DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA DIRECTIVE 6517
Transmittal Sheet
November 15, 2016

RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING SERVICES

1. **REASON FOR ISSUE:** This Directive is being reissued to reflect VA's commitment to cloud computing services and align with the VA Cloud Computing Strategy. The specific changes required include reflection of roles and responsibilities of a VA Cloud Broker, the addition of Cloud Consumer management responsibilities and alignment of these roles with specific VA organizations.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This Directive establishes policy, roles and responsibilities regarding evaluation for selection of secure cloud computing services for VA. This document also establishes VA policy for compliance with the Federal Chief Information Officer's (CIO) mandate for a 'Cloud First' policy. The CIO's policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new technology investments. This is supported by current Federal laws, Office of Management and Budget mandates, National Institute of Standards and Technology recommendations, and VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program*.

3. **RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security (005R2) is responsible for the content contained in this Directive.

4. **RELATED HANDBOOK:** VA Handbook 6517, *Risk Management Framework for Cloud Computing Services,* (under development).

5. **RESCISSIONS:** VA Directive 6517, *Cloud Computing Services,* published February 28, 2012.

CERTIFIED BY:	**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**
/s/ LaVerne H. Council Assistant Secretary for Information and Technology	***/s/*** LaVerne H. Council Assistant Secretary for Information and Technology

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING SERVICES

1. PURPOSE AND SCOPE

a. The purpose of this Directive is to establish Department of Veterans Affairs (VA) policy for adoption of cloud computing services within the VA in alignment with VA's Cloud Computing Strategy. This Directive establishes VA's policy to ensure compliance with Federal laws, Office of Management and Budget (OMB) mandates, National Institute of Standards and Technology (NIST) Special Publications (SP), the Federal Risk and Authorization Management Program (FedRAMP), VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program.*

b. Each agency Chief Information Officer (CIO) has been directed to comply with the Federal CIO's mandated, "25 Point Implementation Plan to Reform Federal Information Technology Management," dated December 9, 2010, for the "Cloud First" initiative. This is also in compliance with the revised OMB Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*. The initiative requires that agency CIO's implement cloud computing services whenever possible. The Federal CIO has established FedRAMP to provide a standard approach to Assessment and Authorization (A&A) (formerly Certification & Accreditation) of cloud computing services and products. The Federal CIO has directed NIST to serve as the technical advisor for assessing risks in implementation that is focused on cloud computing solutions. The assessment of risk must be consistent with the six-step Risk Management Framework identified in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

c. FedRAMP is managed by the Federal CIO's Council on cloud computing and allows joint authorizations and continuous security monitoring services for government cloud computing systems intended for multi-agency use. Joint authorization of cloud providers results in a common security risk model that can be leveraged across VA in cooperation with other agencies. The use of this common security risk model provides a consistent baseline for cloud-based technologies. This common baseline ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government.

d. All new technology solutions, and existing solutions undergoing development, modernization or enhancement (DME), shall use cloud computing solutions. Any exceptions that demonstrate a cloud solution cannot be implemented and be approved by the VA CIO or designee must meet the following criteria:

(1) Performance – If performance characteristics (e.g. latency, reliability, etc.) are so stringent that existing cloud options cannot meet the requirements, the solutions will not be considered cloud ready.

(2) Compatibility – If the technical solution has proven technical constraints (e.g. proprietary hardware, technology solution unable to be virtualized, portability of data, etc.) that are not supported by the cloud, the solutions will not be considered cloud ready.

(3) Infrastructure Management – If the technology solution has proven requirements to manage its underlying physical infrastructure for the solution (e.g. prototype, etc.), the solutions will not be considered cloud ready.

(4) Security – If the cloud provider cannot meet the federal and VA security, privacy, records management, and business requirements (e.g., Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Modernization Act (FISMA), National Archives and Records Administration (NARA), Trusted Internet Connection (TIC)), ability to preserve data as required by litigation) the solutions will not be considered cloud ready.

(5) Cost - If the cost of using the cloud is prohibitive, the solutions will not be considered cloud ready.

(6) Portability – If the application design and deployment is operated with significant manual configuration at the production level, then it will not be considered cloud ready and shall not be deployed at external hosting facilities.

e. There are three services that will be available for implementation. These services are the only services and platforms for implementation. The service models are: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS). There are four deployment models: Private Cloud; Community Cloud; Public Cloud; and Hybrid Cloud.

f. This Directive applies to all VA organizations and information technology (IT) resources including contracted IT systems acting on behalf of the VA.

2. POLICY

a. VA will comply with the requirements for a “Cloud First” policy as established by the Federal CIO. The CIO has required Agencies to evaluate the feasibility of a cloud service prior to hardware and software acquisition.

b. VA will continuously identify and evaluate available business use cases for implementation of a cloud service.

c. The VA CIO, or designee, will review and approve/disapprove cloud computing business use cases for VA. VA will ensure that NIST security requirements for cloud computing services are met.

d. VA will conduct and document a feasibility study for a cloud computing service prior to hardware and software acquisition.

e. Each prospective cloud computing business use case will be assessed according to NIST, VA and FedRAMP requirements. The assessment will occur prior to adoption of the service to ensure compliance and adherence to security requirements. This will be conducted in accordance with an A&A standardized approach for cloud computing services based on

NIST “Best Practices” prior to becoming operational.

f. VA will consult with FedRAMP, as needed, to provide a standardized approach to A&A cloud computing services and products. The Federal CIO has established FedRAMP to identify requirements for cloud computing security controls and has directed NIST to serve as the technical advisor for assessing risks in implementation of these services.

g. VA will follow FedRAMP policies, procedures and guidelines in all cloud deployment scenarios.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** is responsible for designating the VA CIO as the senior agency official responsible for the Department’s IT program.

b. **Assistant Secretary for Information and Technology,** as the CIO and Authorizing Official (AO) is responsible for the following:

(1) Authorizing cloud computing services to be used in VA;

(2) Establishing policies and procedures to ensure the provision of effective and secure cloud computing services to support the Federal CIO’s mission for secure, cost-saving technological innovations to support VA’s infrastructure, information systems, and data repositories;

(3) Implementing a risk management approach to IT operations that applies risk categorizations to VA information and information systems; establish secure, cost-saving procedures for implementing cloud computing services whenever feasible, and ensures a balance between risk to information and information systems with cost-saving cloud computing services to preserve VA business requirements and support continuity of operations;

(4) Monitoring, reviewing, and evaluating compliance with this Directive; and

(5) As the overall VA system owner, delegating the daily operations and maintenance of responsibilities to VA officials, as appropriate.

c. **Deputy Assistant Secretary, Service Delivery and Engineering** is responsible for developing, procuring, integrating, modifying, maintaining, and implementation of security over VA information and information systems, and as the VA Technical Cloud Broker, manages the use, performance, and delivery of cloud services, and negotiates relationships Responsibilities include:

(1) Assisting and coordinating with the VA information system owners in managing cloud computing services for VA information systems;

(2) Assisting and coordinating with VA information system owners in creating, maintaining and submitting cloud computing service change requests for continuous monitoring, implementation, or maintenance for approval to the Enterprise Security Change Control Board (ESCCB);

(3) Providing services intermediation at the technical level;

(4) Providing service aggregation at the technical level in close coordination with Enterprise Program Management Office (EMPO);

(5) Providing service arbitrage at the technical level in close coordination with EPMO;

(6) Serving as Contracting Officer's Representative (COR) for Cloud Infrastructures, applications and platforms; the contracting officer representative (COR) duties may be delegated.

(7) Leading Technical Working Groups to standardize Cloud Service Deployment across the OI&T pillars;

(8) Supporting the development and implementation of standardized Service creation and Infrastructure contracting with the Technical Assistance Center (TAC);

(9) Developing standard SLAs for cloud services consistent with design patterns, portability standards and application performance requirements;

(10) Supporting development and enforce enterprise design patterns and portability standards for cloud services;

(11) Developing and maintain a Technical Catalogue of Enterprise Cloud Services;

(12) Overseeing development of an acquisition plan for cloud migration in conjunction with SDE, PD and contracting (TAC);

(13) Supporting OIS, to ensure infrastructure level ATO process standards and Plan of Action and Milestones (POA&M) requirements are met; and

(14) Providing Centralized Capacity Management for Internal and External Capacity.

d. **Deputy Chief Information Officer, Architecture, Strategy and Development (ASD)** is responsible for standards for implementation of IT solutions that best serve Veterans through the integration of technical, business and data architecture, IT strategy, systems design, and knowledge management, while exercising proper stewardship of resources and maintaining transparent operations. ASD responsibilities as the business cloud broker include:

(1) Providing service intermediation at the business level;

(2) Establishing Standardized Service Creation and Infrastructure Contracting with TAC. Develop Standard Contract language that incorporates the Enterprise standard cloud solutions as GFE in conjunction with TAC;

(3) Supporting the development of Standard Contract language for cloud computing by technical broker, central Cloud consumer and contracting;

(4) Assisting TAC and others to establish consumption based contracting and service delivery models;

(5) Creating enforceable enterprise design patterns and portability standards for cloud services;

(6) Coordinating the development of design patterns for migration of activities to and from a cloud provider;

(7) Establishing the framework needed to broker services in support of the Business that enable application sustainment and portability and include in needed design patterns;

(8) Evaluating Business Requirements against design patterns for existence, and if not available, analyze need for design pattern as well as whether this should be leveraged as an Enterprise Design Pattern that should be published as an automated solution;

(9) Ensuring the Technical Reference Model compliance criteria is appropriately defined to apply to Cloud Services;

(10) Defining and evolve appropriate Cloud design patterns managed under ASD Technology Strategies;

(11) Utilizing Enterprise Cost Model for Cloud Service in design patterns;

(12) Maintaining a business catalogue of all current and planned cloud deployments for use in long and short term planning and utilization;

(13) Developing and complete Implementation plans for cloud computing long term solution, midterm objectives and short term objectives;

(14) Supporting development of an acquisition plan for cloud migration in conjunction with ASD, PD and contracting (TAC);

(15) Ensuring design patterns meet security compliance criteria;

(16) Updating, as needed, and maintain Governance organization charters (Enterprise Architecture Council (EAC), Architecture and Engineering Review Board (AERB) and Enterprise Technical Architecture Work Group (ETAWG)) and operating guides;

(17) Develop and review Enterprise Risk Management in support of cloud migration;

(18) Identify changes needed to PMAS and ProPath to support cloud migration;

(19) Representing a person or organization that maintains a business relationship with, and uses the service from a cloud provider;

(20) Browsing the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service; and

(21) The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

e. **Deputy Assistant Secretary, Enterprise Program Management Office (EPMO)** is the chief advisor to AS/IT for all enterprise application development activities. Development consists of planning, developing (or acquiring), and testing applications that meet business requirements. As the central cloud consumer for VA, PD's responsibilities include:

(1) Support Technical Working Groups to standardize Cloud Service Deployment across the OIT Pillars in coordination with the technical cloud broker;

(2) Support the development and implementation of standardized Service Creation and Infrastructure Contracting with TAC;

(3) Develop and track application Performance criteria;

(4) Develop Standard Contract language for cloud computing performance and that requires contractors to follow ASD design patterns and portability standards in coordination with TAC;

(5) Support development of an acquisition plan for cloud migration in conjunction with ASD, SDE and the TAC;

(6) Support OIS, to ensure application level ATO process standards and POA&M requirements are met;

(7) Developing and maintain a Catalogue of Enterprise Cloud Services;

(8) Leading Technical Working Groups to standardize Service Deployment across the OIT Pillars in coordination with the technical cloud broker; and

(9) With OIS, ensuring ATO process standards and POA&M requirements are met.

f. The **Technology Acquisition Center (TAC)** in the Office of Acquisitions Operations under the Deputy Secretary for Acquisitions and Logistics is part of the contracting, acquisition and procurement staff for VA. The TAC is responsible for:

(1) Advising and providing guidance to senior leaders regarding acquisition strategy and issues and provides acquisition, contracting and procurement support to VHA, VBA, NCA, OIT, and VACO staff;

(2) Providing dedicated acquisition and program management expertise and support for life cycle management of enterprise wide solutions in information and technology, primarily for the Office of Information and Technology (IT);

(3) Working closely with the business and technical cloud broker and the central cloud consumer;

(4) Supporting the development and implementation of standardized Service Creation and Infrastructure Contracting;

(5) Developing Standard Contract language for cloud computing performance that requires contractors to follow ASD design patterns and portability;

(6) Supporting development of an acquisition plan for cloud migration in conjunction with ASD, SDE and EPMO;

(7) Assisting the development and implementation of consumption based contracting and service delivery models;

(8) Establishing Standardized Service Creation and Infrastructure Contracting. Develop Standard Contract language that incorporates the Enterprise standard cloud solutions as GFE;

(9) Supporting the development of Standard Contract language for cloud computing by technical broker, central Cloud consumer and contracting;

(10) Supporting SDE as COR for Cloud Infrastructures, applications and platforms;

(11) Supporting the development and implementation of standardized Service creation and Infrastructure contracting with the TAC; and

(12) Developing standard SLAs for cloud services consistent with design patterns, portability standards and application performance requirements.

g. **Deputy Assistant Secretary (DAS) for Information Security,** as VA Chief Information Security Officer, has authority over the VA enterprise cyber security budget and is responsible for ensuring that the capability of utilizing cloud computing services is properly identified and securely managed. In addition, the DAS for Information Security is responsible for:

(1) Developing VA information security policies and procedures consistent with federal laws and guidance, and VA regulations and policies;

(2) Reviewing VA information security policies and procedures related to information security that are under the management and oversight of other Department organizations;

(3) Ensuring that all Memoranda of Understanding and Interconnection Security Agreements clearly define the security controls implemented to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted within or between interconnected systems;

(4) Ensuring voting representation on the ESCCB so that cloud computing services are executed in accordance with federal laws, OMB Circulars and Memoranda, and VA policies for privacy and records management; as well as the Federal CIO’s mandated, “25 Point Implementation Plan to Reform Federal Information Technology Management” dated December 9, 2010, for the Federal Government’s “Cloud First” initiative;

(5) Evaluating and testing the feasibility of cloud computing services to determine security control requirements prior to making recommendations for their adoption or refusal;

(6) Monitoring all cloud computing services for compliance with existing federal laws and VA policies in conjunction with FedRAMP stipulations as directed by the Federal CIO Council;

(7) Ensuring design patterns meet security compliance criteria; and

(8) Ensuring ATO process standards and POA&M requirements are met.

h. **Under Secretaries, Assistant Secretaries, and Other Key Officials** are responsible for ensuring compliance with this Directive within their respective Administrations, Staff Organizations, and Program Offices by coordinating and collaborating with Office of Information and Technology officials.

4. TERMS AND DEFINITIONS

a. **Business Use Case*:*** Simulations are conducted on a continual basis to determine whether selected business processes are feasible for a cloud service. The business use case may be recommended for implementation once the capability for a cloud service has been determined. The business use case simulation does not include VA security controls that may be required for implementation.

b. **Cloud Broker:** The central cloud consumer within VA will request cloud services from a cloud broker, composed of business and technical representatives, if no services of a like kind already exist, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. In general, a cloud broker can provide services in three categories:

(1) Service Intermediation: A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc. Services intermediation within VA occurs at the business and technical levels and is supported accordingly by ASD and SDE. SOURCE: NIST SP500-291

(2) Service Aggregation: A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers. SDE provides this support in close coordination with EPMO as the central cloud consumer. SOURCE: NIST SP500-291

(3) Service Arbitrage: Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score. SDE provides this support in close coordination with EPMO as the central cloud consumer. SOURCE: NIST SP500-291

c. **Central Cloud Consumer:** The central cloud consumer is the principal stakeholder for the cloud computing service. Within the VA all internal cloud consumers will be represented by a single organization resident in EPMO2016.

d. **Cloud Computing:** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. Source: NIST 800-145

e. **Cloud Infrastructure as a Service (IaaS):** The capability available to the consumer is to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). Source: NIST 800-145

f. **Cloud Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Source: NIST 800-145

g. **Cloud Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Source: NIST 800-145

h. **Community Cloud**: A community cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Source: NIST 800-145

i. **Hybrid Cloud:** A hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Source: NIST 800-145

k. **Private Cloud**: A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Source: NIST 800-145

l. **Public Cloud**: A public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Source: NIST 800-145

5. REFERENCES

a. 36 C.F.R. Part 1236, *Electronic Records Management*

b. E-Government Act of 2002, P. L. 107-347

c. Federal CIO's mandated, *25 Point Implementation Plan to Reform Federal Information Technology Management,* dated December 9, 2010, for the Federal Government's "Cloud First" initiative

d. FIPS 140-2, *Security Requirements for Cryptographic Modules*

e. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

f. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

g. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

h. NIST SP 800-53 rev. 4, *Recommended Security Controls for Federal Information Systems*

i. OMB Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*

j. OMB Circular A-130, *Management of Federal Information Resources*

k. OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*

l. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*

m. VA Handbook 6500, *Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program*

n. NIST SP 800-145, *The NIST Definition of Cloud Computing*

o. NIST SP 500-291, *NIST Cloud Computing Standards Roadmap, Version 2*

p. NIST SP 500-292, *NIST Cloud Computing Reference Architecture*

q. FedRAMP Concept of Operations

6. ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization (formerly Certification & Accreditation)
AERB	Architecture & Engineering Review Board
ATO	Authorization to Operate
AO	Authorizing Official
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAS	Deputy Assistant Secretary
DME	Development, Modernization or Enhancement
EAC	Enterprise Architecture Council
EPMO	Enterprise Program Management Office
ESCCB	Enterprise Security Change Control Board
ETAWG	Enterprise Technical Architecture Working Group
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PMAS	Project Management Accountability System
POA&M	Plan of Action and Milestones
SaaS	Software as a Service
SLA	Service Level Agreement
SP	Special Publications
TIC	Trusted Internet Connections
VA	Department of Veterans Affairs