VA Enterprise Design Patterns
Cloud Computing

Transition to Cloud

Office of Information and Technology (OIT)

Version 1.0

Date Issued: February 2018

APPROVAL COORDINATION

Deeneen U Akeo 622220

Digitally signed by Deeneen U Akeo 622220
Date: 2018.02.08 20:57:10 -05'00'

DEENEEN AKEO
DIRECTOR, ARCHITECTURE & ENGINEERING, EPMO DEMAND MANAGEMENT

Everett, John P.

Digitally signed by Everett, John P.
Date: 2018.02.14 13:28:15 -05'00'

JOHN EVERETT
EXECUTIVE DIRECTOR, EPMO DEMAND MANAGEMENT

REVISION HISTORY

Version	Date	Approver	Notes
1.0	10/05/2017	Bonnie Walker	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

CONTENTS

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

This Enterprise Design Pattern (EDP) provides the guiding principles for migrating to cloud-based IT solutions for business owners and other VA stakeholders at the Office of Information and Technology (OIT). Cloud computing is defined by the National Institute of Standards and Technology (NIST) as 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). The solutions entail access to virtual servers and storage, secure network connections, and well provisioned service models, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS). Cloud adoption is a business decision that will enhance VA's mission, services, capabilities, and enable rapid development, deployment, and operations that comply with VA Handbook 6500 security and privacy guidelines.

Figure 1 highlights the key components of cloud computing. These components are based on NIST recommendations for architecture framework, enabling VA to maximize the benefits of migrating to cloud services.

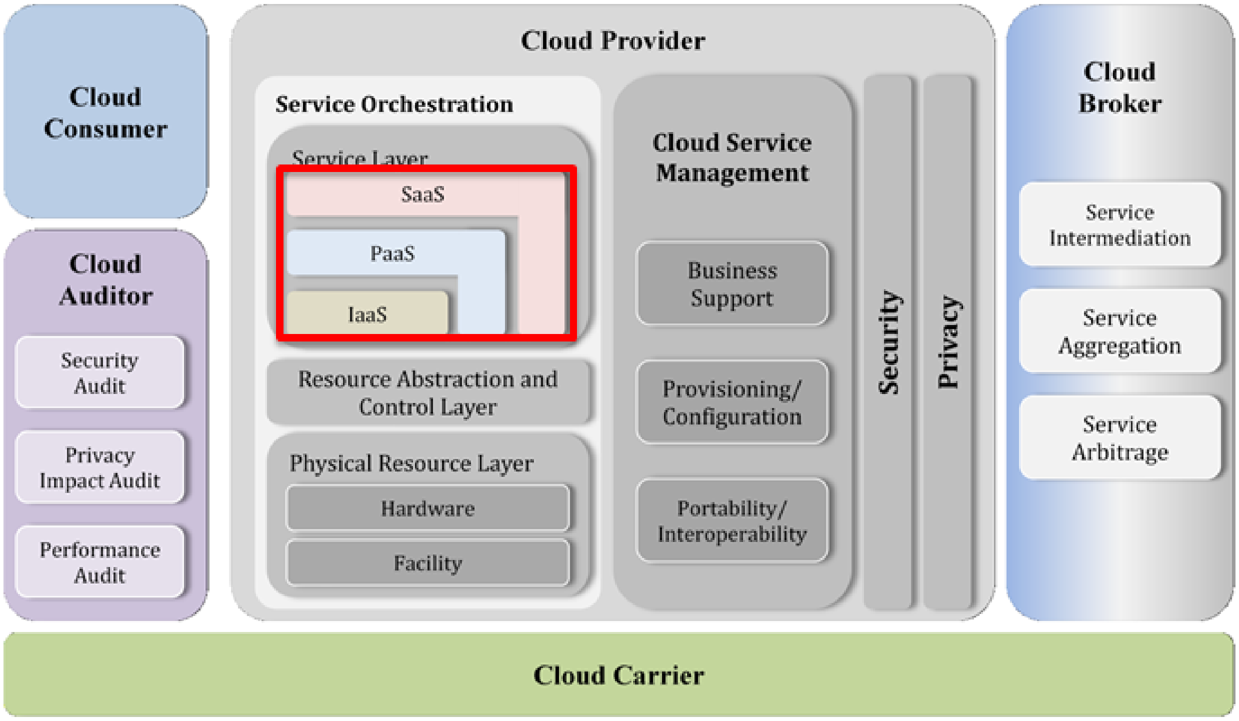


FIGURE 1: ARCHITECTURAL CONCEPT FOR VA CLOUD COMPUTING BASED ON NIST ARCHITECTURE

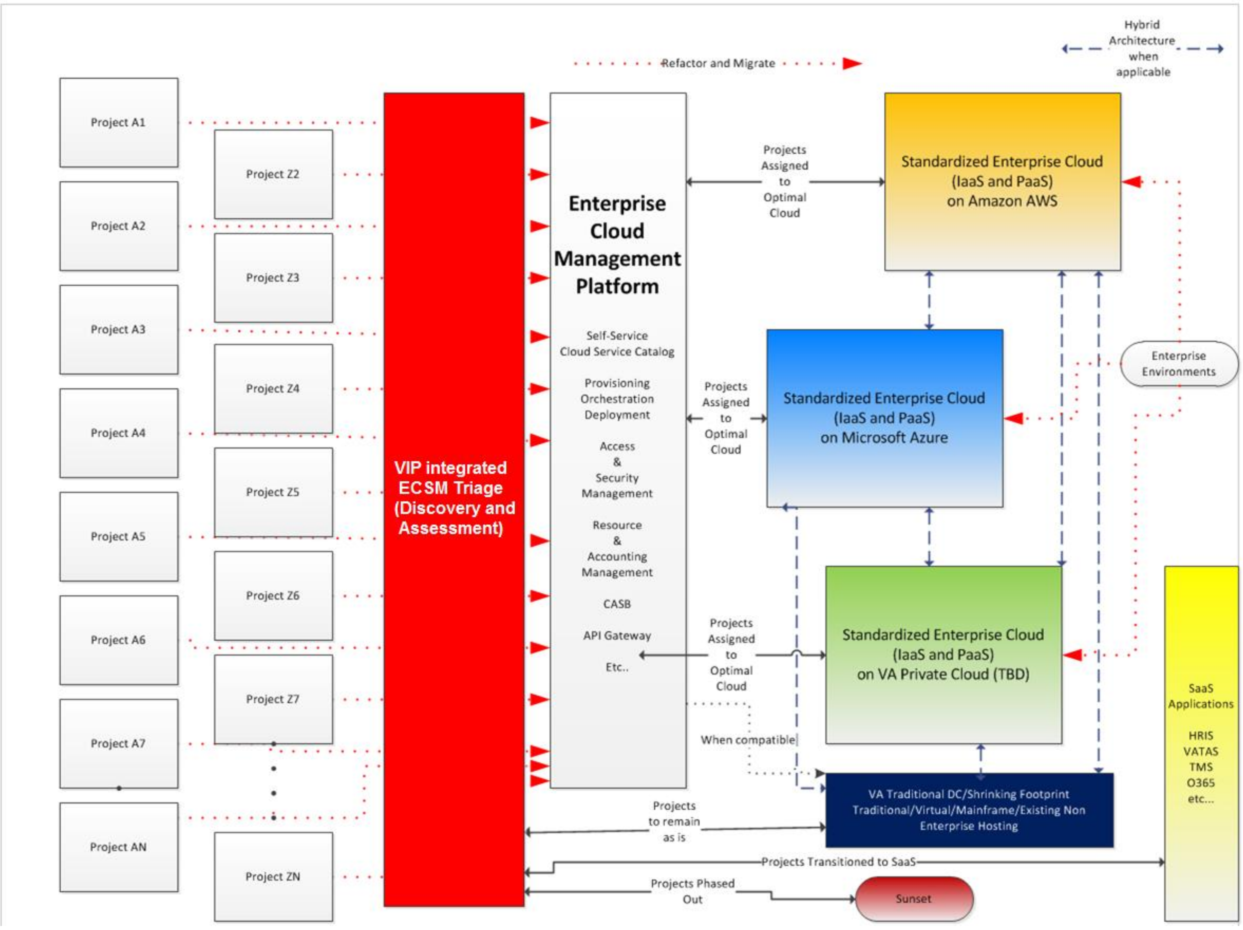
The functions and associated responsibilities will be tailored to the unique VA organizational structure and its existing activities. The result will simulate the arrangement depicted in Figure 2.

1.1 Business Problem

Currently, there is not a standard approach to deploying and migrating to the cloud to address business needs across all VA Lines of Business (LOBs). Despite VA's adoption of the VA Cloud First Policy (VA Directive 6517), stakeholders have been reluctant to transition to cloud services. Among the concerns are security, a lack of familiarity with cloud migration, and inadequate guidance on cost/benefit analysis. As a result, there has been a natural tendency to develop custom in-house solutions to address business needs, which creates duplicative and competing technology infrastructure and expands the enterprise risk landscape. The expansion leads to higher cost solutions and increased complexity for IT support, even when more cost-effective cloud solutions are readily available.

1.2 Business Need

A framework for cloud-based capabilities that is used consistently by project teams will address strategic infrastructure gaps that exist between current cloud implementation and the IT vision, as identified in the Enterprise Technology Strategic Plan (ETSP). The framework will support a smooth transition of VA applications to the VAECE by providing common services and security controls to all service delivery models (IaaS, PaaS, SaaS) that host applications within it. These common services and controls will simplify the ability to build, deploy, and migrate native cloud applications. The appropriateness of the transition to the cloud will be evaluated by business and technical requirements criteria. In addition, it will contain insight into the cost/benefits of cloud migration and guidance for selecting service delivery models within the VAECE (SaaS/PaaS/IaaS). The framework is expected to leverage existing cloud computing Enterprise Design Patterns (EDPs).



Hybrid Architecture when applicable
Refactor and Migrate
Project A1
Project A2
Project A3
Project A4
Project A5
Project A6
Project A7
Project AN
Project Z2
Project Z3
Project Z4
Project Z5
Project Z6
Project Z7
Project ZN
VIP integrated ECSM Triage (Discovery and Assessment)
Enterprise Cloud Management Platform
Self-Service Cloud Service Catalog
Provisioning Orchestration Deployment
Access & Security Management
Resource & Accounting Management
CASB
API Gateway
Etc..
Projects Assigned to Optimal Cloud
Standardized Enterprise Cloud (IaaS and PaaS) on Amazon AWS
Projects Assigned to Optimal Cloud
Standardized Enterprise Cloud (IaaS and PaaS) on Microsoft Azure
Enterprise Environments
Projects Assigned to Optimal Cloud
Standardized Enterprise Cloud (IaaS and PaaS) on VA Private Cloud (TBD)
When compatible
VA Traditional DC/Shrinking Footprint Traditional/Virtual/Mainframe/Existing Non Enterprise Hosting
Projects to remain as is
Projects Transitioned to SaaS
Projects Phased Out
Sunset
SaaS Applications
HRIS
VATAS
TMS
O365
etc...

FIGURE 2: VA ENTERPRISE CLOUD OVERVIEW

VA is in the process of establishing a system for Enterprise Cloud Service Management (ECSM) in order to realize measurable efficiencies and governance within every layer of the VA Enterprise Cloud Environment (VAECE), from the infrastructure of the Enterprise Cloud Management Platform (ECMP), to application. The ECSM will function to guide, organize, and control the multiple clouds within both public and private environments (including IaaS, PaaS, and SaaS). Please note that the SaaS applications in Figure 2 are displayed in yellow and are in the cloud.

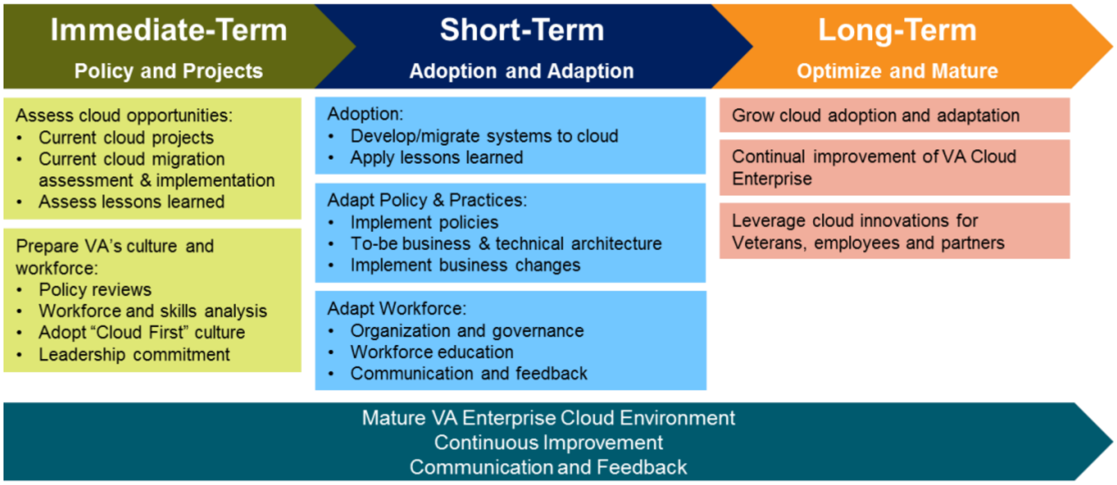
Refer to appendix A for more detail on the scope, intended audience, document development and maintenance.

1.3 Business Case

The benefits of deploying and migrating to cloud services include the following:

- Optimize infrastructure: Reduce data center infrastructure expenditures through simplification, transitioning from fragmented and duplicative systems.
- Compute on-demand: Facilitate utility computing, paying only for the virtual resources consumed.
- Improve uptime: Use built-in availability that is managed by the service provider.
- Adapt: Elastic computing enables dynamic adaptation of capacity to meet a varying workload.
- Focus: Shift focus from IT infrastructure to business logic.
- Regularly update: Cloud Service Providers (CSPs) regularly update offerings to give the cloud consumer the most up-to-date technology.
- Reduce risk: Consistently implement security standards to decrease the risk of insider threat and outside intrusion.
- Maintain business continuity: Provide a low-cost option for disaster recovery, replication, failover, and backup storage.
- Access: Provide seamless accessibility to cloud-based applications and data from virtually any internet connected device.
- Collaborate: Worldwide access means teams can collaborate from a wide variety of locations.
- Support Development Operations (DevOps) processes: Cloud environments strongly support continuous integration, testing, deployment, and infrastructure-as-code, all key principles under the umbrella of DevOps. Cloud environments act as accelerants in deploying systems to meet requirements.

As indicated in figure 3, from the VA Cloud Strategy draft, the VA CIO will initiate a three-phase strategy to adopt and optimize cloud computing. The IT strategy will enable VA to adapt its organization, policy, processes, and culture to achieve VA mission goals and overall business priorities.



Immediate-Term
Policy and Projects

Assess cloud opportunities:
- Current cloud projects
- Current cloud migration assessment & implementation
- Assess lessons learned

Prepare VA's culture and workforce:
- Policy reviews
- Workforce and skills analysis
- Adopt "Cloud First" culture
- Leadership commitment

Short-Term
Adoption and Adaption

Adoption:
- Develop/migrate systems to cloud
- Apply lessons learned

Adapt Policy & Practices:
- Implement policies
- To-be business & technical architecture
- Implement business changes

Adapt Workforce:
- Organization and governance
- Workforce education
- Communication and feedback

Long-Term
Optimize and Mature

Grow cloud adoption and adaptation

Continual improvement of VA Cloud Enterprise

Leverage cloud innovations for Veterans, employees and partners

Mature VA Enterprise Cloud Environment
Continuous Improvement
Communication and Feedback

FIGURE 3: VA CLOUD COMPUTING ADOPTION PHASES

This process should include laying the foundation to enable the start of new cloud native services and applications. The foundation should have a consumerization focus on Veterans and their overall experience at VA.

1.4 Approach

This EDP defines a framework for deploying and migrating to cloud solutions. Guidance pertaining to the framework can be found in the ensuing sections: current limitations, key attributes of a transition to cloud framework, use cases, service model selection, and future capabilities. A project team determines how to transition to cloud by answering the following questions:

- What customer needs drive requirements and what are the current limitations?
- What are the key attributes of a transition to cloud framework?
- In what sequence are cloud service models (SaaS/PaaS/IaaS) reviewed for consideration?
- Where does a migration application fit within the VAEC or alternate CSPs and how does it contribute to the future capabilities?

Additionally, this EDP establishes a path for migrating to the cloud to address a wide variety of VA business needs. The target state for VA's IT infrastructure is achieved through a comprehensive approach that includes cloud-based services in the Enterprise Architecture (EA). This approach consists of the following:

- Gather business needs and define requirements.

    - Guide VA to business capabilities decisions that are best supported by cloud services.

- Define the attributes of a cloud transition framework.
- Use VA furnished cloud capacity (instead of acquiring project specific capacity). This transition-to-cloud framework will have the potential to provide the following benefits:
    - Time to market
    - Cost savings
    - Flexibility
    - Standardization
    - Sustainment efficiencies
    - Improved performance
    - Reduction of enterprise risk
    - Improved end user experience

Note that this document provides two best practice use cases which project teams can reference for guidance for two scenarios:

- Lift-and-Shift Cloud Migration – Transport a non-cloud environment to a cloud environment, as is.
- Refactoring Cloud Migration – Transport parts of a non-cloud environment to a cloud environment in iterations.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA is in the process of evaluating applications and systems for cloud migration. OIT has adopted virtualization solutions, but these currently do not address all NIST-defined characteristics of cloud computing. To be accepted as a true cloud solution, a service provider needs to offer on-demand self-service, broad network access, resource pooling, elasticity, and a measured service. VA is preparing to leverage additional commercial cloud services that align to the NIST definition as part of its overarching IT strategy and vision, as documented in the Enterprise Technology Strategic Plan (ETSP).

2.1 Capabilities

- Public/Community Enterprise Cloud:
    - AWS – Government and Commercial
        - Already has VA Authority to Operate (ATO)
        - Existing project using Vets.gov
        - Existing Trusted Internet Connection (TIC) Compliant connection
    - Azure – Government and Commercial

- Already has VA ATO
- Existing projects using Enterprise Development Environment (EDE) Azure Labs, Veterans Point of Service (VPS)
- Compatible with Office 365; SaaS project leverages connection
- Existing TIC Compliant connections

- Private Enterprise Cloud:
    - Provides a hosted infrastructure virtual environment for applications that cannot be hosted in public/community clouds for technical, security, and privacy related reasons
    - Leverages prior acquisition efforts, lessons-learned, and reusable acquisition documentation/requirements
    - Solves numerous security concerns for applications that cannot go to commercial clouds
    - Enables hosting of government furnished equipment (GFE) for application architectures that are not cloud-ready
    - Creates consolidation points for VA data centers
    - May leverage existing VA data center infrastructure and capacity
    - Provides an internally managed virtualization environment for applications that provide elasticity and scalability to meet changing capacity demands
- Some other private cloud initiatives underway:
    - EDE Azure Labs – VA-hosted, private cloud for development and test environments on the VA Network and in the Microsoft Azure Cloud
    - Austin Information Technology Center – A hosting environment that has virtualization capabilities associated with 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), among others
- SaaS Solutions:
    - HRIS
    - VATAS
    - IRIS
    - TMS
    - VA Pulse
    - Office 365 - Pilot

Although VA Directive 6517 established policies, roles, and responsibilities for the adoption of cloud computing services, VA is working to ramp up an ECSM to guide stakeholders. VA mainly deploys private cloud solutions, using CenturyLink and a smaller subset of SaaS solutions hosted in private implementations at various vendor facilities. And VA is initiating on-line development environments for testing. Despite this "Cloud First" push, there are a number of challenges to increasing flexibility and reducing costs.

2.2 Current Limitations

- Current offerings that are used by VA and marketed as cloud solutions may fall short of providing the full characteristics of cloud computing, as defined in the NIST definition. These solutions have limited elasticity and scalability, and do not provide complete on-demand self-service.
- Cloud providers need to meet rigorous Federal Risk and Authorization Management Program (FedRAMP) requirements. These cloud providers require an ATO, as referenced in VA Handbook 6517 and VA Handbook 6500.
- The Office of Information Security (OIS) and the Network and Security Operations Center (NSOC) are currently resolving challenges with TIC integration and data security requirements, in accordance with the Cloud Security EDP. Based on experience, VA understands that substantial time is necessary to acquire ATO and establish TIC compliant connectivity to a cloud system (6 months to 12 months or more each).
- All cloud providers need to be integrated with the ECSM to address challenges associated with integrating multiple cloud providers to a common cloud management platform. Specifically, this addresses challenges for LOBs who desire a self-service interface to cloud service offerings that meet the service level agreements (SLAs) that are required to support business needs.
- Current tool limitations are related to enterprise scalability and central management for multi-cloud environments; integrated cybersecurity tools include privileged account and access management.
- Availability of Government Subject Matter Experts (SMEs) can be difficult to obtain in a successful cloud migration.
- Education and cloud literacy are usually some of the greatest challenges in cloud migrations.

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 attributes of cloud service models, data migration, cost/benefit analysis, and the sunset of legacy systems.
- As part of the implementation of the VA Cloud First Policy (VA Directive 6517), projects will address their business needs by evaluating the best type of cloud service among

SaaS, PaaS, and IaaS. A determination will be made for where the project fits within the VAECE.

- Future use of cloud solutions at VA will be managed through the ECMP, a standard management platform that is part of the VAECE. Projects will leverage enterprise IT asset management capabilities to keep track of SaaS/PaaS/IaaS subscriptions that are monitored by VA through the ECMP.
- Applications are complex and integrated with many components in today's enterprise architectures. Some may be more cloud-ready than others, and some may be more difficult and expensive to migrate, depending on many technical, operational, security, business, and other factors.
- Cloud migration plans are being developed that take into account the mission critical applications that meet VA business needs. These migration plans are based on a cost-benefit analysis, with regard to on-premises, off-premises, and hybrid approaches. Note that application migration planning usually consumes 40-50% of migration time per industry partner.
- Future capabilities under development include the ECMP tools, Cloud Access Security Brokers (CASBs), API Gateway, CMP, and CI/CD tools for managing multi-cloud CSP cybersecurity, application APIs, and for supporting rapid DevOps deployments.

3.1 Key Attributes of a Transition to Cloud Framework

The key attributes of a Transition to Cloud Framework include the following:

- Utilizes the VAECE as the transition target
- Flexible enough to be adjusted to meet individual application needs
- Infrastructure, platform, and/or common software/services (networks, servers, operating systems, storage, applications, etc.) are managed by the VAECE service provider(s) and IT Operations and Services (ITOPS)
- Improves asset utilization and productivity in application development and management
- Provides a subscription service that is fully integrated with the ECMP
- Provides a measured service and consistent performance, utilizing the VAECE monitoring capabilities
- Leverages the VAECE capabilities:
  - Processes data in parallel and/or has the ability to utilize the scalable, distributed, and computational nature of a cloud environment
  - Provides an on-demand-based business functional service that is accessible to both IT and business users

    - Provides capability in near instantaneous increases and reduction in capacity, acting more responsively to urgent agency needs
    - Provides rapid scaling that is based on demand, and that does not require user interaction, generally resulting in lower costs
    - Provides a multi-tenant environment for a wide variety of VA customers, enabling resource and cost-sharing among a large pool of users
    - Provides minimized capital expenditure (CapEx) – infrastructure is provider-owned and transfers spending to an Operational Expenditure (OpEx) Model
- Provides guidance for cost/benefit analysis and comparison
- Begins with a small environment and expands as needed
- Reduces impact by performing migration in a service window that creates minimal downtime or no downtime at all
- Takes into account that workload or business transition occurs for many reasons:
    - Imposed timeline for migration – If the hardware, software, or hosting contract is falling out of support, the business may have a tight deadline to move the business process to a new environment
    - Improve service – The existing platform may not be providing the features or performance necessary to meet business expectations
    - Lower costs – Moving an existing application to a CSP may lower hosting or internal charge-back costs
    - Modernization – Application modernization is usually refactoring, unless it is the operating environment itself that needs to be updated
    - Compliance changes – Sometimes changes to compliance rules can best be implemented by migrating the application to an environment that already supports the new rules

An example of the framework is below in Table 1.

Table 1: Cloud Transition Framework

Select	Provision	Manage
• Identify which IT services to move and when • Identify sources of value for cloud migrations: efficiency, agility, innovation • Determine cloud readiness:	• Aggregate demand at Department level where possible • Ensure interoperability and integration with IT portfolio • Contract effectively to	• Shift IT mindset from assets to services • Build new skill sets as required • Actively monitor SLAs to ensure compliance and continuous improvement

Select	Provision	Manage
security, VAECE, government readiness, and technology lifecycle	ensure agency needs are met • Realize value by repurposing or decommissioning legacy assets and redeploying freed resources	• Re - evaluate vendor and service models periodically to maximize benefits and minimize risks

Framework is flexible and can be adjusted to meet individual agency needs.

Journey for cloud adoption includes the following:

- Align cloud and business strategy: Understand the agency mission, strategy needs, and requirements. Incorporate the business requirements into the Cloud Adoption Strategy. Leverage the EA. Engage stakeholders and develop a business case and total cost of ownership (TCO). Aligning cloud and VA's overall business priorities will improve the ability to focus on key mission areas.
- Rapid discovery and planning: Baseline capabilities, fill gaps, evaluate, and plan. Fully understand and document the opportunities to develop cloud capabilities. Plan the journey and develop a unique strategic adoption roadmap.
- Execute the plan: Assemble migration focused project teams.
- Realize and sustain business value: Integrate best practices. Run, measure, and report the value of cloud services. Look for opportunities to enhance, simplify, and optimize the environment. Update the business case and TCO models to account for cloud-based Enterprise Shared Services (ESS).
- Innovate and transform: Increase the value of the cloud by incorporating a DevOps approach of continual improvement. Review the applications and develop a strategy to innovate and transform the application portfolio. Develop a cloud first strategy that includes agile application development and a fail fast system, increasing application value to the business. Please refer to PaaS and Microservices EDPs for further information.

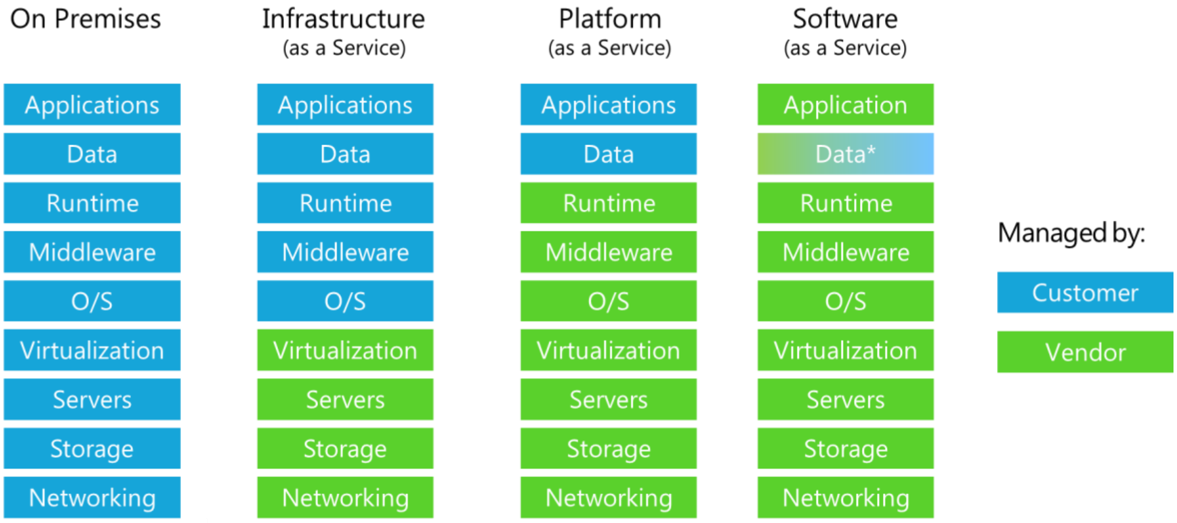
3.2 Service Model Selection

The three major service models defined by NIST are SaaS, PaaS, and IaaS. **SaaS** is defined as the capability for consumers to run the provider's applications on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface or a program interface. 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. SaaS helps get applications to market faster, creates value faster, innovates faster, and generates a flexibility to implement change. SaaS business applications are continuously updated, not only to improve functionality, but for security and usability, including the ability to patch and provide bug fixes that are transparent to the user.

PaaS is a capability provided to the consumer to deploy consumer-created or acquired applications. Acquired applications are created through the use of programming languages, libraries, services, and tools that are supported by the provider to the cloud infrastructure. To be consistent with VA Enterprise Cloud definitions, the consumer does not manage or control the underlying cloud infrastructure. This includes networks, servers, operating systems, and storage. The consumer does have control over the deployed applications. The consumer does have possible control over the configuration settings for the application-hosting environment.

IaaS is a capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources. The consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure. The consumer does have control over operating systems, storage, and deployed applications. The consumer may also have limited control over selecting networking components.

The VA Cloud First Policy states that all solution architectures are subject to the Veteran-focused Integration Process (VIP). Project teams will evaluate approved CSP applications in the One-VA Technical Reference Model (TRM), and integrate with the ECSM. If business requirements dictate that a cloud solution is not feasible, the project teams will coordinate with the Enterprise Program Management Office (EPMO) and ITOPS to determine a viable hosting environment within VA’s IT infrastructure.



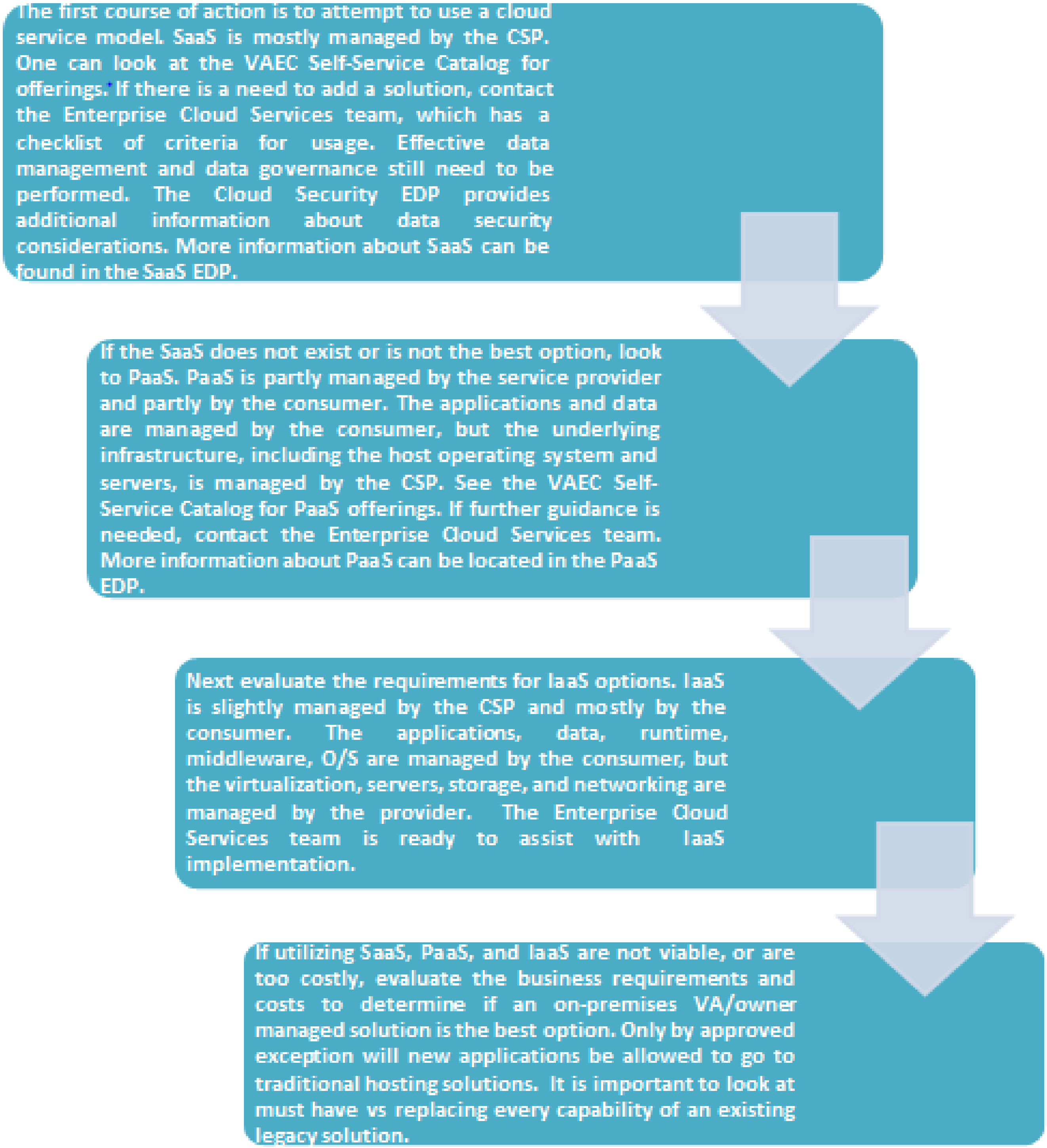
*Customer owns the data, and chooses what data to place in SaaS solution
CSP is the custodian of the data

FIGURE 4: CLOUD SERVICE MODEL COMPARISON PROVIDED BY INDUSTRY PARTNER

The above figure depicts the comparison of the cloud service models and on-premises options.

When transitioning to the cloud, projects focus on business and mission needs. The business/mission merits must be weighed against the VA EA to select a cloud service model within the VAECE. This includes a cost/benefit analysis and an alignment with business needs and functions. In general, it works best to choose a service model that requires the least amount of effort by the consumer, with as much reliance on the provider as possible. This frees the consumer to focus on other specialized tasks.

It is often helpful to prioritize the selection of the cloud service models of SaaS, PaaS, or IaaS sequentially, beginning with SaaS. The figure below depicts the order of service model selection:



The first course of action is to attempt to use a cloud service model. SaaS is mostly managed by the CSP. One can look at the VAEC Self-Service Catalog for offerings. If there is a need to add a solution, contact the Enterprise Cloud Services team, which has a checklist of criteria for usage. Effective data management and data governance still need to be performed. The Cloud Security EDP provides additional information about data security considerations. More information about SaaS can be found in the SaaS EDP.

If the SaaS does not exist or is not the best option, look to PaaS. PaaS is partly managed by the service provider and partly by the consumer. The applications and data are managed by the consumer, but the underlying infrastructure, including the host operating system and servers, is managed by the CSP. See the VAEC Self-Service Catalog for PaaS offerings. If further guidance is needed, contact the Enterprise Cloud Services team. More information about PaaS can be located in the PaaS EDP.

Next evaluate the requirements for IaaS options. IaaS is slightly managed by the CSP and mostly by the consumer. The applications, data, runtime, middleware, O/S are managed by the consumer, but the virtualization, servers, storage, and networking are managed by the provider. The Enterprise Cloud Services team is ready to assist with IaaS implementation.

If utilizing SaaS, PaaS, and IaaS are not viable, or are too costly, evaluate the business requirements and costs to determine if an on-premises VA/owner managed solution is the best option. Only by approved exception will new applications be allowed to go to traditional hosting solutions. It is important to look at must have vs replacing every capability of an existing legacy solution.

FIGURE 5: ORDER OF CLOUD SERVICE MODEL SELECTION

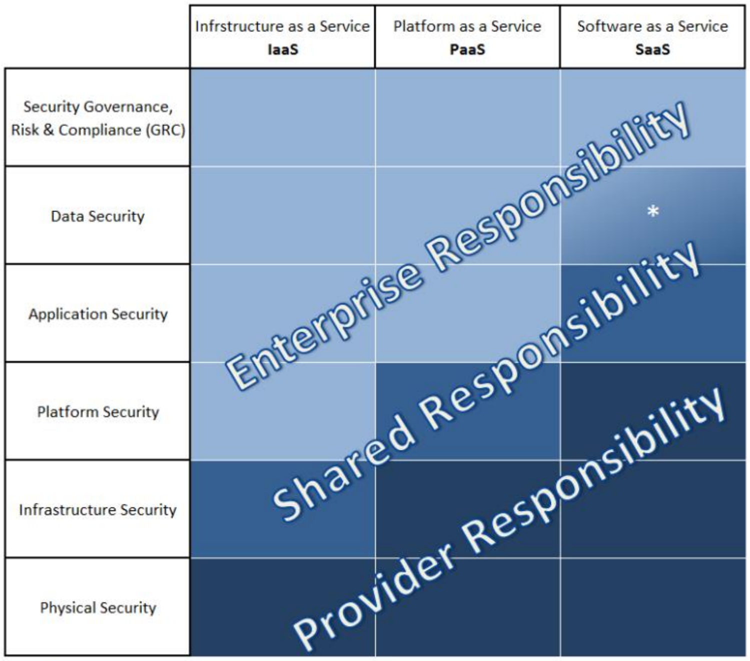
Note that it is possible to consider switching from the current CSP to an alternate one for the same service model. For example, if a solution is deployed on the SaaS model for a given CSP, the need may arise to migrate to another CSP. Another possibility is that it may become necessary to choose an orchestration of solutions that may span multiple CSPs.

The security responsibilities for cloud services are shared differently among different cloud service models. This can be seen in the figure and list that follows.

- Physical security is the provider's responsibility in all models
- Infrastructure security:
    - Owned by the provider for PaaS and SaaS
    - Jointly shared by the provider and the enterprise (consumer) for IaaS
- Platform security:
    - Enterprise is responsible for IaaS
    - Provider is responsible for SaaS
    - Shared responsibility by the provider and the enterprise for PaaS
- Application security:
    - Enterprise is responsible for IaaS and PaaS
    - Shared responsibility by the provider and the enterprise for SaaS
- Data security:
    - Enterprise is responsible for IaaS and PaaS
    - Provider delivers data security for SaaS
- Security governance, risk, and compliance (GRC) is the enterprise responsibility for all the service models

As an example, if an organization is small and does not want responsibility for infrastructure security or physical security, then it may choose SaaS. On the other hand, a large organization that wants to own application and data security may choose IaaS or PaaS in order to have more control over security.

Note that providing security also consists of defining security requirements. Further information on security can be found in the Cloud Security EDP.



* Enterprise Responsible for the security ***of*** the data; Provider provides security ***for*** the data.
Source: (ISC)2 Official Certified Cloud Security Professional Training Guide (2016)

Figure 6: Cloud Security Responsibility Model Comparison Provided by Industry Partner

The asterisk has hidden risk for VA and will need to ensure the SaaS provider meets all data privacy, security, and compliance requirements for handling electronic protected health information (ePHI), personally identifiable information (PII), financial data, DNA/genomics, bio-metrics, and other applicable requirements.

3.3 Data Migration

When planning for a data migration, VA needs to determine how much data is being moved and how long the transfer will take using its existing internet connection. When VA migrates data from on-premises to cloud storage services, VA wants to take the least possible amount of time to move data over the internet connection, with minimal disruption to existing systems. The bandwidth that is being used for data migration will not be available for VA's typical internet traffic.

In addition, VA may be concerned with moving sensitive business information from its internal network to a secure cloud environment. The security level can determine the cloud services that are necessary for data migration. VA needs to identify the data elements and number of unique records involved to ensure that appropriate policies are applied and understood. The policies should be based on how to best handle and safeguard VA's information, as part of an overall data governance strategy. For more information about data security, please see the future capabilities guidance in the sections on TIC compliance and cloud encryption in the Cloud Security EDP.

The VAECE's approach is to create a dedicated direct connection between the VA network and various CSPs included in the VAECE. This will enable VA to transfer data directly, without accessing the internet. Although this is a direct approach, an investment in dedicated connections is necessary for implementation of this option. Alternatives may be used while dedicated connections are established and as CSPs are added to the environment.

If the data is too large to move over the network in a timely manner, it is possible to store it on local moveable storage media. Encryption and chain of custody process and procedures should be established. This includes an authorized delivery provider that meets VA requirements and standards for data privacy and security. The media can then be shipped to the CSP. The provider then handles the storage and places it in the cloud in an operation referred to as bulk transfer. Bulk transfer is especially useful for large quantities of data that can bog down networks. After the bulk transfer is complete, the application can move any updates to the cloud to synchronize the data. This approach may not be an ideal solution if the data can be transferred via the internet within a short period. If applications cannot tolerate the offline transfer time, the data should be moved ahead of the cutover time period.

Data migration requires the performance of thorough testing on the cloud, with real data before it goes into production. When transitioning data to the cloud, the cloud and legacy should be run in parallel. The establishment of a disaster recovery plan is necessary in case of failure. Data loss prevention should be a primary focus. Data should be fully backed up before the migration occurs.

Data migration needs to follow the established data governance, a quality control discipline for assessing, managing, using, improving, monitoring, maintaining, and protecting organizational information.

3.4 Cost/Benefit of Cloud Migration

The transition to cloud services has financial, budgetary, and acquisition implications. Some of the variables for consideration in the cost/benefit analysis include cost of operating data centers and corresponding infrastructure. The numbers of users to support as well as the cost impact of using a private or public cloud are also key variables to consider. VA will address these at strategic and operational levels. The major CSPs have calculators on their websites where one can input compute engine, cloud storage, networking, servers, databases, applications, and IT labor. The calculator generates a TCO. An example of this can be seen by choosing 20 Virtual Machines, 2 CPU cores, 12 GB of memory, and 10 TB of storage. A major cloud provider states that for this example, cost savings would be 79% per year ([On-premises server is $139K / storage is $80K / network $15K – total $233K] vs. [CSP server is $40K, storage is $10K, network $0K – total $50K]). If the benefits outweigh the costs, then one should consider migrating to the cloud.

Migration to cloud services will shift the cost model from CapEx to OpEx, resulting in significant cost savings, in most cases. This is especially true when moving to a Pay-As-You-Go (PAYG) Model, when there is little utilization of cloud bandwidth. In general, PAYG is a more affordable approach, with accrued benefits and cost reductions during each iteration of cloud migration.

The benefits of transition to cloud address time, risk, innovation, and cost factors. This includes faster projects starts and completions, faster provisioning of users and environments, and faster responses to mission priorities. It could require less time provisioning for patching, backups, and recovery. There is a consistent implementation of security standards, decreased risk of insider threat, and increased compliance with government mandates. Cloud enables faster innovation and improved performance. Cost benefits generally include lower capital expenses, lower TCO, and reduced contractor labor.

As VA shifts to a service-oriented enterprise, cloud migration will include assessments of existing capabilities and cost-benefit analysis. VA will leverage private, off-site virtualized environments, and commercial CSPs. Shared computing resources can be utilized. This will help VA capitalize on rapid elasticity, on-demand self-service, broad network access, resource pooling, and measured service to meet growing capacity needs. This allows VA to trade off a costly CapEx Model with OpEx and adapt to rapidly changing requirements. VA will maximize computing power, minimize server sprawl, and ultimately pay only for what is used. In addition to the agility, accessibility, and capabilities that cloud computing offers, the switch from a depreciative CapEx to a renewable OpEx will generally cut costs. To maximize the benefit of this approach, VA is creating the VAECE to provide a consistent cloud capability that leverages shared services and minimizes duplication of efforts and costs that are incurred with many independently acquired and managed cloud solutions.

Moving to the cloud is not always the best approach. If the cost of using the cloud is prohibitive, the solution will not be considered cloud-ready. As an example, if terabytes of data exist in a medical records system, the performance and requirements needed to support the cloud model (network, cost) are important factors. The wide area network (WAN) may not be able to handle the required volume and latency issues. Even if the latency issues are taken into account, the cost may be high and impractical. The costs of recovery of data or moving data to a different CSP or VA's private cloud stack should also be considered. Data extraction or replication for back-up and analytics may have real costs that need to be factored into the overall cloud costs for the different LOBs.

In addition, some applications can be so intertwined in legacy systems that a transition is determined to be overly burdensome. (Often, a Lift-and-Shift migration can be applied if refactoring is difficult.) From a budget perspective, cloud services are consumption-based and can fluctuate dramatically from month to month. For this reason, effective monitoring is essential.

3.5 Retirement of Legacy System

When moving to the cloud, it is often imperative to decommission legacy systems. The process for doing this can be complicated. In general, a step-by-step mechanism is needed. The following is an example of the actions that are necessary to retire a legacy system.

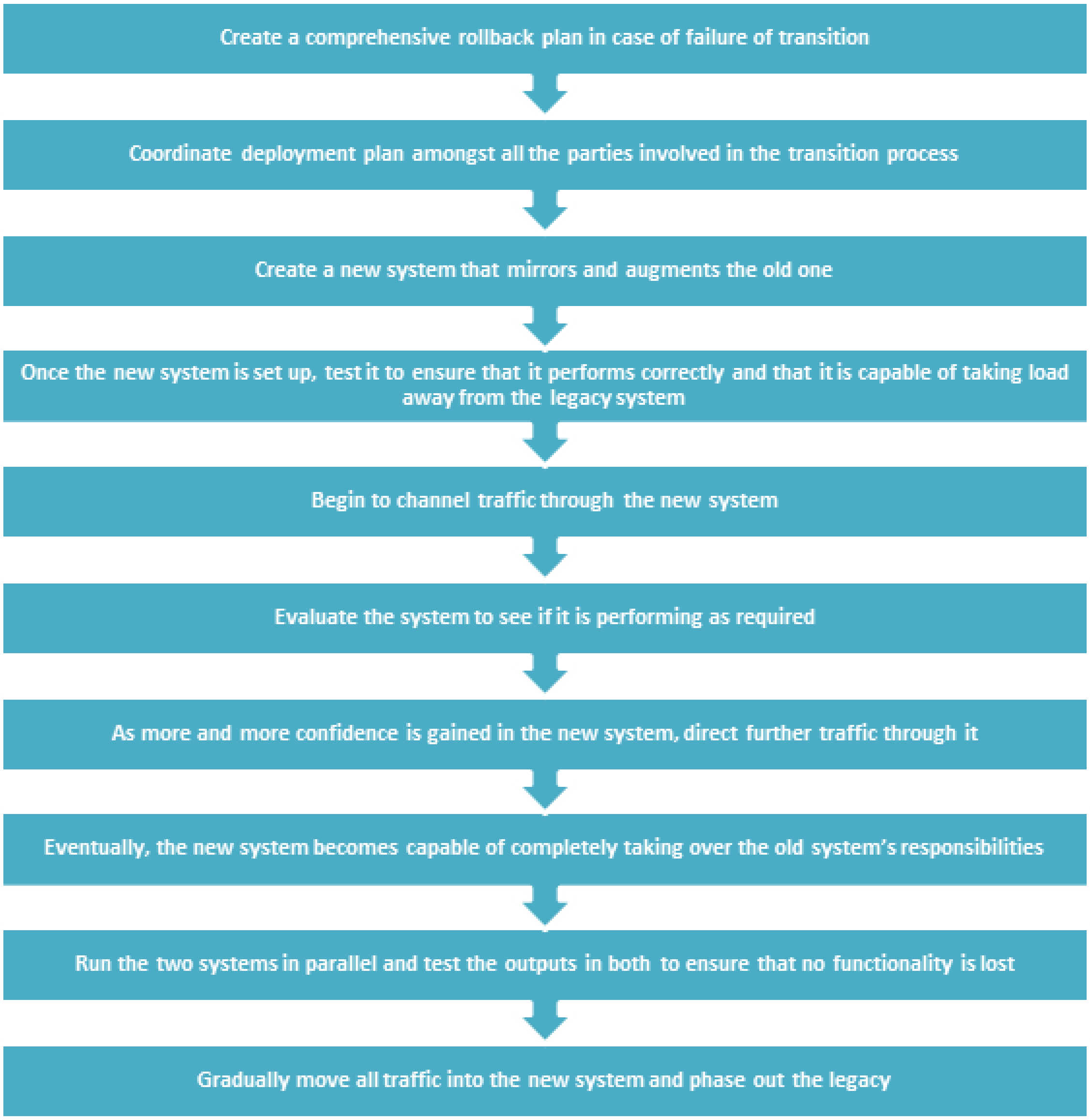

Create a comprehensive rollback plan in case of failure of transition
Coordinate deployment plan amongst all the parties involved in the transition process
Create a new system that mirrors and augments the old one
Once the new system is set up, test it to ensure that it performs correctly and that it is capable of taking load away from the legacy system
Begin to channel traffic through the new system
Evaluate the system to see if it is performing as required
As more and more confidence is gained in the new system, direct further traffic through it
Eventually, the new system becomes capable of completely taking over the old system's responsibilities
Run the two systems in parallel and test the outputs in both to ensure that no functionality is lost
Gradually move all traffic into the new system and phase out the legacy

FIGURE 7: EXAMPLE OF RETIREMENT OF LEGACY SYSTEM PROCESS FLOW

Process flows will vary, based on different types of systems, complexities, opportunities to migrate, and dependencies between different parties involved.

As a caveat, there are alternative courses of action for a legacy system. Modernization or replacement with commercial-off-the-shelf (COTS) products may also be possible. This is based on several factors, such as operating costs, number of users, vendor support, and ease of migration to the cloud. (Is the software 40 years old and the vendor out of business? Can Lift-and-Shift be performed or is it necessary to refactor the business logic first?) The business workflow and process, the efficiencies gained, and the activity-based cost savings should factor into the overall decision when refactoring. Also, the legacy system costs that have an annual increase in budget to maintain overtime should be considered. Lift-and-Shift of a legacy system may be easier, but may lack significant benefits. While refactoring includes a larger initial investment, the benefits can make the investment worthwhile.

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

The EDP and the One-VA TRM are authoritative sources that can be combined to lead to a more coordinated approach to project management and compliance. The One-VA TRM identifies the technologies and standards within the VA production computing environment that can be used at VA; and it determines the conditions for how they can be used. The One-VA TRM also enables users to request an assessment of a new technology, or a new version of an existing technology, and to interpret assessment results. The List of Approved Tools and Standards Table below enables users to easily search for comparable technologies at the One-VA TRM. Please note that the most current list of approved tools and standards are available at the One-VA TRM on the internal VA network.[1]

Table 2: List of Approved Tools and Standards

TRM Domain	TRM Area	TRM Category	Example Approved Technologies
Systems Management	Systems Management Tools	Application Management	Azure PowerShell, Citrix XenApp
Systems Management	Systems Management Tools	Data Center Automation Software	HP Command View EVA
Platforms and Storage	Operating Systems	Application and OS Deployment	BMC BladeLogic Middleware Automation
Platforms and Storage	Cloud Services/Server Virtualization	Cloud Technologies	CloudForms, EMC Atmos GeoDrive, iCloud, Heroku, OpenShift Enterprise, OpenStack,
Platforms and Storage	Storage	Operational Recovery	Atlantis USX, Spectrum Protect for Space Management
Platforms and	Cloud	Virtualization Software	Linux Containers (LXC), IBM

[1] The most current list of authorized software is located at the One-VA TRM on the internal VA network for authorized users at http://trm.oit.va.gov/. Vendors may view a database that is updated less frequently at One-VA TRM at https://www.oit.va.gov/services/trm/.

TRM Domain	TRM Area	TRM Category	Example Approved Technologies
Storage	Services/Server Virtualization		WAVE for z/VM, VMware Tools, VirtualBox, Citrix XenApp
Platforms and Storage	Miscellaneous	Other	Veritas Enterprise Administrator
Application Technology	Development Tools	Build and Deployment Tools	Docker
Systems Management	Systems Management Tools	System Change and Configuration Management	IBM WAVE for z/VM
Systems Management	Systems Management Tools	Mobile Device Management	PhoneView
Systems Management	Systems Management Tools	Asset Management	PhoneView
Systems Management	Systems Management Tools	Data Center Automation Software	BMC BladeLogic Middleware Automation
Systems Management	Systems Management Tools	Monitoring	CA Systems Performance for Infrastructure Managers (SPIM)

3.7 Alignment to Veteran-Centric Integration Process (VIP)

All projects that are subject to VIP will evaluate cloud-based services prior to making decisions about on-premises development, testing, and operations. This process will include conducting cost/benefit analysis of cloud. All cloud-based services are constrained by approved providers that are located in the One-VA TRM, which satisfy the attributes discussed in this document. Projects will evaluate approved hosting environments and cloud solutions during the Project Phase; this consists of completing certification and accreditation and determining FISMA rating. Projects will include cloud solutions in the final designs that are evaluated prior to VIP Critical Decision 2.

3.8 Summary

The following table highlights key areas of content.

Table 3: Summary of Transition to Cloud EDP

Section #	Highlights
3.1 Key Attributes of Transition to Cloud Framework	VA will need to create a framework that is flexible enough to be adjusted to meet individual agency needs. VA framework will provide guidance for cost/benefit analysis and comparison.
3.2 Service Model Selection	VA projects will select cloud service models in the order of SaaS, PaaS, IaaS, and on-premise solutions. VA security accountability is shared differently among different cloud service models.
3.3 Data Migration	VA can implement data migration over an internet connection, via a dedicated connection, or it can be shipped using moveable storage media.
3.4 Cost/Benefit of Cloud Migration	VA can enjoy the benefits of pay-as-you-go, elastic, and scalable systems. However, at times, costs can be prohibitive, so a move to the cloud needs to be well thought out.
3.5 Retirement of Legacy System	VA must develop a plan to phase out its legacy systems. The process may be complicated, and may require failover systems in parallel to implementation of new systems.

4 Use Cases

4.1 Lift-and-Shift Cloud Migration

4.1.1 Purpose

Reduce the IT footprint and operating costs by migrating VA on-premises software and infrastructure to the VAECE. The Lift-and-Shift type of migration usually requires minimal effort to move applications, resulting in faster migration and deployment.

4.1.2 Assumptions

- Security requirements for integrating the cloud services are met per FedRAMP and VA cloud security handbook.
- The VAECE has been deployed and is in use to manage the cloud services that are consumed by VA.
- The application starts in a non-cloud environment and moves to the VAECE.
- The application cannot be taken down for maintenance.

4.1.3 Use Case Description

- VA OIT performs an analysis of the current architecture of its IT systems.
- VA assesses the feasibility of a cloud solution for migration.
- If there appears to be feasibility, VA implements a proof of concept using a fork-lifting approach (moving the system as-is directly to the cloud).
- As part of the proof of concept, there is a utilization of the VAECE or the EDE, or Veterans Health Administration (VHA) Future Technology Labs capability as appropriate.
- VA validates the proof of concept and obtains the lessons learned from the implementation.
- VA adjusts the proof of concept as necessary, based on lessons-learned.
- Depending on the results of the evaluation, VA makes a “go” or “no-go” decision about whether to expand the proof of concept for a full migration.
- If the result of the evaluation is not successful, OIT does not migrate to the cloud at this point in time.
- Assuming the proof of concept is successful, OIT makes the decision to expand the proof of concept to full cloud migration.
- As part of the expansion, data is migrated to the cloud.
- The next phase involves migrating applications to the cloud.
- OIT completes full migration to the cloud.
- OIT optimizes performance of the cloud, and implements modifications based on usage trends and lessons learned.

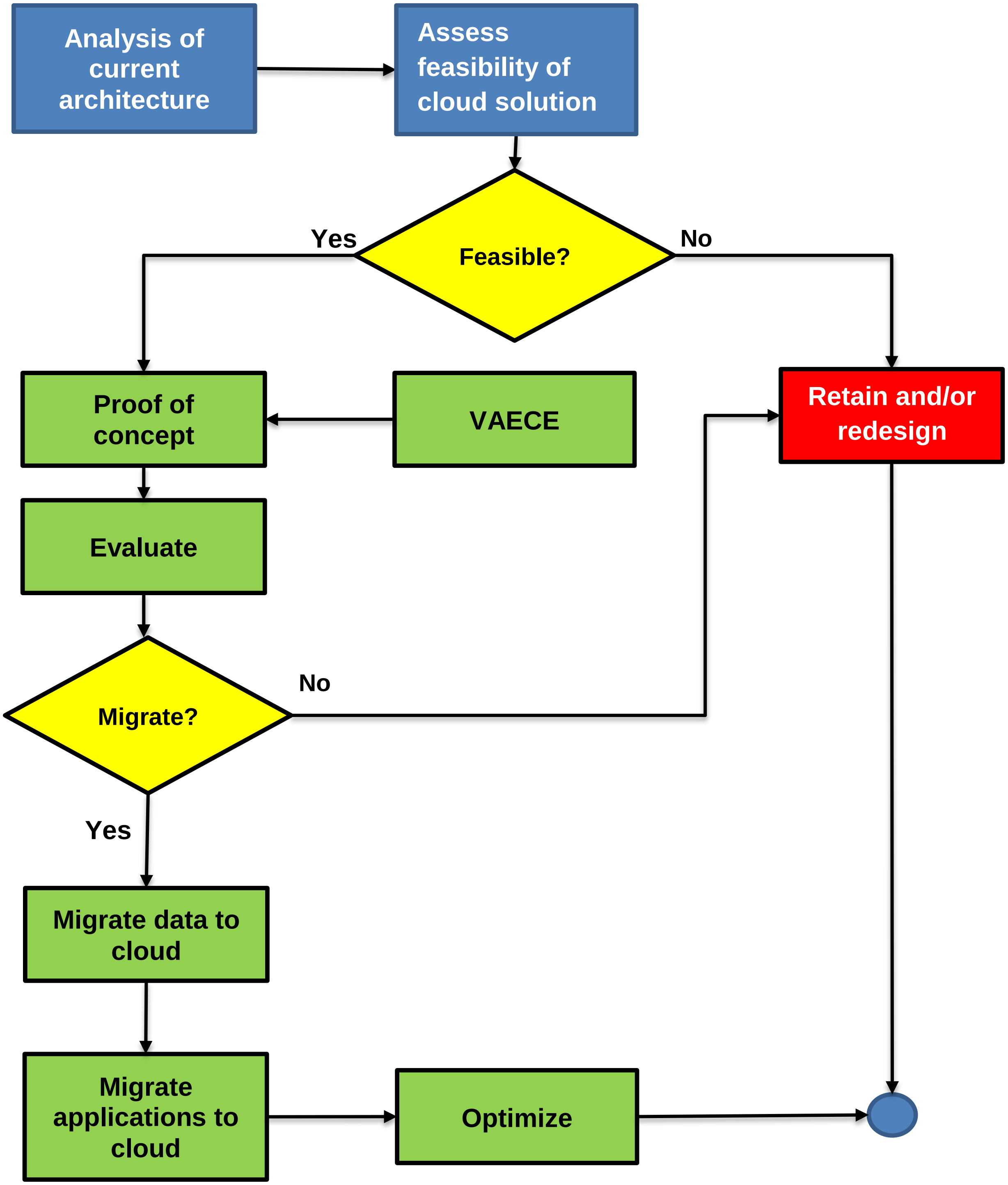


Figure 8: Life-and-Shift Cloud Migration

4.2 Refactoring Migration

4.2.1 Purpose

The following use case provides an example of how VA can use a refactoring approach to migrate applications to the cloud. The refactoring migration usually requires considerable effort, but can lead to greater efficiency in the long term.

4.2.2 Assumptions

- Security requirements for integrating with the cloud services are met per FedRAMP and VA cloud security handbook.
- The VAECE has been deployed and is in use to manage the cloud services that are consumed by VA.
- The application starts in a non-cloud environment and moves to the VAECE.
- The application cannot be taken down for maintenance.

4.2.3 Use Case Description

- VA OIT performs an analysis of the current architecture of its IT systems.
- VA analyzes the business functions that the current systems provide.
- The IT systems are logically broken down into its components. Some recoding may be required for this refactoring process.
- The current component logical grouping is decoupled from the rest.
- Data is migrated to the cloud for the component in question.
- Applications are migrated to the cloud for the current component.
- Optimization of the current component/system is completed.
- If there are additional components remaining, a migration for those components occurs.
- The process continues until all of the components are migrated.

This high level process flow is depicted in Figure 9 below:

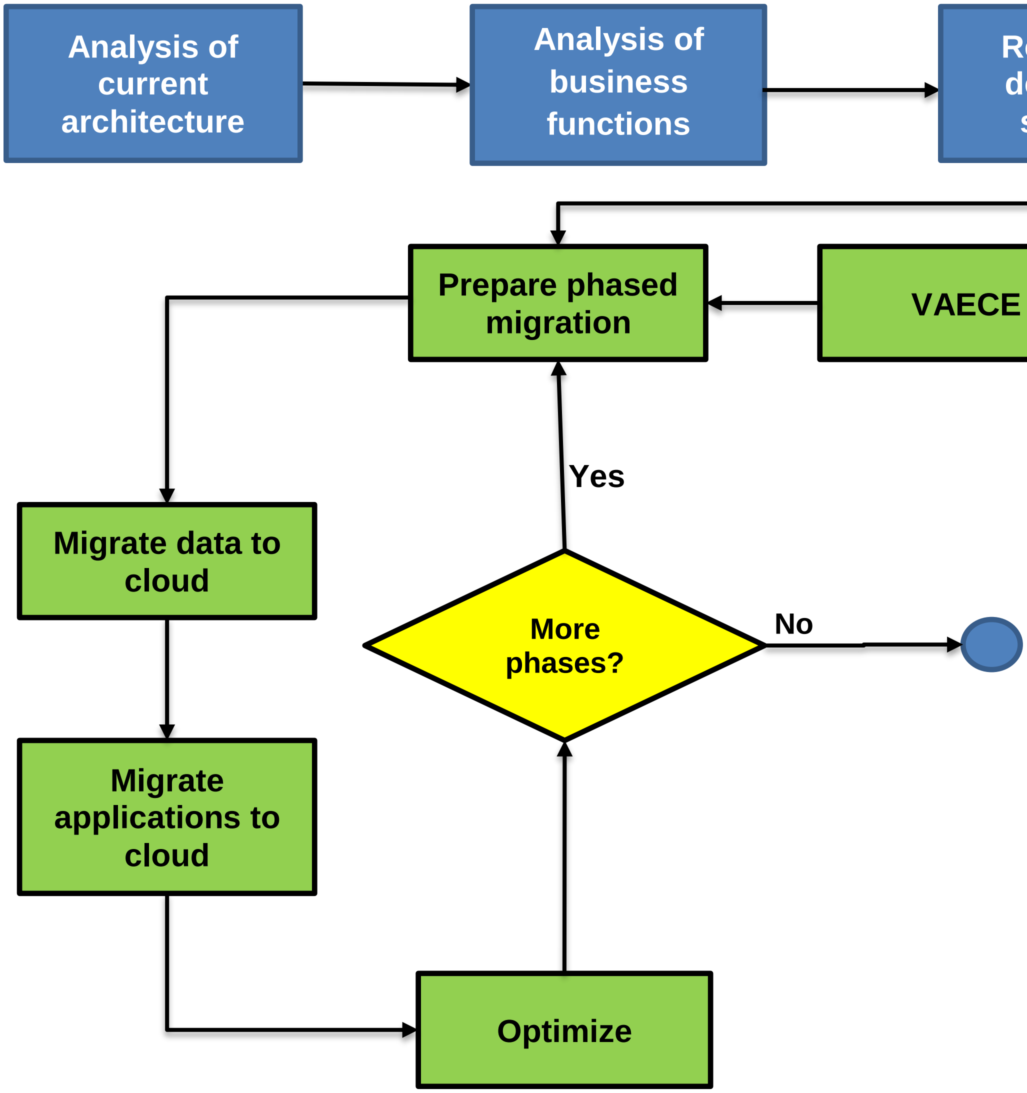

Analysis of current architecture
Analysis of business functions
Refactor / decouple system
Prepare phased migration
VAECE
Migrate data to cloud
Migrate applications to cloud
Optimize
More phases?
Yes
No

FIGURE 9: REFACTORING PROCESS FLOW

APPENDIX A. SCOPE

The Cloud Computing Transition to Cloud EDP defines a framework for the transition to cloud services that are provided by the VAECE:

- What requirements must be known before the determination is made to move to the cloud?
- What are the customer needs that drive these requirements?
- What is the order to consider cloud services (SaaS/PaaS/IaaS)?
- How are best practices and lessons-learned leveraged? (These include leveraging existing Cloud Computing EDPs, Lift-and-Shift migration, refactoring migration, migration of data, risk/vulnerability analysis, cutover, and retirement of legacy version)?

Intended Audience

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

- System and application owners/stewards /portfolio managers/project managers
- Executive leadership in IT (e.g., CIO, division head, etc.)

This document is also intended for those in leadership roles, who can establish governance mechanisms and policies that are related to cloud services.

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across VA, including participation from OIT's EPMO, OIS, and ITOPS pillars. Extensive input and participation was also received from the VHA, Veterans Benefits Association (VBA), and the National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts for review, input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be 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, particularly those related to databases, database management, and data integration.

Key Term	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses services from, cloud providers.
Cloud Provider	A person, organization, or entity that is 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 Carrier	An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.
Microservices	A software architecture style in which a large application is divided into smaller, discrete, and combinable services that communicate with each other through language-agnostic Application Programming Interfaces (APIs).

APPENDIX C. ACRONYMS

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

Acronym	Description
API	Application Programming Interface
ASD	Architecture, Strategy, and Design
ATO	Authority to Operate
CAPEX	Capital Expenditure
COTS	Commercial-Off-the-Shelf
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DevOps	Development Operations
EA	Enterprise Architecture
ECMP	Enterprise Cloud Management Platform
ECSM	Enterprise Cloud Services Management
EDE	Enterprise Development Environment
EDP	Enterprise Design Pattern
ePHI	Electronic Protected Health Information
EPMO	Enterprise Program Management Office
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IAM	Identity and Access Management
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GRC	Governance, Risk & Compliance
IaaS	Infrastructure-as-a-Service
IT	Information Technology
ITOPS	IT Operations and Services
JAB	Joint Authorization Board
LOB	Line of Business
NCA	National Cemetery Administration

Acronym	Description
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OIT	Office of Information and Technology
OIS	Office of Information Security
OPEX	Operational Expenditure
PaaS	Platform-as-a-Service
PAYG	Pay-As-You-Go
PII	Personally Identifiable Information
SaaS	Software-as-a-Service
SDE	Service Delivery and Engineering
SLA	Service Level Agreement
SME	Subject Matter Expert
SOA	Service-Oriented Architecture
SPIM	Systems Performance for Infrastructure Managers
TCO	Total Cost of Ownership
TIC	Trusted Internet Connection
TRM	Technical Reference Model
TS	Technology Strategies
VA	Veterans Affairs
VAECE	Veterans Affairs Enterprise Cloud Environment
VAMF	VA Mobile Framework
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VIP	Veteran-focused Integration Process
VPS	Veterans Point of Service
VRM	Veteran Relationship Management
WAN	Wide Area Network

Appendix D. References, Standards, and Policies

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

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=829&FType=2	Establishes a mandatory policy for establishing and utilizing EDPs by all VA projects that develop IT systems, in accordance with VA OIT integrated development and release management process – VIP
2	VA OIS	VA 6500 Handbook	The directive from the OIT OIS establishes an information security program at VA for 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	VA EA, July 12, 2002
5	VA	VA Handbook 6517	Risk Management Framework for Cloud Computing Services (draft)
6	VA	VA Directive 6517	Establishes VA policy for the adoption of Cloud computing services within VA, in alignment with VA's Cloud Computing Strategy
7	NIST	NIST SP 500-291	NIST Cloud Computing Standards Roadmap, Version 2, July 2013
8	NIST	NIST SP 500-292	NIST Cloud Computing Reference Architecture
9	NIST	NIST SP 800-145	The NIST Definition of Cloud Computing, NIST SP 800-145, Sept. 2011
10	NIST	NIST SP 500-299	NIST Cloud Computing Security Reference Architecture
11	DoD	DoD Cloud Strategy	Department of Defense Cloud Computing Strategy

#	Issuing Agency	Applicable Reference/ Standard	Purpose
12	GSA	Government Accountability Office (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
13	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
14	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
15	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 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
16	Federal	Federal Information Processing Standard (FIPS) Publication 199	FIPS 199
17	Federal	FIPS 200	Establishes minimum security requirements for Federal information and information systems
18	VA	VA Memorandum Consideration of Open Source Software (VAIQ#7532631)	Establishes requirements to evaluate open source software (OSS) solutions and consider OSS development practices for VA-developed software
19	GAO	GAO 16-325	Appendix II - Analysis of Agencies’ Cloud SLAs against key practices

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.