

**VA Enterprise Design Patterns  
Cloud Computing**

# **Cloud Computing Architecture**

**OFFICE OF TECHNOLOGY STRATEGIES (TS)  
OFFICE OF INFORMATION AND TECHNOLOGY (OIT)**


**VERSION 1.0  
DATE ISSUED: APRIL 2016**



## APPROVAL COORDINATION

 Digitally signed by Rodney J. Emery  
106229  
DN: dc=gov, dc=va, o=Internal, ou=people,  
0.9.2342.19200300.100.1.1=rodney.emery  
@va.gov, cn=Rodney J. Emery 106229  
Reason: I have reviewed this document.  
Date: 2016.05.12 13:28:56 -04'00'

Rodney Emery  
Director, Technology Strategies and GEAC, ASD  
ASD Technology Strategies

**PAUL A.  
TIBBITS  
116858**  Digitally signed by PAUL A. TIBBITS  
116858  
DN: dc=gov, dc=va, o=Internal,  
ou=people,  
0.9.2342.19200300.100.1.1=paul.tibbits  
@va.gov, cn=PAUL A. TIBBITS 116858  
Reason: I am approving this document.  
Date: 2016.05.27 12:15:42 -04'00'

Paul A. Tibbits, M.D.  
DCIO Architecture, Strategy, and Design

## REVISION HISTORY

Version	Date	Organization	Notes
1.0	April 2016	ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 compliance

## CONTENTS

1	Introduction .....	5
1.1	Business Need .....	6
1.2	Approach .....	6
2	Current Capabilities and Limitations .....	8
2.1	Capabilities .....	8
2.2	Limitations.....	10
2.2.1	Regional Environments .....	10
2.2.2	Automated Provisioning .....	10
2.2.3	Governance .....	10
3	Future Capabilities .....	11
3.1	Benefits.....	11
3.2	Considerations.....	12
3.2.1	Determining Technical Edit – Asking the Right Questions .....	13
3.3	Architecture and Approach .....	14
3.4	Hybrid Cloud.....	15
3.4.1	Process for Hybrid Applications.....	15
3.4.2	Multi-Speed IT.....	16
3.5	Microservices / Containers .....	16
3.6	Cloud Security .....	16
3.7	Alignment to the One-VA Technical Reference Model (TRM) .....	17
3.8	Alignment to Veteran-Centric Integration Process (VIP) .....	17
4	Use Cases .....	18
4.1	IT Health Application Migration .....	18
4.1.1	Purpose .....	18
4.1.2	Assumptions.....	18
4.1.3	Use Case Description .....	18
4.1.4	Use Case Context Diagram.....	19
4.2	Hybrid Cloud Deployment.....	19
4.2.1	Purpose .....	20
4.2.2	Assumptions.....	20
4.2.3	Use Case Description .....	20
4.2.4	Use Case Context Diagram.....	20
Appendix A.	Scope .....	21
Appendix B.	Definitions.....	22
Appendix C.	Acronyms and Abbreviations.....	23
Appendix D.	References, Standards, and Policies.....	25

Table 1:	List of Approved Tools and Standards for Vulnerability Management .....	17
----------	---	----

Figure 1:	Paving the Path to Cloud Computing Success at VA.....	8
-----------	---	---

Figure 2:	Architectural Concept for VA Cloud Computing Based on NIST Architecture.....	12
-----------	--	----

Figure 3:	Hybrid Strategy – diagram provided by industry partner .....	15
-----------	--	----

Figure 4: IT Health Application Migration Process Flow – drafted by TS team .....	19
Figure 5: Hybrid Cloud Deployment Context Diagram .....	20

## QUICK JUMP

Select an icon to skip to a section.



**Current Capabilities**



**Future Capabilities**



**Use Cases**



**One-VA Technical Reference  
Model**



**The Veteran-Focused  
Integration Process**



**Enterprise Design Pattern  
Scope**

---

## 1 INTRODUCTION

The Department of Veterans Affairs (VA) requires a standard approach for adopting cloud computing services to stay abreast with evolving Veteran-centric business requirements. The Office of Information and Technology (OI&T) supports business owners with flexible solutions that extend existing regional data centers with services provided by commercial cloud service providers. This enables VA to establish a cloud computing architecture that includes public, private, community, and hybrid environments in accordance with the National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST SP 800-145) and the Cloud Computing Reference Architecture (NIST SP 500-292), as referenced in Appendix D.

NIST defines cloud computing as “a model for enabling 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 Enterprise Design Pattern provides guiding principles for both business owners and OI&T to leverage a standard set of components required to adopt cloud-based Information Technology (IT) solutions. These components consist of virtual servers and storage, delivery models (Software-as-a-Service, Platform-as-a-Service, or Infrastructure-as-a-Service), and secure network connections that enable rapid development, deployment, and operations of IT solutions in accordance with VA Handbook 6500 security and privacy guidelines.

## 1.1 Business Need

VA IT projects adopting cloud services will improve efficiency and agility in response to changing business needs. This approach leverages industry best practices and applies innovations developed in the private sector for future cloud expandability. Cloud-based solutions reduce development lifecycles and provide platforms that support modern applications (e.g., distributed applications composed of fine-grained, loosely coupled units known as microservices), and Development Operations (DevOps) best practices. Together, this forms the basis of the cloud computing architecture: reducing OI&T's burden of planning, provisioning, and maintaining IT infrastructure while incorporating an agile development processes.

Establishing a cloud computing architecture in VA will enable the following:

- Lower Burden: Reduce data center infrastructure expenditures
- Simplification: Transition from fragmented and duplicative systems
- Focus: Shift focus from IT infrastructure to business logic
- Automation: Create repeatable build and deployment systems by leveraging programmable (Application Programming Interface (API)-driven) infrastructure
- Auto-scaling: Adjust IT services up and down to match unexpected demand without human intervention
- Proactive Scaling: Change resource levels to meet anticipated demand; requires proper planning and understanding of traffic patterns but also enables cost controlling as resource levels are scaled to meet demand
- More Efficient Development Lifecycle: Production environments can be more readily replicated in development, testing, and staging environments
- Improved Testability: Enable automated test environments that are only used for the testing phase
- Disaster Recovery and Business Continuity: Provide a low- cost option for replication, failover and backup storage

## 1.2 Approach

This Enterprise Design Pattern documents VA's current cloud initiatives, defines the attributes of centralized cloud architecture, and provides recommendations that facilitate integrating existing cloud environments into a centralized cloud architecture. A high level approach for establishing a cloud computing architecture is outlined in the steps below.

- Establish cloud brokerage solution in accordance with Enterprise Cloud Services Broker (ECSB) Enterprise Design Pattern
- Establish cloud migration guidelines for both production legacy systems and new applications developed in a “green field” environment
- Conduct strategic sourcing to identify viable commercial cloud service providers that satisfy FedRAMP and VA Handbook 6500 policies for security and privacy
- Establish business relationships with commercial cloud service providers
- Adopt cloud service providers and approve their use in the TRM
- Implement continuous improvement based on lessons learned

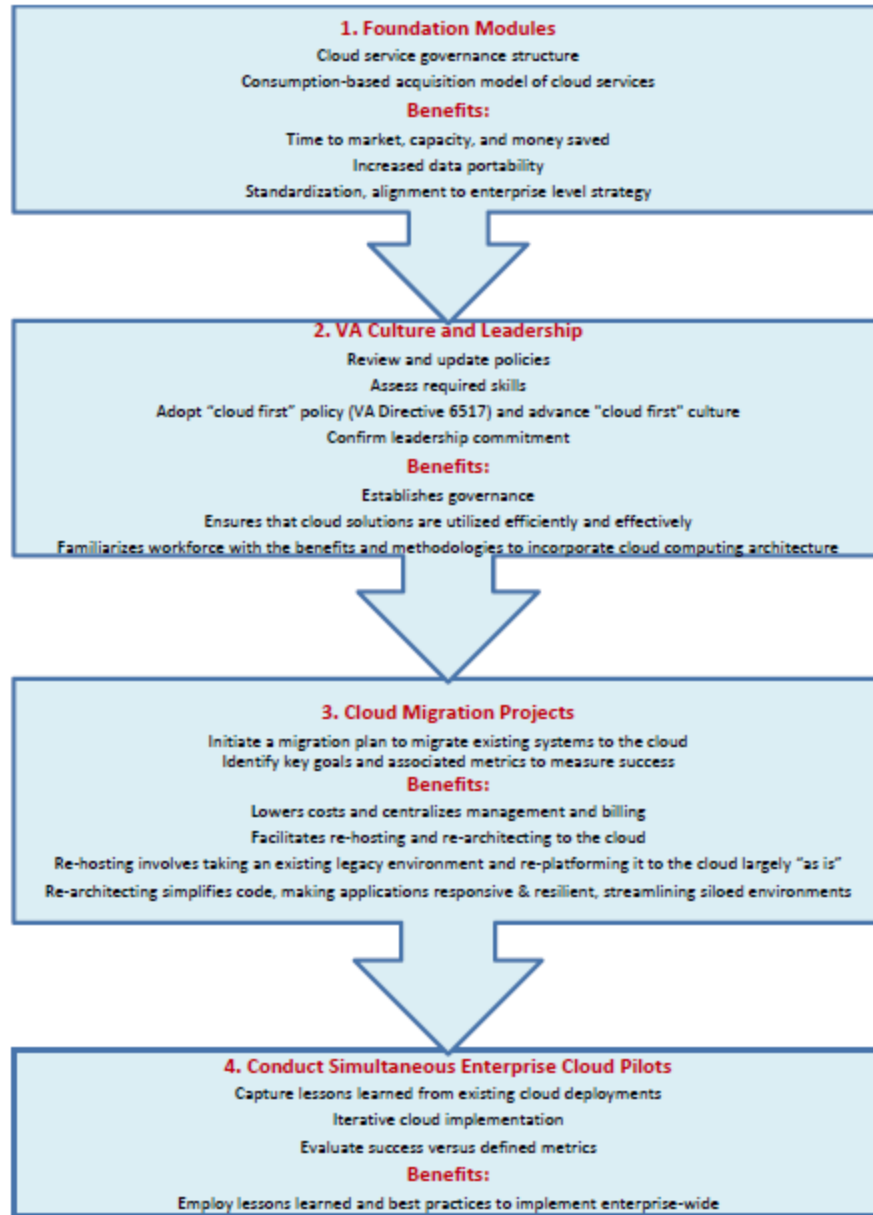


FIGURE 1: PAVING THE PATH TO CLOUD COMPUTING SUCCESS AT VA



## 2 CURRENT CAPABILITIES AND LIMITATIONS

### 2.1 Capabilities

VA OI&T is evaluating pilot solutions that incorporate commercial cloud services to support business requirements. OI&T has adopted virtualization solutions within regional data centers to support a private cloud environment, but the functionality does not provide the NIST-defined essential characteristics of cloud computing. VA is preparing to leverage additional commercial



cloud services that align to the NIST definition as part of its overarching IT strategy and vision documented in the Enterprise Technology Strategic Plan (ETSP).

#### NIST IaaS/PaaS Solutions:

- Amazon AWS
  - Vets.Gov
- Microsoft Azure
  - Veterans Point of Service (VPS)
  - EDE Azure Labs - External Environment
  - EO Migration Pilot

#### NIST SaaS Solutions:

- HRIS
- VATAS
- TMS
- VA Pulse
- Office 365 - Pilot

#### Current capabilities include:

- Virtualized environments distributed across many different regional data centers, including those leased by companies such as Centurylink.
- Many private cloud initiatives.
  - Enterprise Development Environment (EDE) - VA-hosted, private cloud for development and test environments
  - Austin Information Technology Center – A hosting environment that has virtualization capabilities associated with Infrastructure as a Service (IaaS).
  - CenturyLink Environment – an outsourced private hosting environment, which hosts VRM (Veteran Relationship Management) CRM (Customer Relationship Management), Identity and Access Management (IAM), and the VA Mobile Framework (VAMF), amongst others.
  - Hosted Infrastructure Virtual Environment (HIVE) - Provides an internally managed virtualization environment for applications that provides elasticity and scalability to meet changing capacity demands.

## **2.2 Limitations**

While VA has made significant progress leveraging aspects of cloud computing, there are significant limitations which must be overcome to achieve the benefits of a cloud environment. Limitations of VA's current cloud computing architecture include:

### **2.2.1 *Regional Environments***

- Lack of centralization contributes to inefficient development.
- Many of VA's cloud initiatives operate within regional environments (EDE, Austin Information Technology, CenturyLink). This approach does not achieve an enterprise consumption model across all Lines of Businesses (LOBs).
- Dual hosting until projects migrate fully to the cloud; duplications of effort will continue to drive up cost.

### **2.2.2 *Automated Provisioning***

- Limited scalability and elasticity while running on virtual machines. These initiatives are not true clouds (as defined by NIST) and are better characterized as hosted virtualized environments.
- EDE / CenturyLink do not completely provide rapid elasticity and on-demand self-service.
- HIVE is not a truly cloud environment (does not contain all of the NIST essential characteristics: on demand self-service, broad network access, resource pooling, elasticity, measured service).

### **2.2.3 *Governance***

- Lack of VA enterprise visibility of programs being hosted in commercial environment. Data owners fear losing control without this oversight.
- Slow adoption of public clouds due to security and privacy concerns.
- Individual projects do not have official enterprise direction on how to decide whether to migrate workloads to the cloud or keep them on-premises (or both, in the case of hybrid clouds).
- Cloud adoption urgency – VA customers are demanding a cloud computing architecture to help expedite systems and programs into a cloud enclave that works best for them.



### 3 FUTURE CAPABILITIES

VA continues to evolve toward a true cloud environment that will realize the business needs described in Section 1. This section outlines the benefits, architecture concept, approach, and example cloud-based tools and technologies currently approved for use in VA. Page 6

#### 3.1 Benefits

An enterprise cloud computing architecture has the potential to:

- Reduce costs
- Enable resource pooling
- Facilitate service flexibility while continuing to provide an environment that meets VA business needs and requirements
- Enable rapid provisioning
- Provide benefits from economies of scale
- Centralize billing

Figure 2 illustrates the key components of cloud computing based on the NIST reference architecture that enable VA to maximize the benefits of integrating cloud services. This document focuses on service models and hosting environments provided by commercial cloud providers, as indicated by the red boxes.

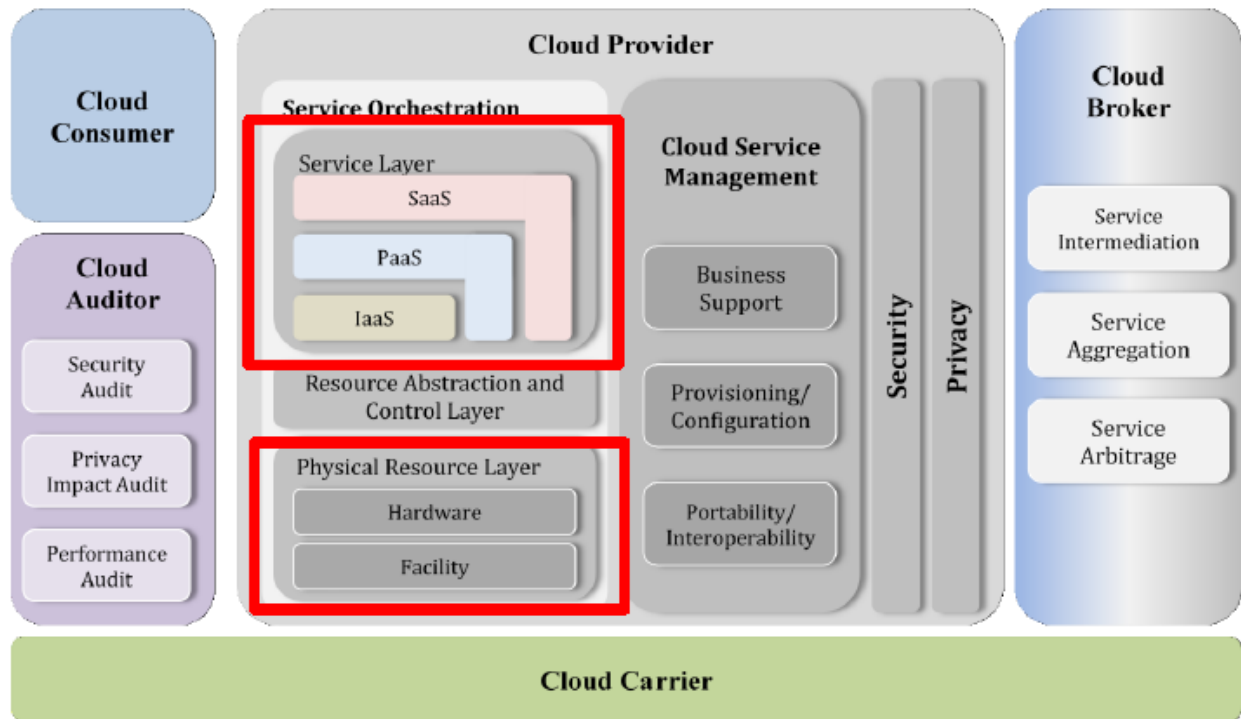


FIGURE 2: ARCHITECTURAL CONCEPT FOR VA CLOUD COMPUTING BASED ON NIST ARCHITECTURE

Advantages of cloud architectures include:

- Faster setup speed: New hosting environments can be setup quickly. No need to plan for and acquire new hardware.
- Economical: Cut costs through reduced capital expenses and operational expenses associated with maintaining an internal IT infrastructure.
- Better: Improved flexibility and scalability through automated configuration management and, security.

### 3.2 Considerations

Maturing a cloud computing architecture requires planning and analysis to understand the requirements, establish the architecture, and ensure that the fielded solution continues to meet Service Level Agreement (SLA) requirements while remaining scalable to emerging needs. This section outlines considerations for adopting cloud architectures.

Cloud Computing Architecture Considerations:

- Rationale for using cloud:
  - Is there a gain in efficiency, agility, scale or cost savings?
- Cloud Architecture relies on VA Enterprise standards and regulations.

- VA standards, regulations and Enterprise Architecture will need to evolve to optimally support cloud solutions.
- Understand Cloud release cycles are far more rapid:
  - Architectures must be flexible.
  - Governance Processes must be adapted to the increased cycle speed.
- Assess appropriateness of solution components for cloud deployment.
  - Need for proximity to a particular locale in the case of a medical device in a medical center.
- Support use of SaaS, PaaS, and/or IaaS as appropriate.
- Engineer solutions to be virtualizable.
- Ensure compatibility with technical environments offered by the Cloud Provider.

For cloud to be successful in VA the solution must be designed in accordance with VA Handbook 6500 security policies that account for:

- Confidentiality – Authentication to, storage of, and data manipulation in the cloud must be as secure, if not more secure, than on VA servers. All actions should be securely logged.
- Integrity – Data is not modified without authorization.
- Availability – The environment is set up for timely access to data. After the need is met, it should be torn down and made available again.

### **3.2.1 Determining Technical Edit – Asking the Right Questions**

Several questions to determine how well a cloud solution will meet VA's user needs are provided below. Considering how users will access applications, the data model, and scalability are important factors for VA to develop and leverage cloud-based resources.

- How will VA users access the applications?
  - Web
  - Mobile
  - Desktop
  - Hybrid
- How many users will there be?
  - Where are the users located?
- What is the applicable data model?
  - Task based
  - Asset based
  - Media based

- How will the VA applications and services need to scale?
  - Increased concurrent users
  - Increase or change to expected workload
- What type of notifications are required?
  - Email
  - SMS
  - Mobile
  - Integrations

### 3.3 Architecture and Approach

Upon deciding to leverage cloud-based resources for the project, determine how to:

- Provide the ability for self-service provisioning of compute, network, storage, and apps.
- Orchestrate across regional infrastructures: stitch services together.
- Integrate with VA Information Technology Service Management (ITSM) approaches (in accordance with ITSM Enterprise Design Patterns such as change and configuration management).
- Support management readiness: monitoring agents, compliance scans, OS hardening.

Coordination with industry experts yielded a set of recommendations for successful cloud adoption. Recommendations include: Identification

- Take a staged approach to cloud adoption, start small
  - Success breeds success
  - Several pilots are already in progress
- Automation and Standardization begin at home
  - Optimize workloads, processes and procedures before moving to cloud
- “Lift and Shift” strategies for cloud do not reap all of the benefits of cloud
  - Moving something as-is to the cloud may not always be the right thing to do
  - Sometimes it is important to see how things will impact the SLAs and still meet the business needs
  - They are more closely aligned to managed services
  - Refactor applications to be cloud optimized the extent possible before migrating to the cloud to maximize benefit
- In order to avoid cloud vendor lock-in, an exit strategy for every cloud entry must be defined
  - Do not get locked into a single provider by relying too heavily on “features”
  - Do not use proprietary vendor features offered by a specific cloud provider

- A hybrid cloud (Private + multiple Public) approach is key

### 3.4 Hybrid Cloud

Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services. A hybrid approach to achieve an enterprise cloud computing architecture enables mission support while incrementally migrating services. Benefits to this approach include:

- Continuity of mission support during the transition.
- Flexibility to learn, train and optimize as you build and transition.
- Transition only what is ready for the cloud and maintain other services within the current architecture until able to be transitioned.

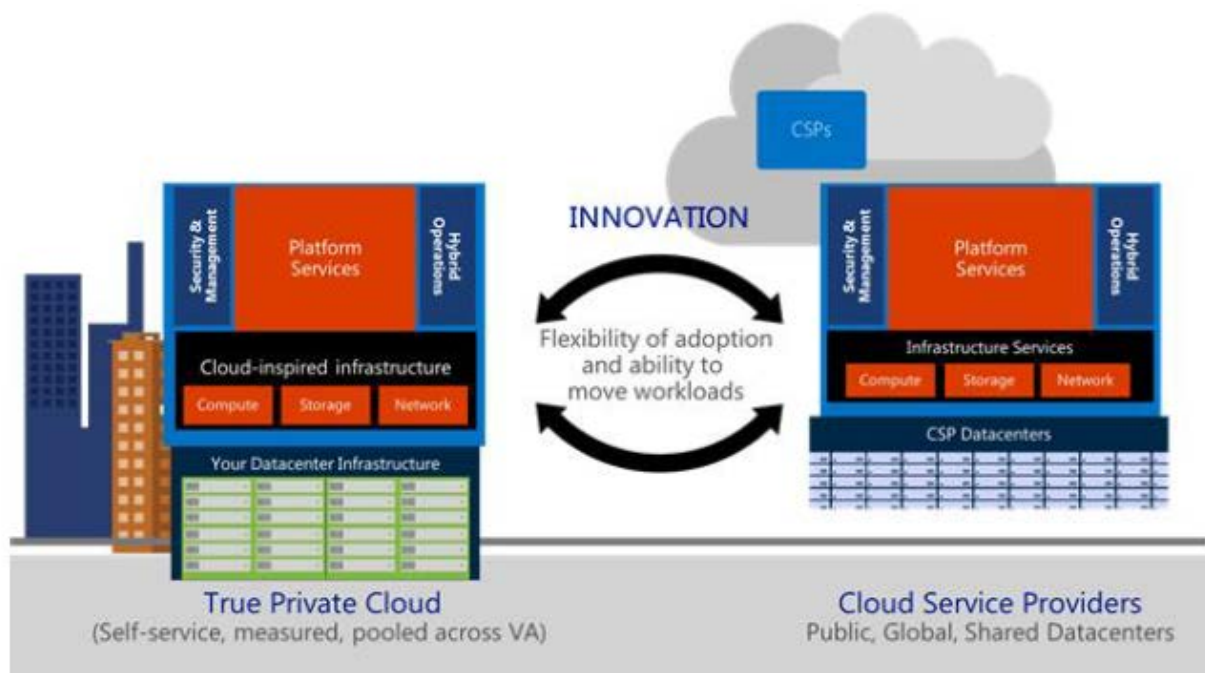


FIGURE 3: HYBRID STRATEGY – DIAGRAM PROVIDED BY INDUSTRY PARTNER

#### 3.4.1 Process for Hybrid Applications

Hybrid applications are architected to perform in hybrid cloud environments. They load-balance between on and off-premises computing resources and respond to changes in network connectivity to provide an optimal user experience. To begin employing hybrid applications:

- Stand-up development and test environments in the cloud and maintain production and disaster recovery environments on-premises.

- Migrate disaster recovery environment into the cloud once development and test environments are successfully operational.
- Migrate the production environment into the cloud with legacy applications still hosted locally. It is important to ensure that the environments mirror each other in order to minimize migration risks.

### **3.4.2 Multi-Speed IT**

Multi-speed IT facilitates rapid development and ensures that developers focus on creating software instead of instantiating development and testing environments. Properties include:

- Composable environments to build and deploy new cloud-native and mobile solutions rapidly.
- Flexibility to move applications to the cloud as-is or build cloud native solutions. Best practice approach includes a Virtual Private Network (VPN) or (secure network connection via Network Security Operations Center (NSOC)) to go from on premises to the cloud.
  - Repurpose owned IT assets into a private, on-premises cloud. Connect to externally-provided cloud resources to achieve the benefits of a hybrid cloud solution.

### **3.5 Microservices / Containers**

VA will leverage fine-grained, distributed applications known as microservices to deliver customer-facing functionality more rapidly as VA shifts to an agile development approach. One best-practice approach to deploying microservices in a cloud environment is through operating system-level virtualization components called containers. The benefits to this approach include:

- Modularity based on each component service
- Update cycles decoupled
- Modular and efficient scalability
- Individual components easier for on boarded developers
- No long term commitment to the technical stack
- Higher availability

More information about microservices and containers can be found in the Microservices Enterprise Design Pattern.

### **3.6 Cloud Security**



Security and privacy considerations are important in determining the appropriate cloud computing architecture. All cloud services adopted for VA use will be subject to VA Handbook 6500 policies and FedRAMP guidelines. Page 11

A future Cloud Security Enterprise Design Pattern will discuss cloud security and privacy requirements in greater detail.

### 3.7 Alignment to the One-VA Technical Reference Model (TRM)

All projects that adopt cloud services will leverage the approved technologies and standards located in the VA Technical Reference Model (TRM). This includes all commercial cloud service providers that meet VA security requirements.

TABLE 1: LIST OF APPROVED TOOLS AND STANDARDS FOR VULNERABILITY MANAGEMENT

Tool Category	Example Approved Technology
Cloud Technologies	CloudForms, EMC Atmos GeoDrive, iCloud, Heroku, OpenShift Enterprise
Virtualization Software	Citrix XenApp, Docker, Linux Containers, IBM WAVE for z/VM, VMware Tools and VirtualBox
Miscellaneous	Atlantis USX, HP Command View EV A, PhoneView, Tivoli Storage Manager for Space Management and Veritas Enterprise Administrator
Physical Servers	TSPrint
Data Center Automation Software	BMC Application Automation and Microsoft Center Operation Management

### 3.8 Alignment to Veteran-Centric Integration Process (VIP)

Cloud services provide the flexibility and adaptability to realize a microservices application architecture, which enables VA IT projects to adhere to DevOps principles following the Veteran-focused Integration Process (VIP).

VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found here: <https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/>.



## 4 USE CASES

The following use cases demonstrate applying the capabilities and recommendations described in this document.

### 4.1 IT Health Application Migration

#### 4.1.1 Purpose

Analyze Health Application Migration as it relates to operating in a cloud environment (scheduling, appointments, etc.)

#### 4.1.2 Assumptions

- Health Application Migration starts out in a non-cloud environment and transitions to a cloud environment.
- Application cannot be taken down for maintenance.

#### 4.1.3 Use Case Description

Migrate Legacy Health Care Application to the Cloud

1. Identify low risk health care applications to move to the Cloud
2. Plan for the pilots
  - a. Budgets
  - b. Schedules
  - c. Impacts
  - d. Transition Plan

\*EDE is currently setting up an Azure external testing environment to help in the testing, validation, and adoption for greater use of Enterprise Cloud Design Patterns
3. Consider Cloud architecture strategies based on pilot needs
  - a. Deployment model (public / community / hybrid / private)
  - b. Service model (infrastructure / platform / software as a service)
4. Rapidly provision necessary compute, storage, and networking using ECSB
5. Develop working version of pilot
  - a. Copy application logic, data, etc. to the Cloud environment
  - b. Test virtualized application
  - c. Resolve any identified deficiencies
6. Update ECSB service catalog to advertise pilot
7. Conduct user acceptance testing (UAT)

- a. Collect user feedback
  - b. Collect performance metrics
  - c. Make adjustments based on user feedback
8. Scale pilot into enterprise capability
  - a. Use performance metrics from UAT to forecast resource needs
  - b. Provision appropriate resources to scale up
9. Monitor performance for compliance with SLA

#### 4.1.4 Use Case Context Diagram

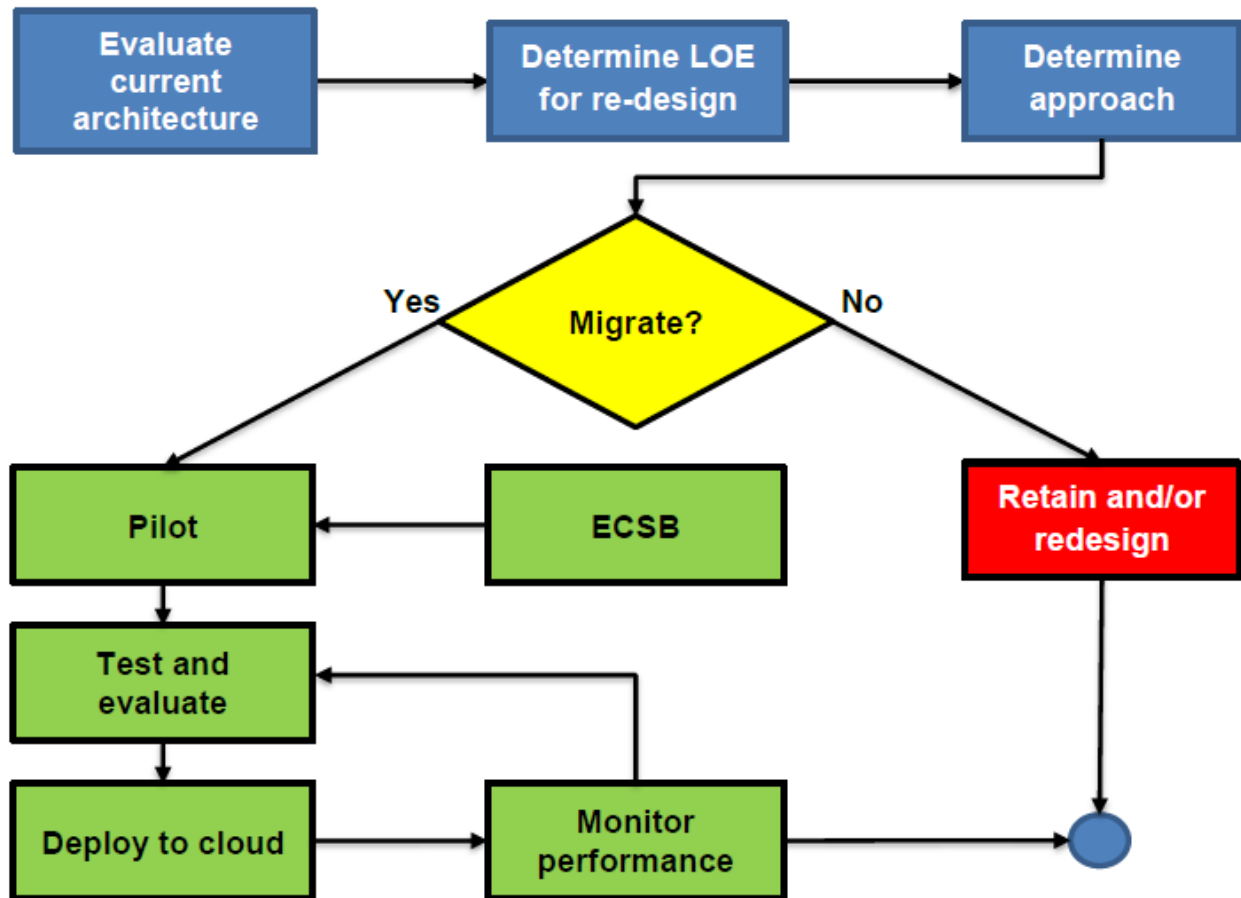


FIGURE 4: IT HEALTH APPLICATION MIGRATION PROCESS FLOW – DRAFTED BY TS TEAM

## 4.2 Hybrid Cloud Deployment

The combination of privately owned and vendor managed assets.

#### 4.2.1 Purpose

Define a framework for establishing an enterprise-wide cloud capability consisting of both VA- and vendor-operated computing resources.

#### 4.2.2 Assumptions

- VA owns cloud-compatible IT assets on premises
- VA's strategy dictates a "cloud first" strategy
- Assets are completely inventoried per configuration management design pattern
- ECSB is already in place

#### 4.2.3 Use Case Description

1. Determine needs for Cloud environment
  - a. Compute, network, storage
  - b. Security, including data confidentiality
  - c. Continuity of operations planning
  - d. Disaster recovery
  - e. ITSM – capacity planning, service strategy, configuration management database
2. Establish SLA based on identified needs.
  - a. Automate enforcement in ECSB where possible
  - b. Consider Open Source (see memo below)  
[http://www.va.gov/vapubs/viewPublication.asp?Pub\\_ID=804&FTYPE=2](http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=804&FTYPE=2)
3. Select and contract with vendor(s) who can fulfill terms of SLA
4. Transition on premises assets to cloud
  - a. Use private cloud for high sensitivity assets
  - b. Use vendor managed cloud for lower sensitivity assets

#### 4.2.4 Use Case Context Diagram



FIGURE 5: HYBRID CLOUD DEPLOYMENT CONTEXT DIAGRAM



## **APPENDIX A. SCOPE**

The Enterprise Cloud Computing Architecture Enterprise Design Pattern increment addresses the following questions:

- What are the requirements that we need to know before we acquire any cloud computing architecture?
- What are the user needs that drive these requirements?
  - Consider business requirements when selecting the type of service (IaaS, PaaS, SaaS)
- Business requirements drive the architecture decisions

It consists of defining a decision framework for using cloud solutions.

### **Intended Audience**

The primary audience for this document consists of VA stakeholders who manage and/or conduct cloud computing activities on behalf of their organization (e.g., office, program, LOB). Specifically, these stakeholders are:

- System and application owners/stewards
- Executive leadership in IT (CIO, division heads, etc.)

This document is also intended for those in leadership roles who can establish governance mechanisms and policies related to analytics.

### **Document Development and Maintenance**

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA OI&T, Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, VBA and the National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates are coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

## APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document.

Key Term	Definition
Cloud Consumer	A person or organization that maintains a business relationship with and uses services from a cloud provider
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers
Epic	Clarification of a business initiative at a high level
Microservices	Dividing a larger application into smaller discrete combinable services

## APPENDIX C. ACRONYMS AND ABBREVIATIONS

The following table provides a list of acronyms and abbreviations that are applicable to and used within this document.

Acronym	Description
AA&A	Authentication, Authorization and Audit
AITC	Austin Information Technology Center
API	Application Programming Interface
ASD	Architecture, Strategy and Design
ATO	Authority to Operate
CIA	Confidential, Integrity and Availability
COTS	Commercial Off the Shelf
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DEERS	Defense Enrollment Eligibility Reporting System
DHS	Department of Homeland Security
DoD	Department of Defense
EA	Enterprise Architecture
ECSB	Enterprise Cloud Services Broker
EDE	Enterprise Development Environment
EDI-PI	Electronic Data Interchange Person Identifier
EHR	Electronic Health Record
EMI	Enterprise Messaging Infrastructure
ESCCB	Enterprise Security Change Control Board
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETA CC	Enterprise Technical Architecture Compliance Criteria
ETSP	Enterprise Technology Strategic Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IPT	Integrated Project Team
IT	Information Technology
JAB	Joint Authorization Board
LOB	Line of Business
MHV	My HealtheVet
MHV IEN	My HealtheVet Internal Entry Number
NIST	National Institute of Standards and Technology

Acronym	Description
NSOC	Network Security Operations Center
OI&T	Office of Information and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
PaaS	Platform-as-a-Service
PATO	Provision Authority to Operate
PHI	Protected Health Information
SaaS	Software-as-a-Service
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
TIC	Trusted Internet Connection
TRM	Technical Reference Model
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VIP	Veteran-Centric Integration Process
VistA	Veterans Health Information Systems and Technology Architecture
VRM	Veterans Relationship Management



## APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the VA Enterprise Technical Architecture (ETA) and the following VA OIT references and standards that are applicable to all new applications developed at VA.:

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with the VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
3	VA	VA Strategy Lockdown VAIQ#7641464	VA Strategy for Adoption of Cloud Computing (draft)
4	VA IAM	VA Directive 6051	Department of Veterans Affairs Enterprise Architecture (VA EA), July 12, 2002
5	VA	VA Handbook 6517	Risk Management Framework for Cloud Computing Services (draft)
6	NIST	NIST SP 500-291	NIST Cloud Computing Standards Roadmap, Version 2, July 2013
7	NIST	NIST SP 500-292	NIST Cloud Computing Reference Architecture
8	NIST	NIST SP 800-145	The NIST Definition of Cloud Computing, NIST SP 800-145, Sept. 2011
9	NIST	NIST SP 500-299	NIST Cloud Computing Security Reference Architecture
10	DoD	DoD	Department of Defense Cloud Computing Strategy

#	Issuing Agency	Applicable Reference/ Standard	Purpose
11	GSA	GAO 14-753	These challenges were derived from DoD Cloud Computing Strategy and the GAO Report 14-753, "Cloud Computing: Additional Opportunities and Savings Need to Be Pursued," Sept. 2014
12	OMB	OMB M-08-05, Implementation of Trusted Internet Connections (TIC)	Establishes TIC to optimize and standardize the security of external network connections for Federal agencies. Three strategic components:
13	Federal	U.S. CIO, Federal Cloud Computing Strategy	This 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 investments.
14	Federal	U.S. CIO, 25 Point Implementation Plan to Reform Federal Information Technology Management	States that the Federal Government will shift to a "Cloud First" policy to better prepare the Government for future computing needs. When evaluating options for new IT deployments, OMB will require agencies to default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.
15	Federal	FIPS 199	FIPS 199 (Federal Information Processing Standard Publication 199)
16	Federal	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
17	VA	VA Memorandum Consideration of Open Source Software (VAIQ#7532631)	Establishes requirements to evaluate Open Source Software solutions and consider OSS development practices for VA-developed software.

**Disclaimer:** This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.