VA Enterprise Design Patterns
Cloud Computing

Software-as-a-Service

Office of Technology Strategies (TS)
Office of Information and Technology (OI&T)

Version 1.0
Date Issued: April 2017

Approval Coordination

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2017.04.20 09:07:16 -04'00'

Gary Marshall
Director, Technology Strategies, ASD

Deeneen U Akeo 622220

Digitally signed by Deeneen U Akeo 622220
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=deeneen.akeo@va.gov, cn=Deeneen U Akeo 622220
Date: 2017.05.08 11:41:56 -04'00'

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

Revision History

Version	Date	Approver	Notes
1.0	April 11, 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

In order to respond to rapidly changing business needs and Information Technology (IT) product capabilities, the Department of Veterans Affairs (VA) requires a standard approach to leveraging Software-as-a-Service (SaaS). SaaS is defined by the National Institute of Standards and Technology (NIST) as a capability provided to the consumer that runs a provider's applications on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or an application programming interface (API). Other than limited, user-specific, application configuration settings, the consumer does not manage or control the underlying cloud infrastructure of network configurations, host operating systems, storage, and individual application capabilities. This Enterprise Design Pattern (EDP) is an extension of the Cloud Computing Architecture EDP, with an emphasis on SaaS.

The VA consensus standard for deploying SaaS consists of the following attributes:

- Provides a fully managed set of business services (e.g., e-mail and Customer Relationship Management [CRM]) that are scalable for enterprise use
- Delivers on-demand IT capabilities that require minimal customization by the Office of Information and Technology (OI&T)
- Allows VA to subscribe to the service provider, pursuant to Service Level Agreements (SLAs) and security requirements that are referenced in the Cloud Security EDP; and within the established Government Accountability Office (GAO) SLAs

Figure 1 illustrates the key components of cloud computing, based on the NIST reference architecture, which enable VA to maximize the benefits of integrating cloud services. In the diagram, the NIST recommendation for the architecture framework for the SaaS component is highlighted in red.

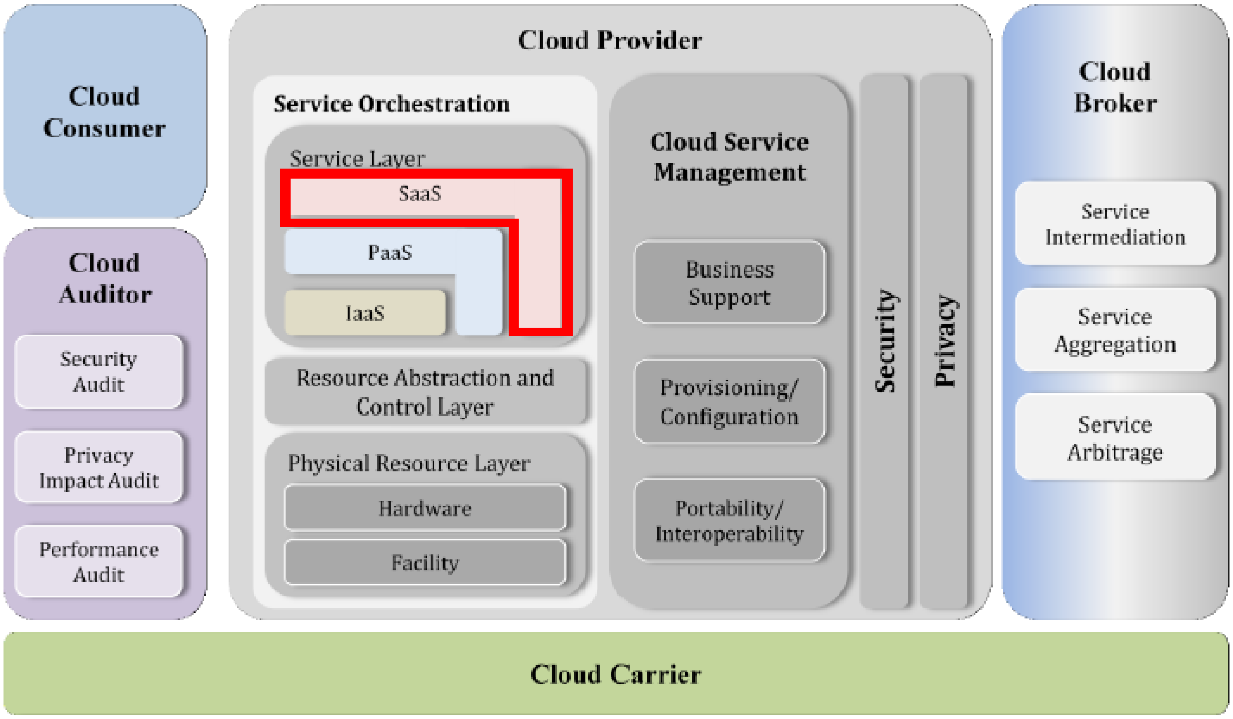


FIGURE 1: ARCHITECTURAL CONCEPT FOR VA CLOUD COMPUTING BASED ON NIST ARCHITECTURE

SaaS delivery models consist of:

- Hosted application management, in which the provider hosts software for the consumer and provides it over the web
- Software on demand, in which the provider gives consumers network-based access to a single copy of an application

1.1 Business Problem

VA requires a more agile IT operating model that provides the ability to rapidly develop, modify, test, and deploy IT capabilities and functionality on scalable, dynamic cloud infrastructure. Across the commercial industry, cloud is now a mainstream delivery platform and market share is increasing dramatically.

Currently, VA does not have a standard approach to evaluating and selecting SaaS solutions to address business needs across all VA Lines of Business (LOBs). Despite VA's adoption of the Cloud First policy (VA Directive 6517), there has been reluctance among OI&T stakeholders to adopt fully managed services. Security concerns and a lack of control over the operating environment have resulted in the tendency to develop custom in-house solutions to business needs, even when more cost-effective SaaS providers are readily available. Therefore, VA OI&T has chosen to implement a VA Enterprise Cloud Brokerage concept to provide and enhance IT services in support of VA's mission capabilities. These efforts combine with strategic policy, tactical support and teamwork by IT Operations, and implementation tools, such as Enterprise Design Patterns (e.g., the Cloud Security EDP), to move VA closer to a Cloud First policy.

1.2 Business Need

VA OI&T can support business needs more efficiently through the use of SaaS providers. SaaS implementation can reduce the code base and development time that streamlines and facilitates agile solutions. SaaS has the potential to simplify development and acquisition of IT capabilities for business operations. VA requires greater awareness of the benefits that a fully hosted and managed SaaS can provide the enterprise.

Cloud computing brings business value to VA. It contributes to savings on capital equipment, operating expenses, and support, while significantly increasing business agility. By optimizing the use of cloud computing, VA will achieve several critical goals:

- Deliver IT systems via mainstream technologies that are flexible and responsive to demand in order to support VA's mission
- Encourage and exploit dynamic and responsive supplier marketplaces and support emerging suppliers
- Achieve economies of scale in IT development and operations, while meeting budgetary and return-on-investment objectives
- Allocate IT expenditures to services and users by shifting from a Capital Expenditures (CAPEX) to an Operational Expenditures (OPEX) model

1.3 Business Case

VA OI&T intends to take advantage of marketplace developments to bring an improved level of agility and cost savings to VA, in support of the Veteran initiatives, while complying with Federal Government mandates, such as FISMA/FedRAMP, FITARA, and Section 508. As VA shifts to a Cloud First approach, it must include an externally managed SaaS as part of its IT service offerings. A SaaS moves the responsibility for software support and improved services to the

SaaS provider, while simultaneously managing costs, enabling innovation, reaching a wider Veteran community, and securely exchanging information among VA partners. SaaS is a managed service that does not require customer maintenance; customization is only conducted through the interface, within the implementation of the service. Managed service is a relationship in which a customer develops customized requirements and the vendor produces a customized solution for the consumer.

The benefits of adopting such an approach include:

- Improved uptime, through built-in availability, that is managed by the service provider
- Reduced need for custom development efforts
- Simplicity from a subscription service that is managed through VA's Enterprise Cloud Service Broker (ECSB)
- Utility computing, paying for only the virtual resources consumed, and leasing instead of licensing
- Elasticity, by dynamically adjusting to future increases in capacity demands, with the ability to meet surges in demand
- Applications and data that can be accessed from anywhere (globally accessible)
- Ease of use
- Standardized software releases
- Automatic updates and patches

1.4 Approach

This EDP defines a framework for using SaaS solutions by addressing:

- VA definitions of the key attributes of SaaS
- VA customer needs that drive SaaS requirements
- Business requirements that drive SaaS decisions
- Industry and government SaaS best practices and lessons learned

Additionally, this EDP formally establishes an architecture standard for evaluating and selecting commercial SaaS solutions 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). For SaaS, this approach consists of the following:

- Gathering business needs and defining requirements:
    - Guide VA to decisions about the business capabilities that can best be supported by a SaaS provider

    - Conduct a review of existing VA applications and determine whether they are cost effective candidates for migration to SaaS cloud environments; cloud provides the potential to help collapse systems and consolidate infrastructure
    - Identify SaaS solutions to incorporate into the ECSB
- Defining the attributes of a SaaS framework:
    - Subscription service
    - Billing and metering functionality (SLA management)
    - Integration through open-standard APIs
    - Security via data protection, Cloud Access Security Broker (CASB), Identity and Access Management (IAM) requirements, threat protection, encryption standards, data ownership, and data policy enforcement
    - Logging and monitoring SaaS usage

2 CURRENT CAPABILITIES AND LIMITATIONS

VA is working to establish a roadmap for incorporating cloud solutions that utilize industry best practices. Specifically, VA is analyzing all applications to determine their readiness to move to the cloud. Current efforts are underway to move e-mail and CRM systems to the cloud. The following subsections leverage these efforts as good use case examples of cloud migration activities. The use cases in Section 4 enable this EDP to highlight various challenges that VA encounters when moving applications to the cloud to implement SaaS solutions.

2.1 Current Software-as-a-Service Offerings

2.1.1 Cloud Email

- VA currently has an on-premises e-mail infrastructure (e.g., MS Outlook and Active Directory). While attempts have been made to migrate to SaaS solutions, the efforts have not been successful.
- VA is in the process of migrating its e-mail infrastructure to Office365, in accordance with the IT modernization efforts of the VA Enterprise Roadmap.
- Enterprise portal services (e.g., MyHealtheVet) are currently on VA premises. Vets.gov is already hosted through a cloud environment.
- Office of Information Security (OIS) and Network and Security Operations Center (NSOC) are currently resolving challenges with Trusted Internet Connection (TIC) integration and data security requirements, in accordance with the Cloud Security EDP.

2.1.2 Customer Relationship Management (CRM)

- Traditionally, Customer Relationship Management (CRM) applications are hosted by a private cloud that is managed by an external company. The CRM environment used in VA, however, is provided by Microsoft Dynamics, a line of enterprise resource planning (ERP) and CRM software applications. The Microsoft Dynamics' applications are delivered through Microsoft Azure, a cloud computing service in which the CRM exists as a SaaS. It is hosted by CenturyLink, an Internet service provider.
- Salesforce, a cloud computing firm whose revenue comes from a CRM product, has also been considered for use as a CRM platform in multiple VA environments. For example, the VA Center for Innovation leverages Salesforce to track workflows that support the transition of pilot projects to enterprise solutions.
- CRM requires a secure connection between on-premises and cloud-based environments prior to a migration to a SaaS solution, in accordance with the Cloud Security EDP

2.2 Current Limitations

- Current offerings that are used by VA and marketed as SaaS solutions may fall short of providing the full characteristics of cloud computing, as defined in the NIST definition. For example, some managed service providers still require a manual configuration of the underlying infrastructure (such as configuration of host operating systems). SaaS, by definition, is a completely managed service that only requires integration with its interfaces in order to provide services to its customers.
- SaaS providers need to meet rigorous Federal Risk and Authorization Management Program (FedRAMP) requirements. These cloud providers require an Authority to Operate (ATO) by the FedRAMP Joint Authorization Board (JAB), as referenced in VA Handbook 6517 and VA Handbook 6500.
- All SaaS providers need to be integrated with the ECSB to address challenges associated with integrating multiple SaaS 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 SLA requirements.

3 Future Capabilities

- As part of the Cloud First policy, VA Directive 6517, project teams will evaluate the recommended type of cloud service, whether it is SaaS, Infrastructure-as-a-Service (IaaS), or Platform-as-a-Service (PaaS), to address their business needs.
    - It is recommended that project teams evaluate SaaS services prior to making decisions about the development of custom solutions.

  - Leveraging a SaaS solution results in significantly less operational management overhead and opens up VA's production environment to private sector innovations.
  - SaaS users are able to focus on "what," rather than "how."
  - A transitional implementation cost may exist because applications migrating to the cloud may require hosting in dual environments during the transition.
- Projects will leverage enterprise IT asset management capabilities to keep track of SaaS subscriptions that are monitored by VA's ECSB.
- Strategic sourcing will be conducted by OI&T to identify SaaS vendors and establish relationships among providers of key VA business functions. Third-party solutions, provided by SaaS vendors, enable OI&T to focus on innovation, rather than infrastructure management.
- OI&T will leverage the ECSB and formalized SLAs to support SaaS products and vendor relationships in a centralized fashion.
- Cloud migration plans are being developed that take into account the mission critical applications that meet VA business needs. These migration plans are developed based on a cost-benefit analysis, with regard to on-premises, off-premises, and hybrid approaches. Further information about One-VA Technical Reference Model (TRM) alignment can be seen in section 3.3.

3.1 Key Attributes of Software-as-a-Service

- Infrastructure and platform (networks, servers, operating systems, storage, etc.) are fully managed by the service provider.
- Provides RESTful open standard API set for management of the business functionality exposed by the service.
- Provides a subscription service that is fully integrated with the ECSB.
- Provides high availability (e.g. maximum uptime) in accordance with SLA guidelines, as provided by the Government Accountability Office (see Appendix D).
- Provides the ability to process data in parallel and/or the ability to utilize the scalable, distributed, computational nature of a cloud environment.
- Provides on-demand-based business functional service that is accessible to both IT and business users.
- Provides rapid scaling that is based on demand that does not require user interaction.
- Provides a measured service that is integrated with the ECSB monitoring capabilities.
- Provides resource pooling that ensures a multi-tenant environment for a wide variety of VA customers.
- Provides broad network access through integration with the VA TIC and the VA Wide Area Network (WAN), to ensure seamless communications.

- Provides the ability to configure web content and display without the need for custom coding.

3.2 Analysis of Service Models

All solution architectures that are subject to the Veteran-focused Integration Process (VIP) shall evaluate approved cloud service providers in the One-VA TRM and integrate with the ECSB. If business requirements dictate that a cloud solution is not feasible, the project teams will coordinate with the Enterprise Program Management Office (EPMO) and IT Operations in order to determine a viable hosting environment within VA's IT infrastructure. The following guidance supports decision-making, using the appropriate decision model to support the business needs of a VA IT project.

- When deploying to the cloud, projects must focus on business and mission needs. The business/mission merits must be weighed against VA's EA to select a cloud solution.
- Based upon the requirements, look first to SaaS to see if there is a ready-made solution (SaaS is a completely managed service, as evident in Figure 2).

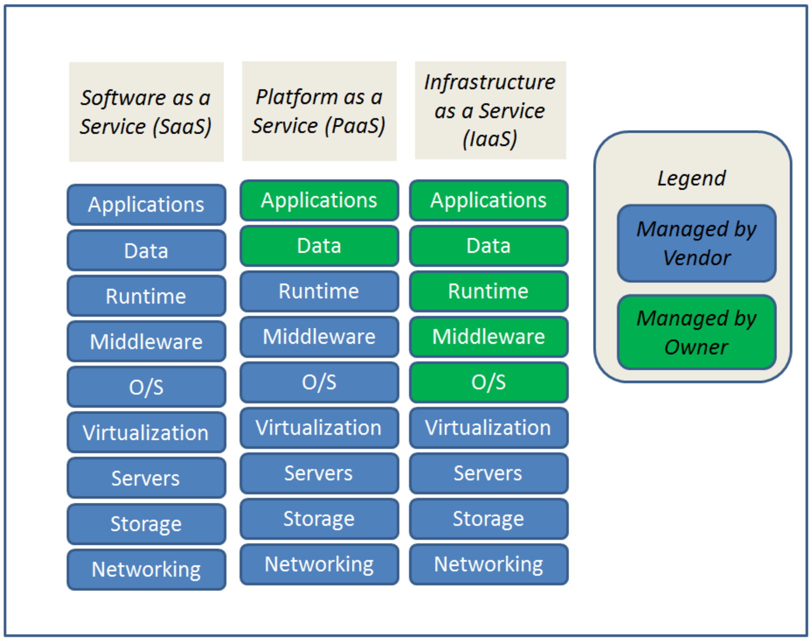


FIGURE 2: DEVOPS PROCESS (VIA VA INDUSTRY PARTNER)

SaaS can be provided by a wide variety of Independent Software Vendors (ISVs), including small or large firms, or a combination that have a business relationship with VA and have met appropriate security requirements.

Note that the consumer is still required to determine the data that goes into the SaaS. Effective data management and data governance still need to be performed and overseen by OI&T Data Governance boards. The Cloud Security EDP provides additional information about data security considerations, such as encryption and transfer of data from one SaaS provider to another.

Please see the table below for further insight on the SaaS governance framework, from the user and cloud provider perspectives, for managing security in the public cloud.

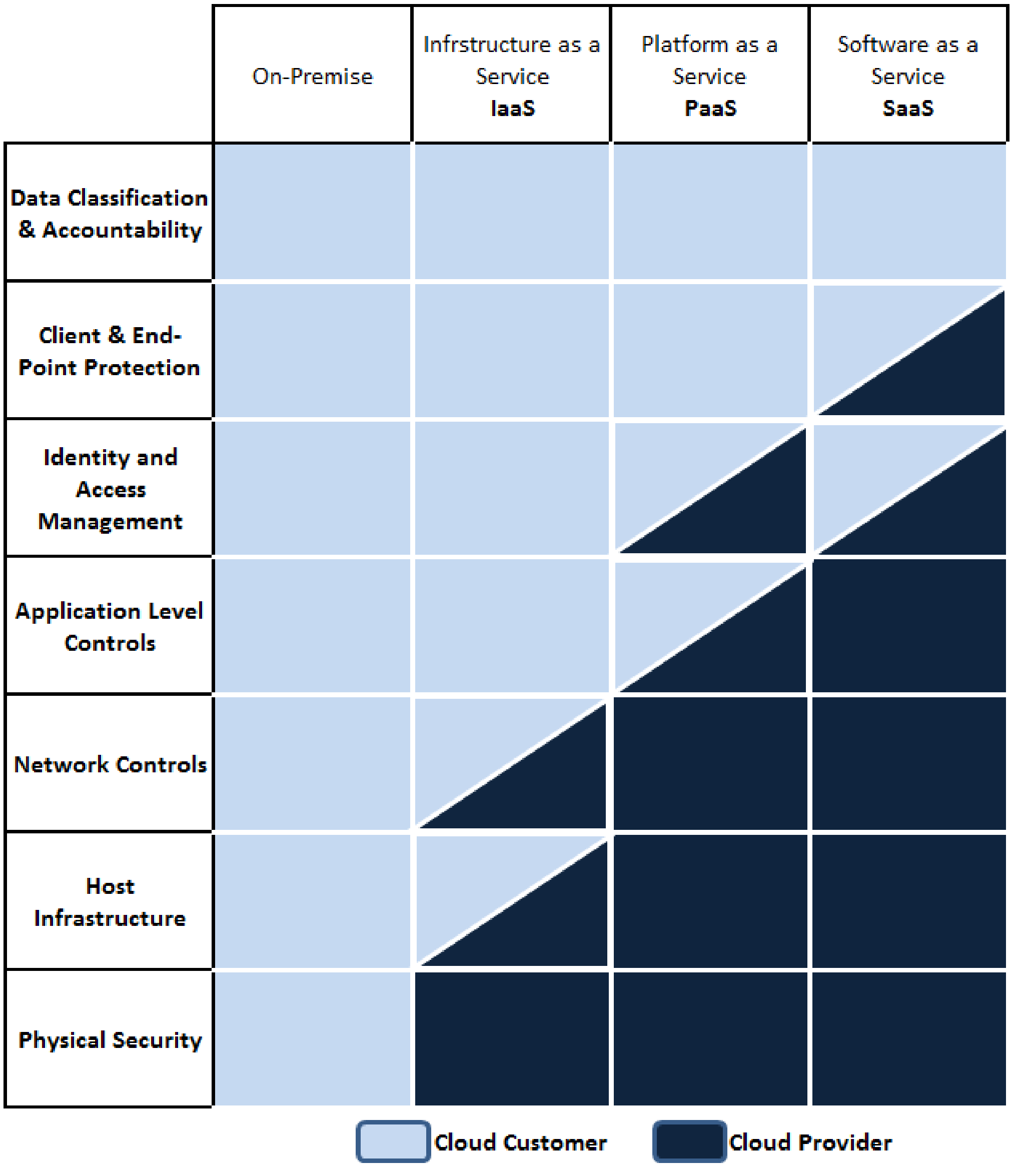
TABLE 1: GOVERNANCE LEVEL ON THE SAAS LAYER

User Responsibility	Cloud Provider Responsibility
Identity Management	Ownership of Physical Structure
Access Control Policy	Physical Security
Authentication	Management of Software Security
Data Loss Prevention	Management of Network Security
Data Policy Enforcement	OS Patch Management
	Incident Response and Resiliency
	Monitoring and Maintenance
	Compliance with Standards and Legal Regulation

In SaaS, the application is developed and maintained by the Cloud Service Provider (CSP). The control and security tends to be higher than the other layers (PaaS, IaaS) because overall responsibility belongs to the CSP. Exceptions to this can be seen in Identity Management, Access Control Policy, and Authentication.

The creation of an iterative process to establish a governance lifecycle framework to address cloud management is important to this effort. This framework helps lessen risks and improve security. It consists of enterprise management, risk management, asset management, security policy, application of security controls, monitoring, compliance, and auditing.

The transition of logical control from the cloud customer to the cloud provider divides responsibility, control, authority, and security, as shown in the figure below. The SaaS layer has minimal control by the user.



	On-Premise	Infrstructure as a Service **IaaS**	Platform as a Service **PaaS**	Software as a Service **SaaS**
Data Classification & Accountability	□	□	□	□
Client & End-Point Protection	□	□	□	◪
Identity and Access Management	□	□	◪	◪
Application Level Controls	□	□	◪	■
Network Controls	□	◪	■	■
Host Infrastructure	□	◪	■	■
Physical Security	□	■	■	■

□ **Cloud Customer** ■ **Cloud Provider**

FIGURE 3: CLOUD SECURITY RESPONSIBILITY MODEL

- If SaaS does not exist or is not the best option, consider the PaaS solution. 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, are managed by the CSP. More information about PaaS can be located in the PaaS EDP.

- If there is no viable PaaS solution, evaluate the requirements for IaaS options. IaaS is slightly managed by the CSP and mostly by the consumer. In the IaaS model, the consumer is responsible for identifying the appropriate compute, storage, and networking capabilities that are virtualized by the cloud provider's hosting environment. Private cloud environments, hosted through VA's enterprise IT infrastructure, provide an IaaS as an alternative to PaaS and SaaS solutions that are provided by public cloud providers.
- If utilizing SaaS, PaaS, and IaaS are not viable, evaluate the business requirements and costs to determine if an on-premises VA/owner-managed solution is the best option.

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

All projects will leverage the approved SaaS providers that are located in the One-VA TRM[1] to comply with the architectural guidance provided in this authoritative source. TRM-approved SaaS providers will be registered through VA's ECSB and include both large software vendors and small business vendors that have established business relationships with VA. Table 1 lists the approved tools for this EDP.

Table 2: List of Approved Tools and Standards

Tool Category	Example Approved Technologies
Cloud Technologies	CloudForms, EMC Atmos GeoDrive, iCloud, Heroku, OpenShift Enterprise, OpenStack, Cloud Foundry, Azure
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, SaltStack, Tivoli Storage Manager for Space Management and Veritas Enterprise Administrator
Data Center Automation Software	BMC Application Automation, SystemEDGE and Microsoft Center Operation Management

3.4 Alignment to Veteran-Focused Integration Process (VIP)

All projects subject to VIP will evaluate cloud-based services prior to making decisions about on-premises development, testing, and operations. All cloud-based services are restricted to One- VA TRM-approved providers that satisfy the attributes discussed in this document. Projects will evaluate approved hosting environments and SaaS solutions during the project phase; projects will include them in the final designs that are evaluated prior to VIP Critical Decision 2.

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

4 USE CASES

4.1 Cloud Email Piloting and Rollout

4.1.1 Purpose

Reduce the IT footprint and operating costs by migrating VA on-premise e-mail servers and infrastructure to a cloud-based e-mail service that is provided by a SaaS vendor. This migration can support business agility by enabling VA's IT infrastructure to respond to concerns that are more focused on traditional VA applications and VA enterprise shared services (ESS). It also enables VA to leverage an externally managed IT infrastructure that meets VA's rigorous security and privacy standards that exist when granted an Authority to Operate (ATO). It is important to leverage a SaaS solution in a prototype – first, in order to apply design thinking, and then to check plausibility.

4.1.2 Assumptions

- Security requirements for integrating the cloud services are met per FedRAMP and VA Cloud security handbook.
- The ECSB has been deployed and is in use to manage the Cloud services that are consumed by VA.
- The e-mail service has already been evaluated and approved by the One-VA TRM.

4.1.3 Use Case Description

- VA OI&T acquires a SaaS e-mail service. SaaS e-mail is being migrated to the Cloud through VA's Cloud broker.
- VA implements a pilot project to demonstrate the viability of the enterprise use of the SaaS e-mail service.
- As part of the pilot, there is a pilot integration of directory services. When migrating to the cloud, there has to be synchronization between on-premises directories and cloud- based directories that are incorporated into the SaaS e-mail provider. Security controls will be in place to ensure Data Loss Prevention (DLP) and data policy enforcement.
- VA executes the pilot and obtains the lessons learned from the implementation.

- Based on lessons learned, the VA pilot is adjusted.
- Depending on the results of the pilot, VA makes a "go" or "no-go" decision about whether to expand the pilot for enterprise use.
- If the pilot is not successful, OI&T retains an on-premises e-mail infrastructure and will evaluate viable SaaS e-mail candidates at a later time.
- Assuming the pilot is successful; OI&T makes the decision to expand the pilot for cloud-based e-mail consumption throughout VA.
- As part of the expansion, OI&T coordinates with the SaaS e-mail provider to determine the course of action for complete migration from the on-premises e-mail infrastructure to the SaaS provider.
- OI&T completes full migration to the SaaS e-mail provider, and completes the synchronization between VA's on-premises directories with those provided by the SaaS e-mail provider.
- OI&T monitors the usage of the SaaS e-mail provider through the ECSB, and implements modifications based on usage trends and lessons learned.

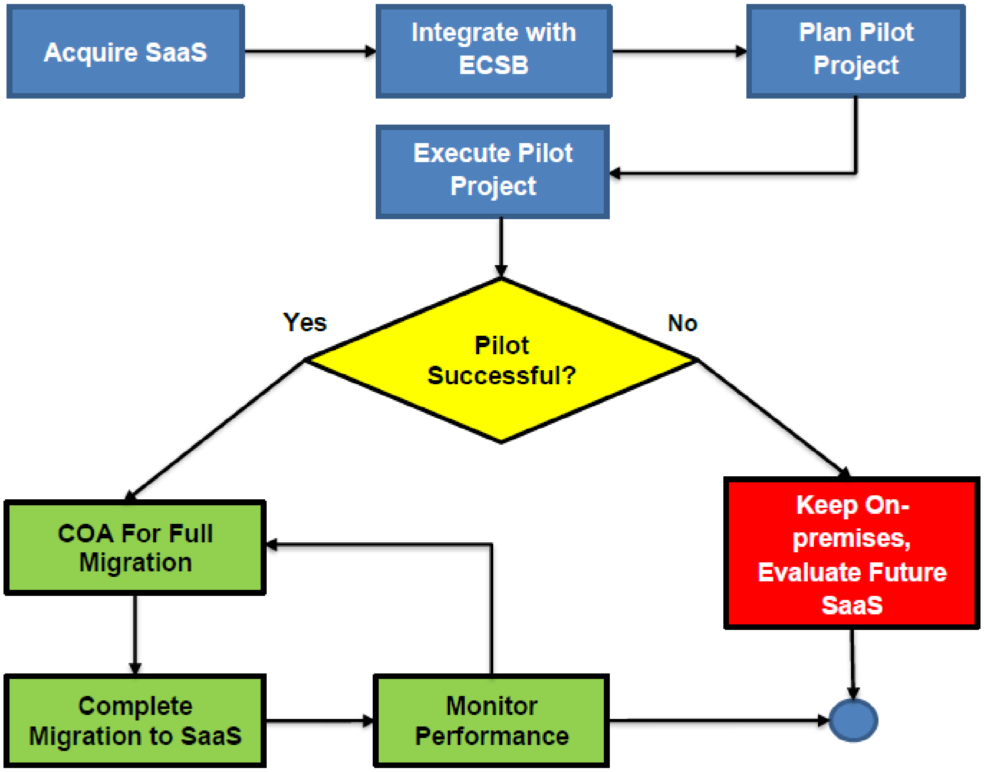


FIGURE 4: PROCESS FLOW OF USING SAAS TO PILOT AND ROLLOUT E-MAIL

4.2 Software-as-a-Service Customer Relationship Management (CRM) Application

4.2.1 Purpose

The following use case provides an example of how VA can leverage a CRM solution that is externally managed and hosted. CRM is one of several types of applications that can be provided by an Independent Software Vendor (ISV) through a subscription that is monitored by VA.

4.2.2 Assumptions

- Security requirements for integrating with the cloud service are met per FedRAMP and VA Cloud security handbook.
- The ECSB has been deployed and is in use to manage the Cloud services that are consumed by VA.
- The CRM solution has already been evaluated and approved by the One-VA TRM.
- VA has established SLAs, based upon the GAO top ten cloud SLAs. These provide information on terms of service, availability requirements, and customer data isolation.

4.2.3 Use Case Description

- Review CRM providers and conduct a market analysis to identify the best fit to meet VA business needs.
- As part of the market research, VA will identify and review the SLA and Terms of Service to ensure that the provider can satisfy the SLA for enterprise consumption.
- After market research is completed, OI&T will narrow the search to a few candidates. A cost-benefit analysis will be implemented during the initial market research to identify the top candidates.
- VA finds two CRM solutions (CRM-A, CRM-B) that are suitable.
- OI&T selects the CRM solution (CRM-A) that meets the business needs and satisfies the SLA as the best fit.
- Ensure that the selected CRM solution is incorporated into the cloud broker.
- As business needs change over time, it is determined through the cloud broker that CRM-A is not able to meet its SLA on a consistent basis.
- OI&T cancels its subscription with CRM-A and changes its status in the cloud broker to “removed.”
- VA selects CRM-B and changes its subscription, as reflected in the cloud broker.
- VA leverages the cloud broker to monitor the performance of the CRM-B, with respect to its SLA.

This high level process flow is depicted in the following figure:

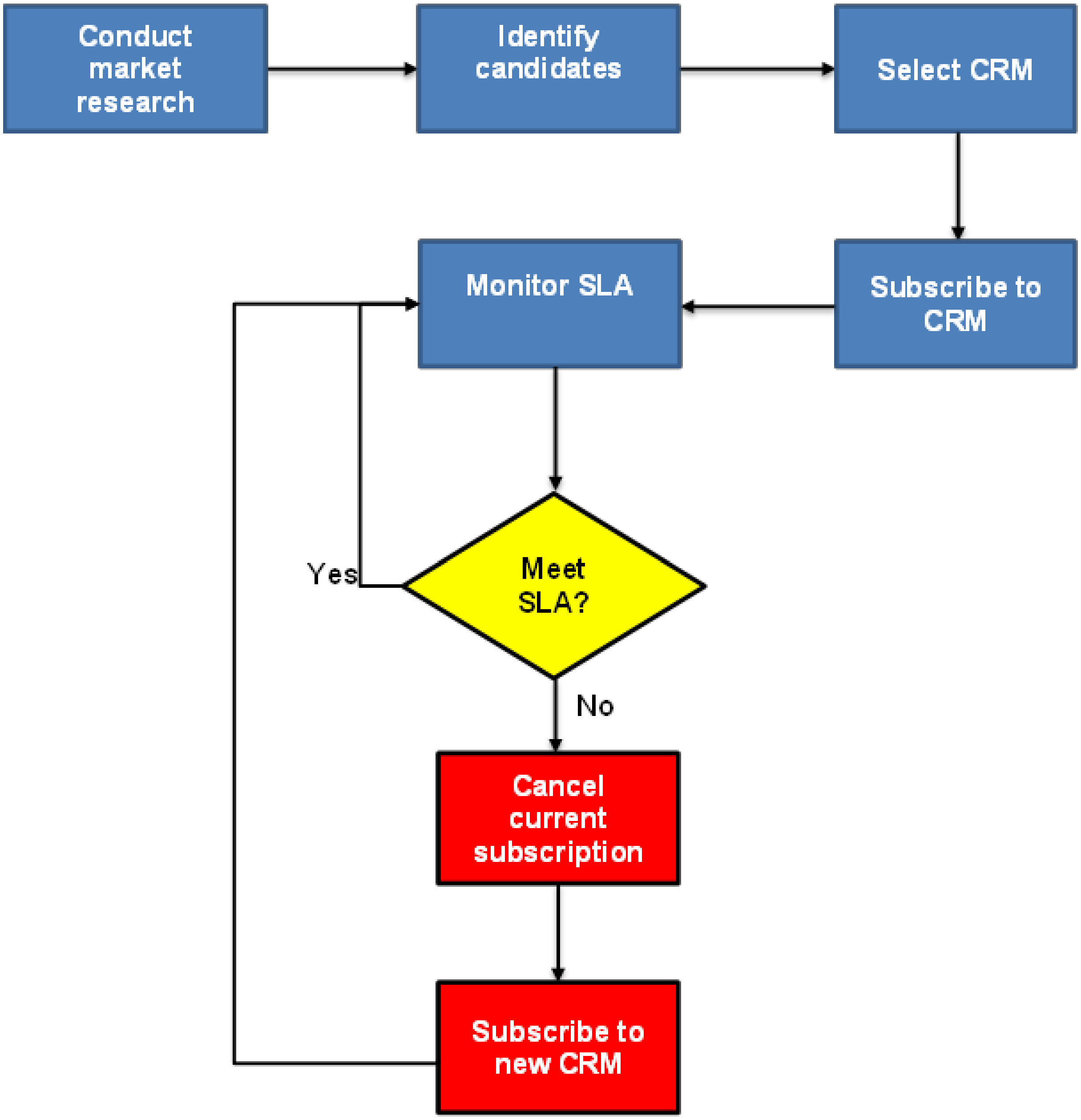


FIGURE 5: CHANGING NEEDS OF SAAS CRM

4.3 Independent Software Vendor (ISV) Software-as-a-Service Deployment and Hosting

4.3.1 Purpose

The following use case provides an example of how an ISV can provide a SaaS for VA. An ISV can be any service provider, large or small, who delivers a packaged application as a cloud-based service that meets the key attributes of SaaS, as defined in section 3.1. The application may

Consist of multiple service components, offered by different vendors, as negotiated by the SLA. The consumer does not manage or control the underlying cloud infrastructure, including networks, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

4.3.2 Assumptions

- In this use case, an external hosting environment is considered which requires FedRAMP security controls and an ATO. Alternatively, the SaaS may be deployed in a VA data center for internal use only and does not require FedRAMP ATO.
- The ECSB has been deployed and is in use to manage the cloud services that are consumed by VA.
- The ISV SaaS solution has been evaluated and approved by the One-VA TRM.
- The ISV SaaS provider has established an SLA with OI&T. These provide information on terms of service, availability requirements, and customer data isolation.

4.3.3 Use Case Description

- In this use case, VA will perform an analysis of its current business needs for internal use.
- OI&T will research and evaluate SaaS solutions to fill in the requirements.
- Potential ISV SaaS providers will be identified (whether they are large or small businesses).
- If the SaaS solution is hosted internally (VA owned SaaS) then FISMA controls are applied.
- If the SaaS solution is hosted externally then FedRAMP policies apply.
- What follows is onboarding the SaaS to the ECSB.
- The next step is utilizing the SaaS.
- This high level process flow is depicted in the figure that follows:

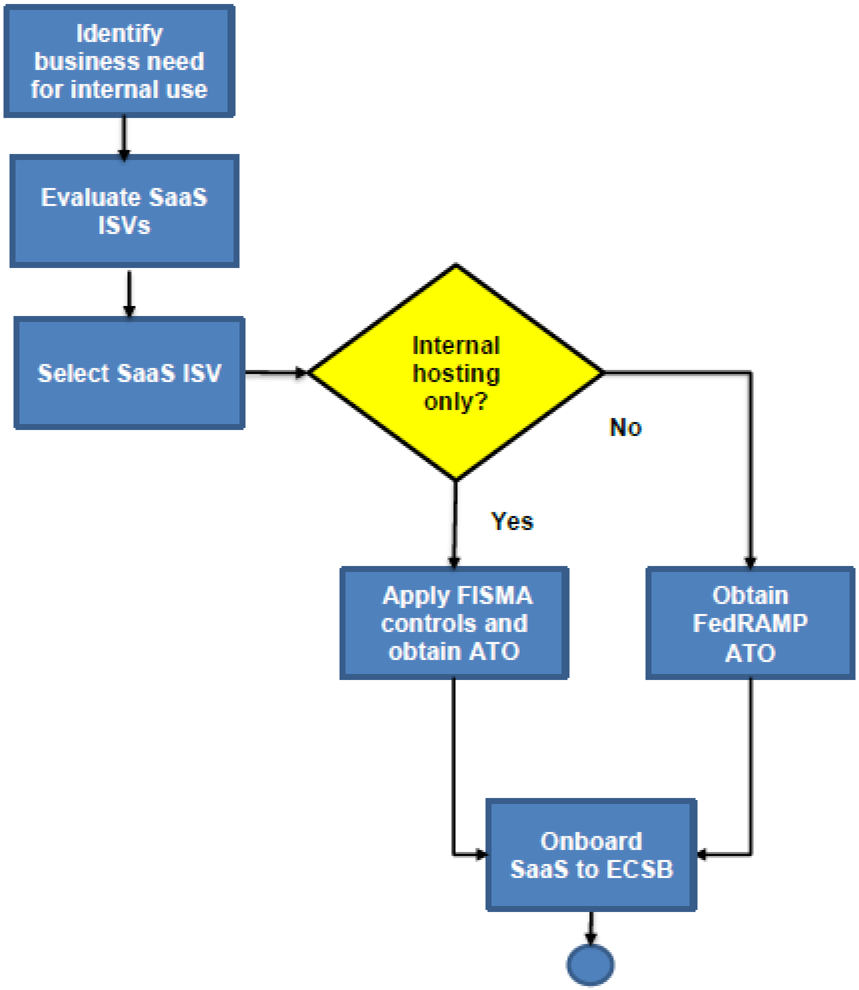


FIGURE 6: SAAS INDEPENDENT SOFTWARE VENDOR WORKFLOW

APPENDIX A. SCOPE

Scope

This EDP defines a framework for using SaaS solutions that address the following:

- VA definitions of the key attributes of SaaS
- VA customer needs that drive SaaS requirements
- Business requirements that drive SaaS decisions
- Industry and government SaaS best practices and lessons learned

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/project managers
- Executive leadership in IT (CIO, division head, etc.)

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

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA's Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO) Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and 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 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 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

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
CRM	Customer Relationship Management
CSP	Cloud Service Provider
EA	Enterprise Architecture
ECSB	Enterprise Cloud Services Broker
EDP	Enterprise Design Pattern
EPMO	Enterprise Program Management Office
ERP	Enterprise Resource Planning
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
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
IaaS	Infrastructure-as-a-Service
IT	Information Technology
JAB	Joint Authorization Board
LOB	Line of Business
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OI&T	Office of Information and Technology
OIS	Office of Information Security
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SDE	Service Delivery and Engineering
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
TIC	Trusted Internet Connection
TRM	Technical Reference Model
TS	Technology Strategies
VA	Veterans Affairs
VBA	Veteran Benefits Association

Acronym	Description
VIP	Veteran-focused Integration Process
WAN	Wide Area Network

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T 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	Policy, Directive, or Procedure	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
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

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
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.
18	GAO	GAO 16-325	Appendix II - Analysis of Agencies’ Cloud Service 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.