidance on security in FedRAMP Cloud environments







NIST 800-53

The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements levied on information systems and organizations and that is consistent with and complementary to other established information security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.

The NIST 800-53 presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) security control baselines; (iii) the identification and use of common security controls; (iv) security controls in external environments; (v) security control assurance; and (vi) future revisions to the security controls, the control catalog, and baseline controls.

Security controls described in this publication have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into eighteen *families*. Each security control family contains security controls related to the security functionality of the family. In addition, there are three general classes of security controls: management, operational, and technical.

FedRAMP

Cloud computing technology allows the Federal Government to address demand from citizens for better, faster services and to save resources, consolidate services, and improve security. The essential characteristics of cloud computing -- on-demand provisioning, resource pooling, elasticity, network access, and measured services -- provide the capabilities for agencies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services.

Agencies have realized the benefits of this technology and are integrating it into their information technology environment. On December 9, 2010; the Office of Management and Budget (OMB) released the 25 Point Implementation Plan to Reform Federal Information Technology Management, establishing the Cloud First policy and requiring agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. The Federal Risk and Authorization Management Program (FedRAMP) was established by a memorandum issued by OMB on December 8, 2011, Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP Policy Memo) to provide a cost-effective, risk-based approach for the adoption and use of cloud services. A key element to successful implementation of cloud computing is a security program that addresses the specific characteristics of cloud computing and provides the level of security commensurate with specific needs to protect government information. Effective security management must be based on risk management and not only on compliance. By adhering to a standardized set of processes, procedures, and controls, agencies can identify and assess risks and develop strategies to mitigate them.

The purpose of FedRAMP is to:

- Ensure that cloud based services have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies

.

FedRAMP was developed in collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), and the Department of Homeland Security (DHS). Many other government agencies and working groups participated in reviewing and standardizing the controls, policies and procedures.

The major participants in the FedRAMP process are:

- Federal agency customer –has a requirement for cloud technology that will be deployed into its security environment and is responsible for ensuring FedRAMP compliance
- Cloud Service Provider (CSP) –is willing and able to fulfill agency requirements and to meet security requirements
- Joint Authorization Board (JAB) –reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO)
- 3rd Party Assessor Organization (3PAO) –validates and attests to the quality and compliance of the CSP provided security package
- FedRAMP Program Management Office (PMO) –manages the process assessment, authorization, and continuous monitoring process

A CSP follows the process for a provisional authorization under FedRAMP and uses a 3PAO to assess and review its security control implementations. CSPs then provide documentation of the test results in a completed assessment package to the FedRAMP PMO. The security package is then reviewed by the JAB and if a CSP system presents an acceptable level of risk, a provisional Authorization is granted. Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments.

FedRAMP Continuous Monitoring Strategy & Guide

FedRAMP assessment process requires that monitoring activities be conducted continuously, quarterly, annually, every three years and every five years. These activities include required activities from the CSP and required activities of a 3PAO. The continuous monitoring program under FedRAMP is designed to provide more transparency into the ongoing security posture of the authorized cloud environment or service environment is acceptable.

The OMB memorandum M-10-15, issued on April 21, 2010, changed from static point-in-time security authorization processes to Ongoing Assessment and Authorization throughout the system development life cycle. Consistent with this new direction favored by OMB and supported in NIST guidelines, FedRAMP has developed an ongoing assessment and authorization program *"Continuous Monitoring Strategy & Guide"* for the purpose of reauthorizing Cloud Service Providers (CSP) annually. Traditionally, this process has been referred to as "Continuous Monitoring" as noted in NIST SP 800-137 *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to "ongoing assessment of security controls". It is important to note that both the terms "Continuous Monitoring" and "Ongoing Security Assessments" mean essentially the same thing and should be interpreted as such.

Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain their FedRAMP Provisional Authorization. After a system receives a FedRAMP Provisional Authorization, it is possible that the security posture of the system could change over time due to changes in the hardware or software on the cloud service offering, or also due to the discovery and provocation of new exploits. Performing ongoing security assessments determines whether the set of deployed security controls in an information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. Ongoing assessment and authorization provides federal agencies using cloud services a method of detecting changes to the security posture of a system for the purpose of making risk-based decisions. . Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows agencies to make informed risk management decisions as they use cloud services. To receive reauthorization of a FedRAMP Provisional Authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

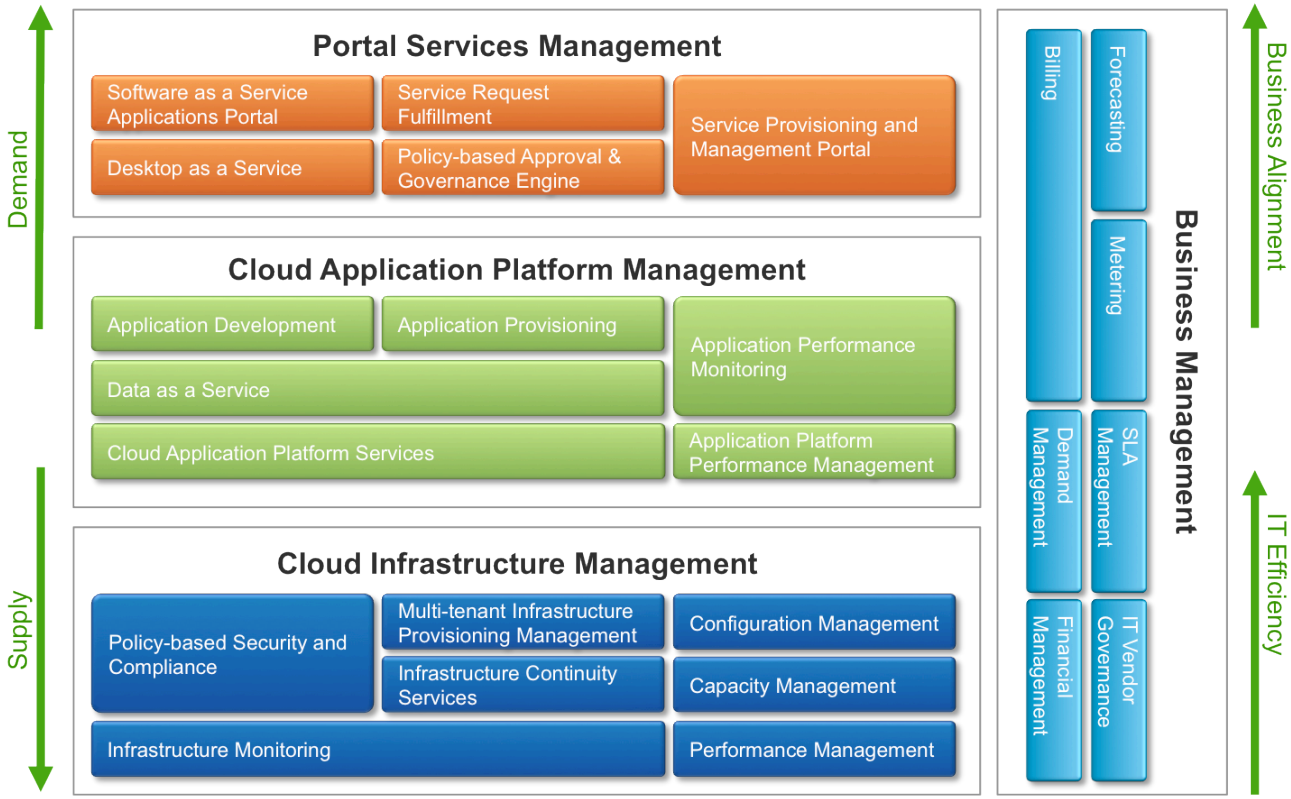
FedRAMP Continuous Monitoring Strategy & Guide is intended to provide CSPs with guidance and instructions on how to implement their continuous monitoring program. Certain deliverables and artifacts related to continuous monitoring that FedRAMP requires from CSP's are discussed in this document.

Cloud Computing

Cloud computing and virtualization have continued to grow significantly every year. There is a rush to move applications and even whole datacenters to the "cloud", although few people can succinctly define the term "cloud computing." There are a variety of different frameworks available to define the cloud, and their definitions are important as they serve as the basis for making business, security, and audit determinations. VMware defines cloud or utility computing as the following (http://www.vmware.com/solutions/cloud-computing/public-cloud/faqs.html):

"Cloud computing is an approach to computing that leverages the efficient pooling of on-demand, self-managed virtual infrastructure, consumed as a service. Sometimes known as utility computing, clouds provide a set of typically virtualized computers which can provide users with the ability to start and stop servers or use compute cycles only when needed, often paying only upon usage.."

Figure 5: Cloud Computing



There are commonly accepted definitions for the cloud computing deployment models and there are several generally accepted service models. These definitions are listed below:

- Private Cloud – The cloud infrastructure is operated solely for an organization and may be managed by the organization or a third party. The cloud infrastructure may be on premise or off-premise.
- Public Cloud – The cloud infrastructure is made available to the general public or to a large industry group and is owned by an organization that sells cloud services.
- Hybrid Cloud – The cloud infrastructure is a composition of two or more clouds (private and public) that remain unique entities, but are bound together by standardized technology. This enables data and application

portability; for example, cloud bursting for load balancing between clouds. With a hybrid cloud, an organization gets the best of both worlds, gaining the ability to burst into the public cloud when needed while maintaining critical assets on premise.

- Community Cloud – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

To learn more about VMware's approach to cloud computing, review the following:

- VMware Cloud Computing Overview
- VMware's vCloud Architecture Toolkit

When an organization is considering the potential impact of cloud computing to its highly regulated and critical applications, it may want to start by asking:

- Is the architecture a true cloud environment (does it meet the definition of cloud)?
- What service model is used for the cardholder data environment (SaaS, PaaS, IaaS)?
- What deployment model will be adopted?
- Is the cloud platform a trusted platform?

The last point is critical when considering moving highly regulated applications to a cloud platform FedRAMP does not endorse or prohibit any specific service and deployment model. The appropriate choice of service and deployment models should be driven by customer requirements, and the customer's choice should include a cloud solution that is implemented using a trusted platform.

VMware is the market leader in virtualization, the key enabling technology for cloud computing. VMware's vCloud Suite 5.5 is the trusted cloud platform that customers use to realize the many benefits of cloud computing including safely deploying business critical applications.

If you are an organization or partner that is interested in more information on the VMware Compliance Program, please email us at compliance-solutions@vmware.com

Where to Start - Considerations for System Owners, IT and Assessors

Migrating a traditional IT infrastructure to a virtual or cloud environment has a significant impact on an organization that extends beyond information technology. Security and compliance continue to remain top concerns for management, IT departments, and auditors. All three areas should be represented and engaged for any IT virtualization or cloud projects to confirm that business, IT operations, and compliance teams carefully consider the benefits and risks.
The following questions may be important when considering the potential business impact, benefits, and risks of a virtual and/or cloud environment.

IT Considerations

1. How does the IT Operations plan address the company's strategic and operational goals?
2. What manual processes are in place that can be automated?
3. What are the skills and capabilities of the IT Department?
4. Have there been any previous attempts to virtualize or outsource critical operations?
5. Which IT initiatives currently underway could impact the FedRAMP system boundary?
6. How is encryption currently used to limit risk?
7. How is sensitive data currently classified (i.e., do you know where all your data resides)?
8. How has security and compliance affected IT Operations?

Assessment Considerations

1. What prior experience does the auditor have with virtual/cloud environments (Third Party Assessment Organization (3PAO))?
2. Has the 3PAO successfully assessed FedRAMP environments?
3. What certifications do they have in VMware products or solutions?
4. How many individuals that are part of the assessment team have experience with VMware?
5. What thought leadership and guidance has the 3PAO published?
6. What are the risks and mitigation techniques the 3PAO believes are appropriate for FedRAMP environments?
7. How long have they been working with VMware architectures?
8. What references do they have for conducting similar assessments?
9. Is the 3PAO assigned to the audit engagement company knowledgeable about the basic components, systems, and software in a VMware cloud?

Guidance from the Federal Risk Authorization Management Program

VMware has identified the FedRAMP controls that highlight some of the critical requirements/guidance that organizations are required to address as part of their deployments. VMware has also provided information regarding how VMware tools are designed to help organizations address these controls.

Cloud computing technology allows the Federal Government to address demand from citizens for better, faster services and to save resources, consolidate services, and improve security. The essential characteristics of cloud computing -- on-demand provisioning, resource pooling, elasticity, network access, and measured services -- provide the capabilities for agencies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services.

Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments. In prior cloud FISMA compliance projects, certain controls have proven to be challenging for service providers to meet. Before you decide to initiate a request to participate in FedRAMP, go through the checklist in Table 3-1 link?and make sure that you are truly able to meet these requirements. Consult with your legal team and technical staff (e.g. systems administrators, database administrators, network engineers etc.) to determine if you have the right controls in place and have the ability to manage them.

Checklist for CSPs getting ready for to undergo the FedRAMP process

1. You have the ability to process electronic discovery and litigation holds
2. You have the ability to clearly define and describe your system boundaries
3. Guide to Understanding FedRAMP
4. You can identify customer responsibilities and what they must do to implement controls
5. System provides identification & 2-factor authentication for network access to privileged accounts
6. System provides identification & 2-factor authentication for network access to non-privileged accounts
7. System provides identification & 2-factor authentication for local access to privileged accounts
8. You can perform code analysis scans for code written in-house (non-COTS products)
9. You have boundary protections with logical and physical isolation of assets
10. You have the ability to remediate high risk issues within 30 days, medium risk within 90 days
11. You can provide an inventory and configuration build standards for all devices
12. System has safeguards to prevent unauthorized information transfer via shared resources
13. Cryptographic safeguards preserve confidentiality and integrity of data during transmission

VMware products and FedRAMP

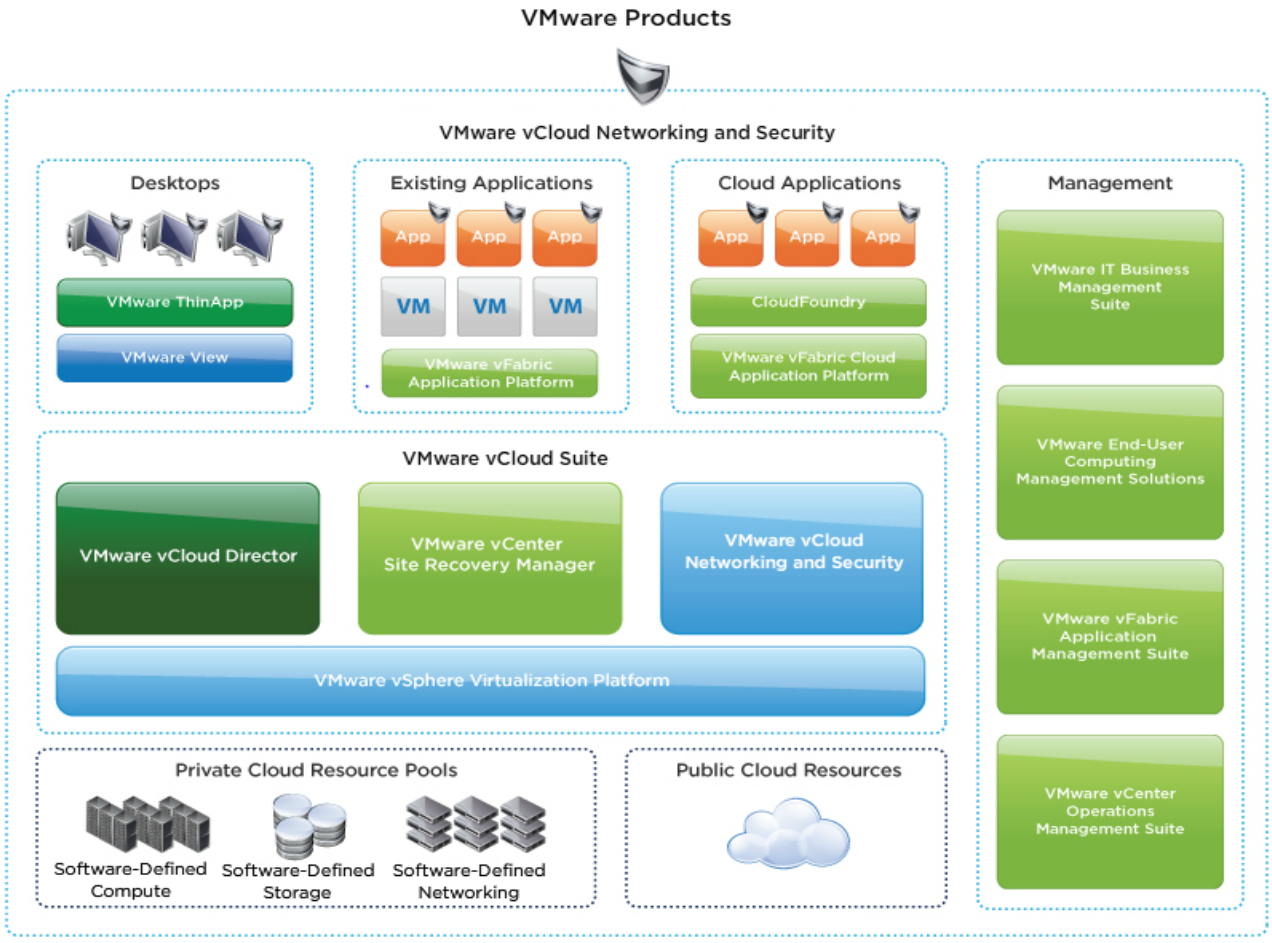
VMware provides an extensive suite of products designed to help organizations support security and compliance needs. While every environment has unique needs, the following FedRAMP Compliance Stack provides a comprehensive mix of VMware solutions with features that are designed to assist with FedRAMP compliance. The solutions' functionality, features, and specific NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 requirements are addressed in detail in the following sections.

VMWARE PRODUCTS	Product Components or Features
vCloud Suite 5.5	vSphere includng: ESXi, vShield Endpoint, vCenter, vCenter Update Manager, vCenter Orchestrator, vMotion, Storage vMotion, High Availability, Data Protection and Replication, Host Profiles vCloud Director including: Elastic Virtual Datacenters, Multi-Tenancy and Service Catalog
vCloud Networking and Security Suite 5.5	Edge, App Firewall, VXLAN, and Data Security
vCenter Operations Management Suite 5.8	VMware vCenter Operations Manager™, VMware vCenter Configuration Manager™, VMware vFabric™ Hyperic®, VMware vCenter Infrastructure Navigator™, and VMware vCenter Chargeback Manager™
NSX 6.0	Logical Switching, Logical Routing, Logical Firewall, VXLAN, NSX 6.0 Edge Gateway (Load Balancing, DHCP, VPN), NSX 6.0 API

To determine the products and features available with VMware Suites please refer to VMware.com:

vCloud Suite 5.5 vCloud Networking and Security Suite 5.5 , vCenter Operations Management Suite 6.0, NSX 6.0

Figure 6: VMware Products Suite Need a New Graphic here with NSX could be a Figure 7 with NSX



VMware FedRAMP Requirements Matrix (Overview)

VMware has created a FedRAMP Requirements Matrix to assist organizations with an understanding of VMware solutions, VMware Partner solutions (where they overlap), and the remaining customer responsibilities that must be addressed separately by the customer through use of other tools or processes. While every cloud is unique, VMware believes that the vast majority of NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 requirements can be addressed through the VMware Suites and/or VMware partner solutions.

The following diagram shows an example of a cloud environment that has been deployed using the VMware FedRAMP suites and VMware partner products.

The remaining gaps in addressing FedRAMP requirements may be filled by the customer through other tools (i.e. approving customers' policies, keeping an updated network diagram, approving changes, etc.)

Figure 7: FedRAMP Requirements and VMware Same as Figure 1? Need NIST CAPS graphic

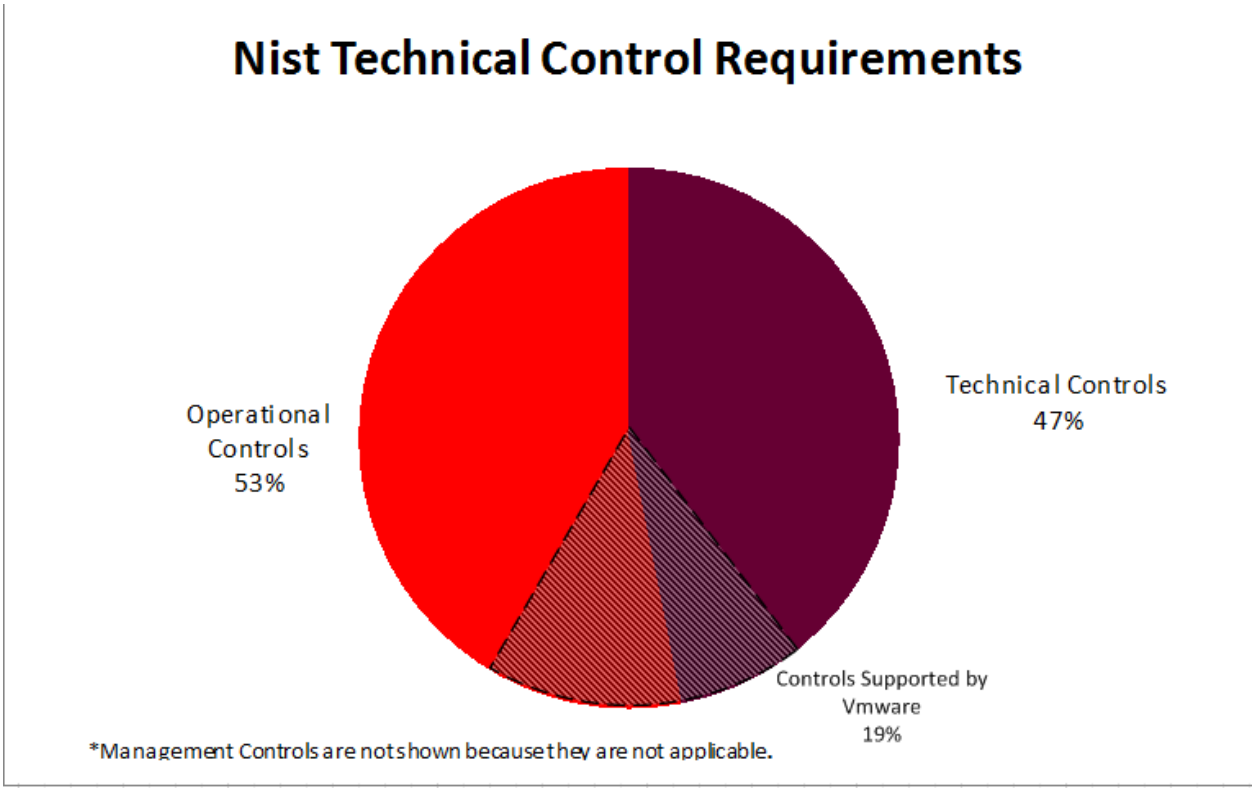


Table 2: NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 Requirements

PIE CHART	NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 REQUIREMENT	# OF FEDRAMP ASSESSMENT TESTS	TESTS ADDRESSED IN VMWARE'S SUITES	??
	Access Control	41	3	38
	Awareness and Training	4	0	4
	Audit and Accountability	21	5	16
	Security Assessment and Authorization	8	0	8
	Configuration Management	21	20	1
	Contingency Planning	24	0	24
	Identification and Authentication	18	0	18
	Incident Response	12	0	12
	Maintenance	12	0	12
	Media Protection	11	0	11
	Physical and Environmental Protection	23	0	23
	Planning	5	0	5
	Personnel Security	8	0	8
	Risk Assessment	9	0	9
	System and Services Acquisition	19	0	19
	System and Communication Protection	40	19	21
	System and Information Integrity	21	12	9
	**TOTAL** **Note: Control totals do not add up to 298 due to overlapping features of VMware products and partner products**	**297**	**59**	**238**

FedRAMP Requirements Matrix (By VMware Suite)

vCloud Suite 5.5

For the purposes of the VMware Applicability Guide for FedRAMP, the vCloud Suite 5.5 includes vSphere (ESXi, vCenter Server), vCenter Orchestrator, vCenter Update Manager and vCloud Director. vSphere provides the foundation of the virtual architecture allowing for the optimization of IT assets. vCloud Director extends the foundation of the vSphere virtual architecture by enabling organizations to build secure clouds and optimizing security and compliance in private, multi-tenant, mixed-mode, and hybrid clouds. As vCloud leverages the vSphere architecture, the vSphere components integrate to create a single vCloud that can be optimized for security and compliance considerations. While it encompasses many features for storage, business continuity, and automation; for the purposes of this FedRAMP reference architecture, the critical components that apply to FedRAMP for vCloud include the following six components – ESXi Hosts, vShield Endpoint, vCenter Server, vCenter Orchestrator, vCenter Update Manager and vCloud Director.

- **ESXi** – ESXi is a type 1 hypervisor (bare metal) that is significantly different than the ESX architecture and offers improvements in security. The ESXi kernel has a small footprint, no service console and can limit communication to vCenter access only. This FedRAMP reference architecture is only applicable to ESXi architectures because the ESXi architecture and the ESX architectures are quite different.

- **vShield Endpoint -** With integration of other 3rd party endpoint solutions (such as anti-virus), vShield Endpoint improves the performance by offloading key antivirus and anti-malware functions to a secured virtual machine and eliminating the antivirus agent footprint and overhead in virtual machines.

- **vCenter Server**—vCenter Server is a server (virtual or physical) that provides unified management for the entire virtual infrastructure and unlocks many key vSphere capabilities. vCenter Server can manage thousands of virtual machines across multiple locations and streamlines administration with features such as rapid provisioning and automated policy enforcement.

- **vCenter Orchestrator** (vCO) – vCO is a virtual appliance that automates tasks for VMware vSphere and enables orchestration between multiple solutions. VMware vCenter Orchestrator allows administrators to automatically create workflows that capture best practices and manual workflows and creates automated, repeatable solutions.

- **vCenter Update Manager** (vUM) – vUM automates tracking, patching and updating for vSphere hosts (ESXi hosts and clusters), VMtools, and VMware virtual appliances. It provides a centralized, automated, actionable patch compliance management solution to confirm that all VMware components are updated and to enforce the latest security patches.

- **vCloud Director (vCD)** - vCD Pools datacenter resources including compute, storage and network, along with their relevant policies into virtual data centers. Fully encapsulated multi-tier virtual machine services are delivered as vApps, using the Open Virtualization Format (OVF). End users and their associated policies are captured in organizations. With programmatic and policy-based pooling of infrastructure, users and services, VMware vCloud Director enforces policies, which enable FedRAMP data to be securely protected, and new virtual machines and applications to be securely provisioned and maintained.

The following product matrix explains which FedRAMP controls are applicable to vCloud Suite 5.5. It also explains how vCloud Suite enables users to meet FedRAMP requirements. The controls highlighted in **Bold** are those that have been selected for the FedRAMP Baseline.

Table 3: Applicability of FedRAMP Controls to vCloud Suite 5.5

NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 V2.0 APPLICABILITY MATRIX		
NIST 800-53 CONTROL FAMILY	**CONTROLS ADDRESSED**	**VCLOUD SUITE 5.5 DESCRIPTION**
Access Control	AC-5, AC-6,	The vCloud Suite 5.5 can be configured to limit access to the Customer environments through a variety of ways. By providing a centralized interface, vSphere Client and vCenter servers can reduce the Customer environments by minimizing the network management and limiting access to critical components in the Customer environments. For example, the vSphere environment allows users to lock down each ESXi server so that it can only be accessed via the vCenter server. vCO can also be used to automate and enforce standardized rules, accounts, profiles, and security settings in order that scope is not impacted as new machines are dynamically added or removed. Additionally, direct access to components can be reduced (such as lock-down mode) to minimize the risk of any direct console or shell access. Integrating into vSphere components such as vUM, Clouds using the vCloud Director environment can be used to push out critical security updates to allow the latest security configurations to be enforced. Hardening guidelines have been developed specifically for the Cloud environment. vCloud and vSphere have built in access control systems in place so that each virtual component can only be accessed by authorized users. Systems can be accessed directly with local accounts, or can be managed centrally through a role based access control systems enforced by vSphere and integrated into centralized access control system. All access to virtual devices within the vCloud and vSphere environment can enforce individual access. Minimum usernames and password requirements can be set on many systems natively (such as the ESXi host). Other virtual components can be configured to use centralized authentication servers (such as Active Directory) which can enforce additional controls for password rotation, lockout, duration etc.
Audit and Accountability	AU-2, AU-3, AU-6 (1), AU-8, AU-12,	vCloud and vSphere has the ability to log access to components within the environment. Individual access to components can be tracked, logged, and enforced. Audit trails can capture event, time, action, and other critical requirements that are required for monitoring. Logs can be centrally consolidated, reviewed, and retained for analysis. All systems can be configured with time synchronization, normally by enforcing primary and secondary NTP servers in the cloud environment.
System and Communications Protection	SC-4, SC-6, SC-7, SC-30	The vCenter Orchestrator (vCO) can be used to configure new virtual components to communicate only within the environment in which they were intended. vCO can reduce the manual configuration processes which are prone to user error and misconfiguration in a large, dynamic environment.

vCloud Networking and Security Suite 5.5

For the purposes of the VMware Applicability Guide for FedRAMP, the suite is a group of products that deliver a virtualized security model specifically designed to overcome the traditional challenges of managing security in a virtual environment. vCloud Networking and Security provides a software based approach to application and data security in virtual and cloud environments, which have traditionally been enforced primarily through physical security appliances. The vCloud Networking and Security Suite 5.5 consists of the following five (5) products:

- **App Firewall?**
  Protects applications in a virtual datacenter against network-based threats by providing a firewall that is hypervisor-based and application-aware. vCloud Networking and Security App has visibility of intra-VM communication, and enforces policies, firewall rules based on logical groups, and workloads.

- **Data Leak Prevention**
  Adds to Sensitive Data Discovery across virtualized resources allowing the organizations to identify and secure different types of sensitive data. For FedRAMP, it provides a way to search for cardholder data and to identify hosts and unauthorized stores of data.

- **Edge Gateway**
  Enhances protection of a virtual datacenter perimeter by providing gateway security services including careful inspection firewall, site-to-site VPN, load balancing, Dynamic Host Configuration Protocol (DHCP), and Network Address Translation (NAT). It also has the ability to integrate with third-party IDS solutions.

- **Manager**
  Manager is a management application, which includes all vCloud Networking and Security products. Manager is tightly integrated with vCenter and the broader VMware management portfolio.

The following product matrix explains which FedRAMP controls are applicable to the vCloud Networking and Security Suite 5.5. It also explains how vCloud Networking and Security assists users in meeting FedRAMP requirements. The controls highlighted in **Bold** are those that have been selected for the FedRAMP Baseline.

Table 4: NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 v2.0 Applicability Matrix

NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 V2.0 APPLICABILITY MATRIX		
NIST 800-53 CONTROL FAMILY	**CONTROLS ADDRESSED**	**VCNS SUITE DESCRIPTION**
Access Control	AC-05, AC-6	vCloud Networking and Security has built in access control systems in place so that each virtual component can only be accessed by authorized users. Systems can be accessed directly with local accounts, or can be managed centrally through a role based access control systems enforced by vSphere and integrated into centralized access control system. vCloud Networking and Security supports authentication based on job classification and function (RBAC), and can be configured to require that only the appropriate administrators and support personnel have access to vCloud Networking and Security components and operations. Manager provides a centralized solution to manage and enforce security profiles across a large distributed environment.
Audit and Accountability	AU-2, AU-3, **AU-6 (1)**, AU-8, AU-12	vCloud Networking and Security App and Edge Gateway have the ability to log access to components within the virtual environment using Syslog. Individual access to components can be tracked, logged, and enforced. Audit trails can capture event, time, action, and other critical requirements required for monitoring. Logs can be centrally consolidated, reviewed, and retained for analysis. All systems can be configured with time synchronization, normally by enforcing primary and secondary NTP servers in the vSphere environment.
System and Communications Protection	SC-4, SC-6, SC-7, SC-7(3)(4)(5)(6)(7)(8)(12)(13)(18), SC-8, SC-8(1), SC-11, SC-13, SC-13(1), SC-30, SC-32	vCloud Networking and Security Manager provides centralized management and can be used to enforce the approval process for changes to network connections. Edge Gateway and App can control how cardholder data flows over a network, and Data Leak Prevention can be used to monitor that those controls are operating effectively. Roles and responsibilities for management can be enforced and defined in Manager and integrated into other RBAC solutions. Edge Gateway can be used as a firewall to separate wireless networks from the virtual infrastructure. Both Edge Gateway and App perform stateful inspection (dynamic filtering). App and Edge Gateway also support comment fields, which can used to document the justification for every open port and service. Manager can be used to view current configurations and allow an administrator to compare it to an approved configuration; This facilitates confirmation that running configurations files for App and Edge Gateway are secured and match the approved configurations. vCloud Networking and Security can provide segmentation for Cloud environments by segmenting virtual machines, port groups, and enforcing perimeter security. Edge gateway provides gateway security services including a stateful inspection firewall, which protects the network from traffic into and out of the virtualized infrastructure. App provides visibility and control for intra-VM communication. Data Leak Prevention can be used to proactively search and identify stores of credit card data and gather data to validate or enforce segmentation.

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

vCenter Operations Management Suite 5.8

For the purpose of the VMware Applicability Guide for FedRAMP, the "vCenter Operations Management Suite 6.0" includes vCenter Operations Manager, vCenter Configuration Manager, vCenter Infrastructure, and vCenter Infrastructure Navigator. The vCenter Operations Management Suite 6.0 enables IT organizations to gain better visibility and actionable intelligence to proactively facilitate service levels, optimum resource usage, and configuration compliance in dynamic virtual and cloud environments.

- **vCenter Operations Manager (vCOPs)** – Uses patented analytics and integrated approach to operations management in order to provide the intelligence and visibility required to proactively maintain service levels, optimum resource usage, and configuration compliance in dynamic virtual and cloud environments.

- **vCenter Configuration Manager** (vCM) – Automates configuration management across virtual and physical servers and desktops, increasing efficiency by eliminating manual, error-prone, and time-consuming work. This enables enterprises to maintain continuous compliance by detecting changes and comparing them to configuration and security policies.

Description of vCenter Infrastructure?

- **vCenter Infrastructure Navigator** – Automatically discovers and visualizes application and infrastructure dependencies. It provides visibility into the application services running over the virtual-machine infrastructure and their interrelationships for day-to-day operational management.

The following product matrix explains which FedRAMP controls are applicable to the vCenter Operations Management (vCOPs) Suite. The following is the detailed description of the controls that may be met through the Suite. The controls highlighted in **Bold** are those that have been selected for the FedRAMP Baseline.

We need to make sure there is vCOps vCloud Connector content for mapping of vCloud Layers to vApps as well as Infrastructure Navigator capabilities to map the application software

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

Table 5: NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 v2.0 Applicability Matrix

NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 V2.0 APPLICABILITY MATRIX		
NIST 800-53 CONTROL FAMILY	**CONTROLS ADDRESSED**	**DESCRIPTION**
Access Control	AC-5, AC-6	Access to vCOPs can be controlled through Microsoft Active Directory. This will allow vCOPs to help the user meet the FedRAMP requirements for access control to the Customer environment.
Audit and Accountability	AU-2, AU-3, **AU-6 (1)**, AU-8, AU-12	vCOPs has the ability to monitor access controls to the Customer environment and thereby monitor compliance with FedRAMP requirements. Specifically, vCOPs will assess and report on the following: - Local and domain-level users (Windows) and users with unique usernames (UNIX, Linux and MAC OS). - System password policies for expiration, length, standards, creation settings, access attempts, (can also remediate) - Changes to user accounts, credential stores, and identifier objects to provide visibility and control over system access - User access across all the systems in the datacenter at once - Disable and remove access for terminated user accounts - Inactive accounts (which it can also disable and remove access for these user accounts) - The status of maintenance accounts and to confirm that they are disabled and configured to only be used during the times specified. - Login policies, to include lockout settings and auto-logout settings, and remediating as needed. Assessment, reporting and remediation are conducted in accordance with scheduling through vCOPs. vCOPs will assess, report and remediate the following: - Configurations of the system auditing and logging services to support proper logging across system components. - vCM collects audit log entries to provide a single view of events. - User access audit trails by ensuring proper permissions for log files and their directories and alert on changes to critical audit trails. vCOPs has the ability to track system changes across thousands of data points and, in conjunction with native auditing, can be used to track account activity and system modifications. vCOPs can assess and report on Syslog configuration details on Unix and Linux systems that specify remote log servers within the network. vCOPs can be also used to assess, report, and remediate audit logging for VMware components and guest operating systems. Changes within the virtual environment are captured by vCOPs and can be displayed in vCM. vCM can

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

NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 V2.0 APPLICABILITY MATRIX		
NIST 800-53 CONTROL FAMILY	**CONTROLS ADDRESSED**	**DESCRIPTION**
		collect audit log entries within an organization vDC to allow an organization a single view of events within their environment. vCM is also able to control user access to audit trails within an organization by providing proper permissions for log files and their directories.
Configuration Management	CM-2**, CM-2**(1)(3)(**5**), CM-3, CM-4(2), CM-5, **CM-5(1**)(2)(6), CM-6, **CM-6(1**)(3), CM-7, CM-7(1)(3), CM-8, **CM-8** (1)(**3**)(5)	Security hardening and the enforcement of configuration standards are difficult in any environment and have historically relied on manual processes. The vCOPs suite has the ability to assess both physical and virtual machines in the Cloud Computing Architecture and report their compliance with a variety of configuration concerns. vCOPs has the ability to consistently check the compliance status of machines within the environment critical for the configuration management and hardening of systems. Items such as default system settings, system security hardening and base-lining, un-provision and unapproved software or services, and report unnecessary functions from systems. vCOPs allows the customer to customize any number of compliance templates created to meet regulatory and best practices standards including, but not limited to CIS, ISO-27001/27002, SANS and NIST. This function will allow for the simple baseline of standards and security configuration. vCOPs with vCM is able to assess, download, and deploy patches to Windows, Unix, Linux, and MAC operating systems. Assessments are customizable and can be set to verify critical patches in the past 30 days. Changes within the virtual environment are captured by vCOPs and can be displayed in vCM. Each change made to the configuration settings is documented and logged. If a change is made without the proper approval it is alerted with a simple roll back procedure and the change is reversed. vCOPs are able to track changes both made through the standard change process or out of band changes conducted directly on the VMs or through another tool. vCM configured to use the “VMware vCloud 5.5 Hardening Guide” template to report on configuration settings in the virtual environment, as well as the reporting results for a clean scan of the environment with all appropriate configurations correctly applied.
System and Information Integrity	SI-2, SI-3, SI-3(1)(2)(3), SI-4, SI-4(2)(4)(5), **SI-6,** SI-7, SI-7(1)	vCOPs can perform file integrity monitoring (FIM) within the Cloud Computing Architecture for critical files and/or directories. Alerts can also be established to alert personnel of any changes made or attempted and even remediate as needed. vCOPs does not have a built in anti-virus solution, but it can be used to asses and report the anti-virus state of the systems. This allows a determination that all systems have anti-virus software installed and running with the updated signature files. vCOPs can remediate anti-virus problems by installing the customer approved anti-virus software on systems where it is not installed starting/enabling the software services.

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

VMware NSX Suite 6.0 Need information clarifying features vs. products. Should Service Composer be listed?

For the purposes of the VMware Applicability Guide for FedRAMP, the NSX 6.0 suite of products includes Logical Switching, Logical Routing, Logical Firewall, Logical Load Balancer, NSX 6.0 API, NSX 6.0 Gateway, and Logical VPN. The VMware network virtualization solution addresses current challenges with physical network infrastructure and brings flexibility, agility and scale through VXLAN-based logical networks. Along with the ability to create on-demand logical networks using VXLAN, the vCloud Networking and Security Edge gateway helps users deploy various logical network services such as firewall, DHCP, NAT and load balancing on these networks. This is possible due to its ability to decouple the virtual network from the physical network and then reproduce the properties and services in the virtual environment.

- **Logical Switching**
  The logical switching capability in the NSX 6.0 platform provides customers the ability to spin up isolated logical L2 networks with the same flexibility and agility, as it is to spin up virtual machines. there are three main components that help decouple the underline physical network fabric and provide network abstraction, NSX 6.0 Manager, Controller Cluster, User World Agent and VXLAN Tunnel Endpoint.

- **Logical Routing**
  There are two modes of routing supported in the NSX 6.0 platform Distributed Routing and Centralized Routing. The distributed routing capability in the NSX 6.0 platform provides an optimized and scalable way of handling East - West traffic within a data center. There are multiple components for the logical routing; NSX 6.0 Manager, Logical Router Control VM, Logical Router Kernel Module, Controller Cluster, NSX 6.0 Edge Services Router, Routing Deployments, Physical Router as Next Hop, Edge Services as Next Hop, and a Scalable Topology.

- **Logical Firewall**
  The VMware NSX 6.0 platform includes distributed kernel enabled firewalling with line rate performance, virtualization and identity aware with activity monitoring, among other network security features native to network virtualization such as Network Isolation and Segmentation.

- **Logical Load Balancer**
  This service offers distribution workload across multiple servers, as well as high-availability of applications. The NSX 6.0 load balancing service is specially designed for cloud with fully programmable via API and same single central point of management/monitoring as other NSX 6.0 network services.

- **NSX 6.0 API**
  The API interface of the NSX 6.0 manager helps automate deployment and management of logical routers and switches through a Cloud management platform.

- **NSX 6.0 Gateway**
  The gateway is a virtual appliance that performs Logical routing functions. NSX 6.0 Edge services router provides the traditional centralized routing support in the NSX 6.0 platform. Along with the routing services NSX 6.0 Edge also supports other network services that include DHCP, NAT, Load balancing etc.

The following product matrix explains which FedRAMP controls are applicable to the NSX Suite 6.0. It also explains how NSX Suite assists users in meeting FedRAMP requirements. The controls highlighted in **Bold** are those that have been selected for the FedRAMP Baseline.

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

Table 6: NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 v2.0 Applicability Matrix Need More Service Composer

NIST 800-53 REV3 AND FEDRAMP BASELINE CONTROLS V1.1 V2.0 APPLICABILITY MATRIX		
NIST 800-53 CONTROL FAMILY	**CONTROLS ADDRESSED**	**VMWARE NSX 6.0 DESCRIPTION**
Access Control	AC-04	VMware NSX 6.0 allows for pre-defined network rules and policies enabling more effective information flow enforcement at the network layer.
Configuration Management	CM-2**, CM-2**(1)(3)(**5**), CM-3, CM-4(2), CM-5, **CM-5(1**)(2)(6), CM-6, **CM-6(1**)(3), CM-7, CM-7(1)(3), CM-8, **CM-8** (1)(**3**)(5)	NSX 6.0 network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The virtualization of networking services and devices such as Layer 2 switching, L3 routing, load balancing and firewall services, allows Cloud Service Provides to create compliant baseline configurations of networking services and architecture and maintain them under configuration control. These can then be deployed to federal agency customers without the risk of misconfiguration or lengthy replication of effort in provisioning network services.
System and Communications Protection	SC-4, SC-5**, SC-6**, SC-7, **SC-7**(3)(4)(5)(6)(7)(**8**) (**12**)(**13**)(**18**), **SC-11**, SC-13, **SC-13(1**), SC-14, SC-19	Network virtualization through NSX 6.0 allows for pre-defined Layer 2 to Layer 7 services. This adds an additional layer of separation within multi-tenant hosting services and most importantly reduces the risk of misconfiguration of network services and potential exposure of sensitive information and data to unauthorized networks or personnel. NSX 6.0 provides Load Balancing as a service within the networking suite. This service enables workload distribution across physical servers as well as dynamic scalability for high bandwidth. VMware NSX 6.0 Network Virtualization suite provides the following services which can be configured to support boundary protection, network segmentation and trusted patch requirements for federal customers: • **Logical Layer 2** – Enabling extension of a L2 segment / IP Subnet anywhere in the fabric irrespective of the physical network design. • **Distributed L3 Routing** – Routing between IP subnets can be done in a logical space without traffic going out to the physical router. This routing is performed in the hypervisor kernel with a minimal CPU / memory overhead. This functionality provides an optimal data-path for routing traffic within the virtual infrastructure. Similarly the NSX 6.0 Edge provides a mechanism to do full dynamic route peering using OSPF, BGP, IS-IS with the physical network to enable seamless integration. • **Distributed Firewall** – Security enforcement is done at the kernel and VNIC level itself. This enables firewall rule enforcement in a highly scalable manner without creating bottlenecks onto physical appliances. The firewall is distributed in kernel and hence has minimal CPU overhead and can perform at line-rate. • **Logical Load-balancing** – Support for L4-L7 load balancing with ability to do SSL termination. • SSL VPN services to enable L2 VPN services.
System and Information Integrity	**SI-6,**	Virtualization of the network layers devices and services provides the ability to monitor and enforce pre-defined architecture including virtual network devices and services. In the event of a security functionality failure, NSX 6.0 network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks.

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

Disclaimer:

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of competent legal counsel.

Acknowledgements:

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading FedRAMP firm, provided FedRAMP guidance and control interpretation aligned to NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1 v. 2.0 and the Reference Architecture described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire®

Coalfire Systems is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire® has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C., and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire® has developed a new generation of cloud-based IT GRC tools under the Navis™ brand that clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the NIST 800-53 Rev3 and FedRAMP Baseline Controls v1.1, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA. For more information, visit www.coalfire.com.

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