VA Enterprise Design Patterns
Cloud Computing

Enterprise Cloud Service Management

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

Version 2.0
Date Issued: July 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: 2017.08.15 14:40:49
-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: 2017.08.04 16:04:36
-04'00'

Deeneen Akeo
Acting Director, ASD

Revision History

Version	Date	Approver	Notes
1.0	11/17/2015	Tim McGrail (ASD TS)	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.
2.0	6/20/2017	Nicholas Bogden (ASD TS)	Update to align with other Cloud Computing EDPs and feedback from Enterprise Cloud Service Broker (ECSB) Team. Changed EDP name from ECSB to Enterprise Cloud Service Management to reflect current cloud strategy.

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

The Department of Veterans Affairs (VA) invests in cloud computing at the project level, resulting in siloed capabilities, without adequate governance and policies. To achieve VA transformation objectives in accordance with the VA Enterprise Architecture (EA) vision and strategy, the supporting information environment must continue to move from a disparate environment of “stove-piped” systems to a “unified” environment of integrated, interoperable business processes and technical services. VA’s incorporation of cloud service providers (CSPs) in the Enterprise Technology Strategic Plan (ETSP) supports the strategic goals of interoperable infrastructure, virtualized platforms and storage, and enterprise services. This Enterprise Design Pattern (EDP) continues to address the architectural principles and constraints that inform enterprise solutions that leverage CSPs. Based on the National Institute of Standards and Technology (NIST) Cloud Computing Reference Architecture (NIST SP 800-292); this document establishes the requirements for Enterprise Cloud Service Management (ECSM). This EDP will align to all VA governance, policy documents, and mandated federal requirements.

1.1 Business Problem

VA first published the Enterprise Cloud Service Broker (ECSB) EDP in late 2015. In late 2016, VA established an ECSB program to support the creation of new policy and resources related to cloud adoption. As the ECSB matures, its role is shifting to act less like a commercial cloud broker and serve more as a cloud management program. This EDP recognizes this change and identifies the need to create oversight over cloud adoption within a VA enterprise cloud environment. The Enterprise Program Management Office (EPMO) is guiding project managers

(PMs) in cloud adoption through the Veteran-Focused Integration Process (VIP), but gaps still remain:

- Project managers are still struggling to identify points of contact and resources to provide the level of detail required to complete cloud projects.
- Service aggregation, arbitrage, and intermediation have not been clearly defined or implemented to enable more efficient and compliant cloud adoption.
- Current guidance does not account for VIP, new EDPs on cloud services, EPMO, and EA.
- Some technical controls and cloud solutions are stand-alone, while integration with existing VA services is slowly maturing.
- The VA-published cloud policy is limited to the Authority to Operate (ATO) process and not well integrated with the existing ATO process.
- There is a lack of standard contractual language for CSP contracts.
- There is continued adoption of the cloud, without implementing a defined governance strategy to maintain visibility and integrate with enterprise security services to reduce the risk of cloud projects.

1.2 Business Need

ECSM supports all Lines of Business (LOBs) and the Office of Information and Technology (OI&T) in establishing a shared vision for managing the integration of Federal Risk Authorization and Management Program (FedRAMP) accredited CSPs for project-specific business needs. Projects need a "one-stop shop" in conjunction with the EPMO, to discover, access, and integrate CSPs via collaboration with OI&T. ECSM fosters collaboration among both business and IT stakeholders, and supports standardized solutions, including approved enterprise resources hosted outside of VA regional data centers.

1.3 Business Case

The goals of the Enterprise Cloud Service Management EDP are to:

- Be a single point of contact for information on VA's use of the cloud
- Provide governance over the adoption of cloud services
- Control risk by creating fiscal and technical visibility
- Ease the burden on PMs to make cloud adoption faster and easier
- Guide collaboration with enterprise services to support VA strategy

Table 1: Business Benefits

Business Benefits	Description
Be a single point of contact for information on VA use of the cloud	Creates consistent communications to project managers on cloud services, policy, and compliance.
Provide governance over the adoption of cloud services	Provides visibility into cloud adoption and resource utilization to manage risk and reduce shadow IT.
Control risk by creating fiscal and technical visibility	Controls risk by ensuring consistent compliance with federal policy such as FedRAMP and VA policy as well as maintaining oversight of service consumption which incurs a cost to VA.
Ease the burden on PMs to make cloud adoption faster and easier	Enables faster cloud adoption and timely delivery of services to Veterans through inheritable controls via shared infrastructure and services.
Guide collaboration with enterprise services to support VA strategy	Aligns cloud adoption and VA business needs with the Enterprise Technology Strategic Plan (ETSP), EDPs, and Enterprise Shared Services (ESS) to reduce project complexity.

1.4 Approach

VA is establishing a long-term initiative for incorporating external CSPs to achieve objectives established by the Office of Management and Budget (OMB) “Cloud First” strategy and VA Directive 6517. VA’s cloud computing initiative, outlined in “A Strategy for VA Cloud Adoption,” stems from direction by OI&T senior leadership to evaluate criteria for adopting CSPs or migrating existing IT infrastructure to CSPs. The initiative accounts for lessons learned from previous implementations in the Federal Government and the private sector. VA’s cloud computing initiative supports VA’s goal to achieve cost efficiencies while handling increased customer demands for enterprise services. Incorporating CSPs into the EA hinges on establishing and using ECSM to provide governance and monitor cloud adoption among diverse service consumers across VA.

2 Current Capabilities and Limitations

VA continues to support cloud adoption in the interest of improving services to Veterans, despite a lack of efficient processes for cloud adoption. Many projects are increasingly evaluating external CSPs to meet evolving business requirements, but identifying appropriate and compliant cloud services can be complex and time consuming for projects to manage themselves. The current ECSB is meant to ease the burden on the project team by enabling a single point of access for cloud integration, monitoring, and interoperability. The ECSB was designed to balance the strategic adoption of the cloud by VA to maximize value and compliance, while meeting the business needs of the project teams.

While the current ECSB is analyzing some projects to determine readiness for cloud adoption and creating environments in two CSPs to meet FedRAMP and VA security controls, there are continuing limitations, as described in the sections that follow.

2.1 No Single Resource for Cloud Adoption

PMs have become confused when trying to answer basic questions on technical requirements for cloud adoption as they are sent from one group to another in an attempt to find answers. Cloud policy questions may be directed to the Office of Cyber Security (OCS), while Trusted Internet Connection (TIC) questions may be directed to the Network Security Operations Center (VA-NSOC). Some PMs may establish their own conference calls with multiple parties, in an attempt to clarify cloud requirements. The ECSB does not currently advertise itself as a centralized resource to PMs for information on cloud adoption.

2.2 Solutions Not Integrated into the Existing VA Enterprise

The current cloud guidance is not well integrated into existing VA processes, procedures, and services. This challenge occurs across multiple areas where designs are siloed.

- Project Management – The ECSB is not closely integrated into VIP and procurement processes. The process flows do not automatically guide cloud projects to the ECSB for further guidance. Some Software as a Service (SaaS) and other cloud procurements have not been reviewed by the ECSB or examined for compliance with cloud requirements.
- Technical Controls – A basic crosswalk of FedRAMP and VA 6500 (based on NIST 800-53) controls has been performed. However, some controls are still under review and there is ongoing discussion on how many of these controls will be met in the cloud. Roles and responsibilities around cloud are also still being discussed. Until compliant cloud services are designed and managed, PMs cannot benefit from inheriting existing controls and must identify solutions to controls on their own. This increases the risk that cloud projects are not properly monitored.

2.3 Lack of Cloud Governance

VA is in the process of establishing a number of governance boards. In the interim, VA lacks clear oversight of cloud projects. This has had short term impacts, including:

- Involvement of multiple groups in cloud policy and architecture development processes leading to stand-alone or conflicting recommendations
- Procurement of cloud services without proper authorization or compliance[1]
- Cloud projects that lack centralized oversight to ensure costs do not escalate beyond planned budgets[2]

3 Future Capabilities

The adoption of cloud services can be daunting to PMs. There are many cloud services from which to choose. There are also multiple areas of compliance, depending on the project and cloud strategy to be met, including FedRAMP, Federal Information Processing Standards (FIPs), TIC, the Health Insurance Portability and Accountability Act (HIPAA), and others. PMs need help to select the appropriate services and controls, so they can focus on the business goals of their project and reduce the time consumed by compliance. However, using on-demand services in the cloud can still present a significant risk. In addition to typical information security risks, denial of service attacks, malware, and errors that increase service consumption can adversely impact a project's burn rate very quickly. ECSM will provide a significant value to VA projects by providing cloud services and expertise, simplifying compliance, and monitoring VA cloud projects to support cost efficiency.

Table 2: Mapping of Future Capabilities of Business Problems

Business Benefits	Description
Establish and advertise ECSM as a single point of information on cloud adoption	A single point of contact for cloud adoption will enable PMs to get consistent answers and gain the level of support required for each project.
Establish a service catalog and reference architecture for cloud	Projects have different needs when migrating to the cloud, from simple guidance on compliance to full backing for developing platform support. ECSM will provide a clear explanation of the options and levels of support that are available to PMs. The availability of predesigned services or architectures can reduce the compliance burden on projects through inherited controls. Information on cloud services will be provided to EPMO for inclusion in an OI&T service catalog.

[1] http://www.gao.gov/assets/680/676395.pdf

[2] https://www.va.gov/oig/pubs/VAOIG-15-01957-100.pdf

Business Benefits	Description
Seamless integration of cloud options with VA processes	Migration to the cloud will be designed to be an option within existing VA processes such as VIP and ATO. Close integration with existing processes will reduce the management overhead and PM confusion when making decisions on application hosting.
Integrate cloud strategy with VA enterprise strategy	Integrating cloud solutions with existing solutions within VA will improve efficiency and the monitoring of cloud projects for compliance and security while reducing the level of effort for cloud adoption.
Develop standard contractual language for cloud services	PMs will understand the service level agreements (SLAs) available through services already established by VA through existing contracts and be provided contractual language required of all cloud projects when a new contract is required.

3.1 Business Principles

Effective cloud management cannot function without integration with existing VA project management policies and workflows. If projects are able to procure cloud services without going through ECSM, value will be lost and the risk to VA will be significantly increased. ECSM will use two major approaches to improve cloud compliance:

- Encourage participation by PMs by offering value-added services that reduce the level of effort required to migrate to the cloud.
- Collaborate with organizations controlling procurement and other approval processes to identify and steer cloud projects to ECSM before permission is granted to proceed with cloud solutions.

ECSM will integrate with VIP to direct PMs to ECSM when a project becomes a candidate for cloud adoption. ECSM will assist the PM to select a cloud strategy aligned to the project’s risk profile and then support the application of the ATO process.

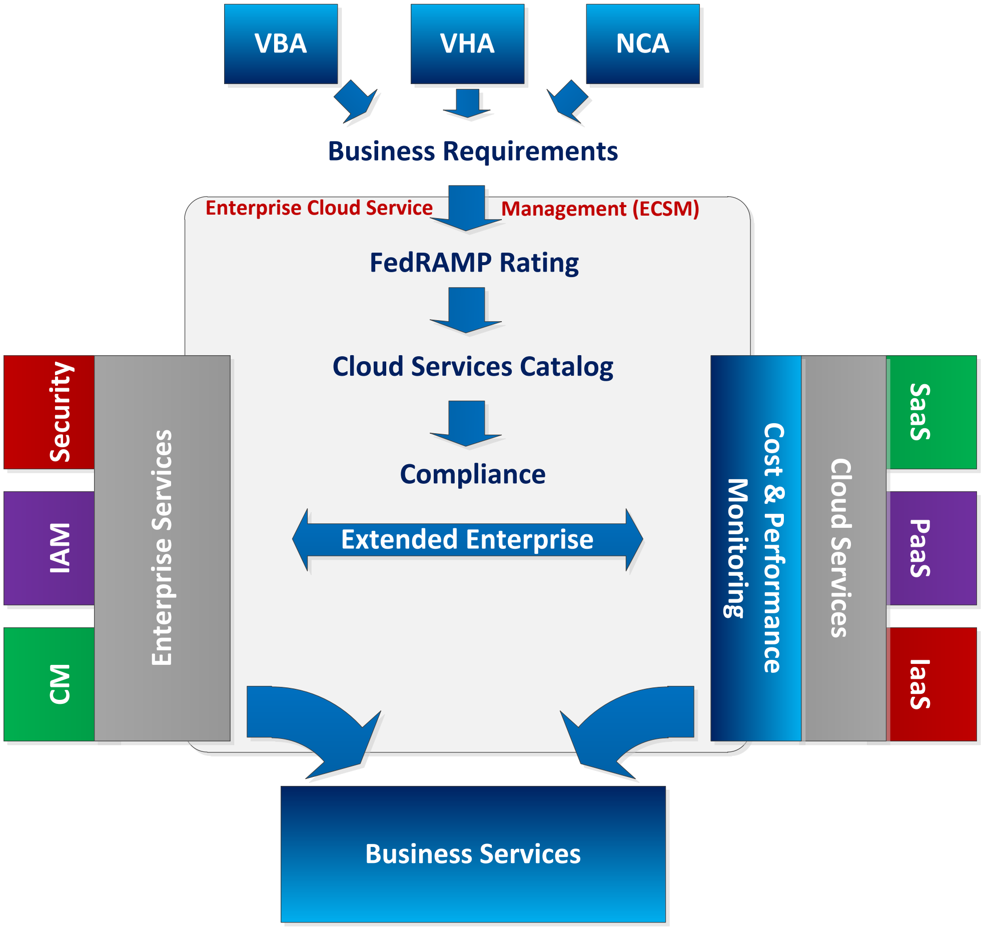

FIGURE 1: NOTIONAL "TO-BE" VA ECSM

Figure 1 Description: The diagram for the Notional "To-be" VA ECSB starts with three boxes at the top representing VBA, VHA and NCA. Arrow point from each to the word "Business Requirements". An arrow points down from "Business Requirements" to a box labeled as the Enterprise Cloud Service Broker (ECSB). Within the box, the arrow points down to "FedRAMP Rating" then another arrow down to "Cloud Services Catalog" another arrow down to "Compliance" and then a horizontal, bidirectional arrow labeled "Extended Enterprise". Overlapping the left side of the ECSB box is a grey box labeled "Enterprise Services". This box has 3 smaller boxes on top: one labeled "CM", one labeled "IAM" and one labeled "Security". On the right side of the ECSB box is another overlapping box labeled "Cost & Performance Monitoring". Above that box is another labeled "Cloud Services" which has 3 smaller boxes on top: one labeled "SaaS", one labeled "PaaS" and one labeled "IaaS". From the overlapping boxes on the left and right sides of the ECSB box are arrows curing downwards to a box outside of the ECSB labeled "Business Services".

As shown by Figure 1, VA OI&T is mandating a robust governance framework and policies on cloud computing to ensure that ECSM aligns to the VA EA Strategy and Vision. ECSM is to be responsible for documenting the overall VA cloud strategy and collaborate with other organizations across OI&T to design enterprise cloud services to support that strategy. Major components of cloud strategy include the following:

- Operations and the role of ECSM are components described in section 3.2.
- Architecture and service strategy are components described in section 3.3.
- Business case analysis – Provide information based on the FedRAMP level and projected services to aid the business case analysis and confirm that migration to the cloud will provide cost savings or enhanced business value over an alternate solution.
- Portability and interoperability – Ensure that applications can move among clouds over time (e.g. cloud bursting). These policies will eliminate the possibility of cloud vendor lock-in and support cloud data across multiple cloud platforms.
- Contractual language – The procurement of new cloud services requires a contract with each CSP. Therefore, ECSM will coordinate with the Technical Acquisition Center (TAC) and other groups as necessary to ensure that standard contractual language including SLAs are defined to support cloud adoption in compliance with VA strategy and risk management.

3.2 Operational Vision

To enable an efficient and compliant adoption of cloud resources that are aligned to VA strategy, VA needs an ECSM with technical functions that are aligned to business needs. As shown in Figure 2 below, the ECSM enables VA to mediate the adoption of cloud services that are based on technical and business requirements, while managing risk.

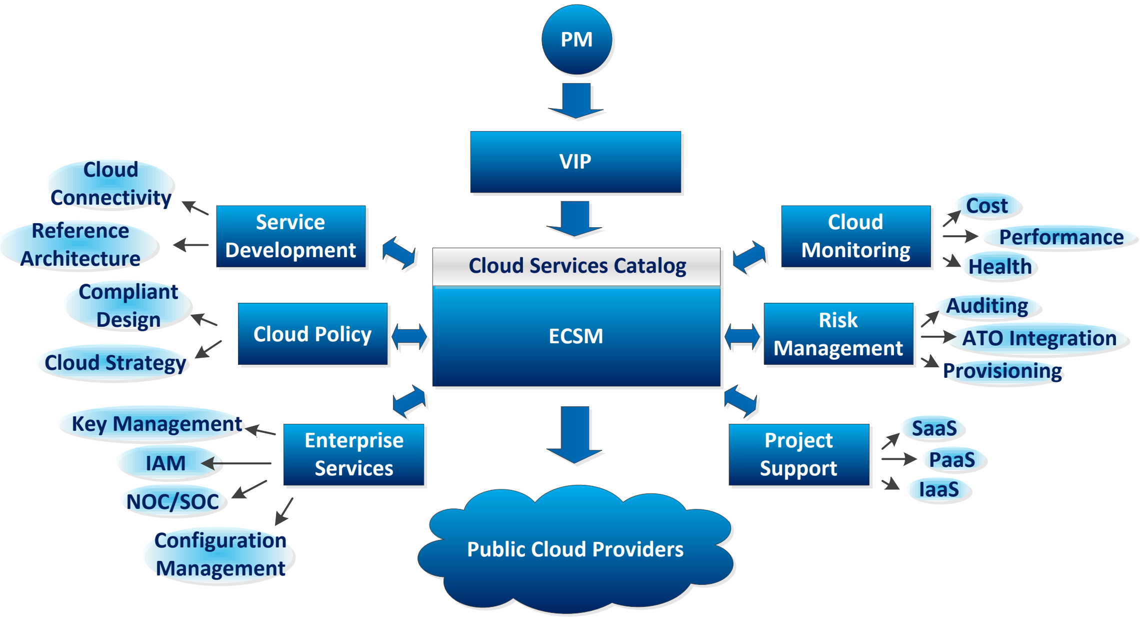

FIGURE 2: VA ECSM OPERATIONAL CONCEPT

Figure 2 Description: The VA ECSB Operational Concept diagram consists of a circle pointing down to other boxes with a series of boxes branching off each side. The top circle is labeled "PM". An arrow points

down to a box labeled "VIP" which points down to a box labeled "ECSB" which says "Cloud Services Catalog" along the top edge. The ECSB box points to 3 boxes on each side which point to supporting services. On the left is "Service Development" which is supported by "Cloud Connectivity" and "Reference Architecture". Next is "Cloud Policy" supported by "Compliant Design" and "Cloud Strategy." Next is "Enterprise Services" supported by "Key Management", "IAM", and "NOC/SOC." On the right side are 3 boxes: "Cloud Monitoring" supported by "Cost", "Performance" and "Health". "Risk Management" supported by "Auditing", "ATO Integration" and "Provisioning". "Project Support" supported by "SaaS", "PaaS", and "IaaS". At the very bottom of the diagram, the ECSB box points down to a cloud labeled "Public Cloud Providers".

ECSM provides the single point of contact for information on cloud adoption, making it available to all stakeholders. ECSM provides guidance and services to projects to reduce the burden on PMs to be experts in all areas of cloud design and federal compliance. ECSM allows the PM to focus more on the business service being delivered. ECSM monitors cloud projects to ensure compliance with VA business goals. ECSM will provide an integrated set of enterprise capabilities, including:

- Provide a single service desk for PM requests that are related to cloud adoption
- Provide a catalog of VA cloud services for integration into OI&T's service catalog
- Provide an internal website from which PMs can access ECSM information and initiate requests for support
- Use distribution lists and intake processes that are not reliant on any single person
- Govern the provisioning of cloud services
- Ensure compliance with FedRAMP and VA policy in cloud-specific services
- Ensure proper integration of cloud services with existing VA enterprise services
- Ensure that CSPs maintain VA standards and architectural compliance
- Enable continuous monitoring and reporting on performance of SLAs and Information Security controls
- Provide governance over usage and cost management down to the project level
- Provide standard contractual language for the adoption of new cloud services

3.3 Governance and Risk Management

If not carefully managed and monitored, the commercial cloud model can create a significant financial risk over the traditional data center. Due to the scalable nature of the cloud, a project could burn through their monthly budget in a matter of days from unauthorized access, insider threats, Distributed Denial of Service (DDoS) attacks, and errors if the project is left unchecked. This increases the importance of governance, over resource utilization and security compliance, to achieve cost savings goals. ECSM will perform the following governance to mitigate this risk:

- Establish a cloud governance solution across multiple CSPs that can provide cost management and SLA compliance monitoring to manage financial risk.
- Create and govern a workflow for cloud provisioning that includes restricting and monitoring accounts with elevated privileges, such as access to the CSP control panel.
- Create an overlay for the existing ATO process to align projects to the appropriate FedRAMP level, in addition to the Federal Information Security Management Act (FISMA) level. Any FedRAMP level specified by a project will be validated by ECSM to be accurate.
- If using auto-scaling, define "caps" for each project to validate significant changes in utilization before exceeding the defined maximum.
- Through invoices or technical means, ECSM will audit the utilization of cloud services to identify resources that are incurring costs, but not actively in use, and collaborate with PMs to control costs to the extent possible.

3.4 Technical and Architectural Principles

The technical concept for the ECSM vision should enable business services by extending the current VA enterprise into the cloud. ECSM will prepare solutions to ease the cloud adoption burden on projects. The guiding principles for the technical support provided by ECSM are as follows:

- Support transition of a largely on-premises IT infrastructure into the cloud by providing a catalog of cloud services which lists the existing CSPs, infrastructure, platforms, and applications that have already been authorized. In addition, the levels of technical support and options available from ECSM will be clearly defined for PMs.
- In alignment with existing cloud EDPs, prioritize Software as a Service (SaaS), Platform as a Service (PaaS), and then Infrastructure as a Service (IaaS) solutions for VA projects through technical analysis of cloud options for each project.
- Reduce the compliance burden on PMs through the following efforts:
    - Create a cloud reference architecture that supports all FedRAMP levels, complies with VA policy, and connects with existing VA enterprise solutions in areas such as security operations, vulnerability management, and configuration management.
    - Support configuration management through standard images for use in the cloud in the same manner as approved baselines within the existing VA enterprise.
    - Perform analysis to create cloud services which are common to many projects that can be easily consumed for areas such as identity and access management

    - (IAM), auditing, storage, key management, and others to be prioritized by projected demand as defined by the Enterprise Shared Service (ESS) strategy.
    - Authorize the cloud reference architecture and other ECSM services so that the controls can be inherited easily as part of the VA ATO process.
- Identify and submit tools for the One-VA Technical Reference Model (TRM) that will support cloud operations. This includes tools for cost management across CSP platforms.

3.5 Security Considerations

In addition to VA requirements, FedRAMP defines a number of security requirements that must be met and all cloud projects are still subject to the normal VA ATO process. This process may require a substantial level of effort to complete, particularly if the project desires to adopt a CSP or service that has not previously been authorized. To support the timely deployment of services for Veterans, ECSM will take the following actions:

- Collaborate with the Office of Information Security (OIS) to identify any enhancements to the existing ATO process that is required to ensure that all projects are aligned to the appropriate FedRAMP High/Moderate/Low. This includes defining the role of ECSM in the ATO process when cloud adoption is indicated, and how the FedRAMP rating will affect the options available to the project for cloud adoption. ECSM will identify services compliant with each FedRAMP level and VA policy in advance, in order to increase the efficiency of cloud adoption from the time the risk profile is completed.
- Support OIS in forming a group, including both business and technical leaders, to discuss the expansion of the General Support System (GSS) to the cloud. While the United States Department of Agriculture (USDA) has done this with success to alleviate problems related to TIC compliance and performance impact, VA must review its own specific risks and the security architecture needed between internal systems and the cloud to provide proper inspection and control. The final decision will be a risk shared by all stakeholders.
- Due to the potential cost implications, accounts which can provision cloud resources will be limited and will be approved and tracked by ECSM. ECSM will need to coordinate with a VA organization that already provides 24x7x365 support. This is to provide alerts for unauthorized account creation or access on a continuous basis, in addition to network security monitoring.
- Collaborate with VA-NSOC to ensure security monitoring of all cloud activity, network segmentation aligned to enterprise security strategy, and proper boundary protections. Identify critical differences between cloud design and VA data centers that would

require modification of existing VA enterprise security strategy, such as a lack of support for passive network monitoring for intrusion detection.

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

All projects will leverage the approved tools and technologies located in the One-VA TRM to comply with the architectural guidance provided in this document. Table 3 lists the approved tools for this EDP.

Table 3: List of Approved Tools and Standards for Cloud Computing

Technology Category	Example Technologies	Example Standards	Mandated ESS
Authentication	Active Directory, CA Federation, Tivoli Federated Identity Manager	X.509, OAuth/OpenID Connect, Kerberos, SAML, LDAP	IAM SSOi/SSOe
Cloud Monitoring	N/A	N/A	N/A
Key Management	HyTrust Data Control, Venafi Trust Protection Platform	ANSI X9.17, X.509	N/A
Security Event Monitoring	Splunk	N/A	VA-NSOC

3.7 Alignment to Veteran-Focused Integration Process (VIP)

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

4 Use Cases

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

4.1 Service Intermediation

4.1.1 Purpose

VA is deploying the Vets.gov website to the cloud, which will consolidate multiple sites and services into one place. The PM is looking for guidance on VA cloud requirements that affect the solution design.

4.1.2 Assumptions

- A cloud policy is available that defines VA controls and requirements that are related to each FedRAMP level.
- A Request for Proposal (RFP) for support services has not been released by the project.
- ECSM has been designed to meet the goals described in the EDP.

4.1.3 Use Case Description

- The PM is directed to ECSM as part of the VIP process of defining requirements to be used in the RFP.
- ECSM reviews the project's risk assessment and validates the FedRAMP rating of the project.
- The VA service catalog, which includes cloud services, is provided to define the existing CSPs that have been authorized by VA, along with available services for the defined FedRAMP level.
- The PM selects the authorized services to be used by Vets.gov. Inherited controls are automatically identified and ECSM provides a list of remaining controls which must be met.
- ECSM supports the PM through the rest of the VIP process to answer questions related to cloud adoption.
- ECSM provisions the cloud environment once procurements are complete as part of release management and confirms required monitoring controls are established.

4.2 Service Aggregation

4.2.1 Purpose

VA is launching a new cloud-based data analytics solution for Veteran health trends. The PM has a limited budget and would like to know how ECSM can help identify and meet security compliance requirements that are related to the use of personally identifiable data in the cloud.

4.2.2 Assumptions

- The cost model for shared cloud services is not fully defined at this time.
- The portfolio of services described is for information purposes only.

4.2.3 Use Case Description

- ECSM reviews the risk analysis of the project and confirms that the project would need to comply with the FedRAMP High level.
- The VA service catalog, which includes cloud services, is provided. It defines the existing CSPs that have been authorized by VA, along with available services for the FedRAMP High level.
- The PM has the option of adopting the VA-authorized cloud space within a CSP that includes security services, including IAM, auditing, monitoring, and internet-facing services, such as Web Application Firewalls and DDoS protection. As these are ESS, they are available at a significantly reduced cost to the project, as opposed to establishing each of these services on their own.
- The PM selects the security services bundle which allows his project to inherit the majority of security controls from the ESS and authorized hosting space.
- The project is able to deploy a solution within budget and receives support from ECSM to understand the remaining security controls as they progress through VIP.

4.3 Service Arbitrage

4.3.1 Purpose

A PM needs to significantly increase data storage for a short term Veterans Health Administration (VHA) project on cancer research and has been asked to identify the most cost effective solution.

4.3.2 Assumptions

- The business requirements for using the cloud are the same as those being met through hosting at the data center.
- VA already has multiple projects in the cloud that support the business case for bulk purchasing.

4.3.3 Use Case Description

- The PM is able to easily locate information on the ECSM website as the single point of contact for cloud information at VA. The VA service catalog confirms that cloud storage is a service supported by ECSM.
- ECSM reviews the risk profile for the project and determines the appropriate FedRAMP level.

- Based on the FedRAMP level, ECSM provides cost information for different types of storage.
- The PM is able to project the cost savings on storage, based on differences for hot and cold storage, while also meeting business requirements related to scalability and compliance with VA policy

APPENDIX A. SCOPE

This EDP focuses on the cloud management program required to provide a cloud-based hosting environment for applications. It will define the ECSM program for project teams to leverage cloud services and outlines the standards and capabilities for ECSM to act as a liaison between VA (Cloud Consumer) and Cloud Providers.

This EDP will conduct the following activities:

- Outline current cloud initiatives within VA and associated challenges, including gaps in the current ECSB.
- Define VA's ECSM Program addressing Service Aggregation, Arbitrage, and Intermediation.
- Define how ECSM integrates with VIP, EDPs, and ESS in support of enterprise strategy.
- Define how ECSM assists project teams to create solutions compliant with VA, FedRAMP, and NIST policies.
- Provide use cases demonstrating how ECSM enables PMs to move to the cloud with less effort.

Topics that are out of scope for this EDP, but may be referenced, are:

- Solutions directed to a specific Cloud Service Provider
- Problems specific to individual projects

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA's OI&T, Enterprise Program Management Office (EPMO), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Information Technology Operations and Services (ITOPS). Extensive input and participation was also received from 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
Access	Access refers to interaction with a computer system, such as the Veterans Health Information Systems and Technology Architecture (VistA). Such interaction includes data retrieval and editing (create, update, delete) and may result from a variety of technical mechanisms, including traditional user log on, consuming applications exercising middleware-based connectivity, Service-Oriented Architecture (SOA) service requests, etc.
Auditing	Auditing is the inspection or examination of an activity that is based on available information. In the case of computer systems, the audit is based on the review of the events generated by the system or application.
Cloud Auditor	A cloud auditor can conduct independent assessments of cloud services, information system operations, performance, and security of the cloud implementation.
Cloud Broker	The cloud broker manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
Cloud Consumer	The cloud consumer is a person or organization that maintains a business relationship with and uses services from a cloud provider.
Cloud Service Provider	The provider is a person, organization, or entity responsible for making a cloud-based service available to interested parties.
Consuming Application	This application consumes services from a provider system. It is generally used when discussing a front-end application that is supporting a user, but even service providers can themselves be a consumer of other services.
Continuous Monitoring	This process uses technology to detect compliance and risk issues associated with an organization's financial and operational environment.

Key Term	Definition
Risk Management	The identification, assessment, and prioritization of risks are followed by the coordinated application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.
Access	Access refers to interaction with a computer system, such as the Veterans Health Information Systems and Technology Architecture (VistA). Such interaction includes data retrieval and editing (create, update, delete) and may result from a variety of technical mechanisms, including traditional user log on, consuming applications exercising middleware-based connectivity, Service-Oriented Architecture (SOA) service requests, etc.
Auditing	Auditing is the inspection or examination of an activity that is based on available information. In the case of computer systems, the audit is based on the review of the events generated by the system or application.
Cloud Auditor	A cloud auditor can conduct independent assessments of cloud services, information system operations, performance, and security of the cloud implementation.
Cloud Broker	The cloud broker manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
Cloud Consumer	The cloud consumer is a person or organization that maintains a business relationship with and uses services from a cloud provider.
Cloud Service Provider	The provider is a person, organization, or entity responsible for making a cloud-based service available to interested parties.
Consuming Application	This application consumes services from a provider system. It is generally used when discussing a front-end application that is supporting a user, but even service providers can themselves be a consumer of other services.
Continuous Monitoring	This process uses technology to detect compliance and risk issues associated with an organization’s financial and operational environment.
Risk Management	The identification, assessment, and prioritization of risks are followed by the coordinated application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.

APPENDIX C. ACRONYMS

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

Acronym	Description
ASD	Architecture, Strategy and Design
ATO	Authority to Operate
CSP	Cloud Service Provider
DOD	Department of Defense
DDOS	Distributed Denial of Service
EA	Enterprise Architecture
ECSB	Enterprise Cloud Services Broker
ECSM	Enterprise Cloud Service Management
EDP	Enterprise Design Pattern
EPMO	Enterprise Project 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
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOB	Line of Business
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OCS	Office of Cyber Security
OIS	Office of Information Security
OI&T	Office of Information and Technology
PaaS	Platform as a Service
PM	Project Manager

Acronym	Description
PMAS	Project Management Accountability System
RFP	Request for Proposal
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDE	Service Delivery and Engineering
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
TAC	Technical Acquisition Center
TIC	Trusted Internet Connection
TRM	Technical Reference Model
USDA	United States Department of Agriculture
VBA	Veterans Benefits Association
VHA	Veterans Health Administration
VIP	Veteran-Focused Integration Process
VistA	Veterans Health Information Systems and Technology Architecture
VPC	Virtual Private Cloud

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 EDPs for all VA projects developing IT systems in accordance with VA's OI&T integrated development and release management process, the 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 Directive 6517	Risk Management Framework for Cloud Computing Services
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
6	NIST	NIST SP 500-291 NIST SP 500 -292	NIST Cloud Computing Standards Roadmap, Version 2, July 2013 NIST Cloud Computing Reference Architecture
7	NIST	NIST SP 800 - 145	The NIST Definition of Cloud Computing, NIST SP 800-145, Sept. 2011
8	NIST	NIST SP 500 - 299	NIST Cloud Computing Security Reference Architecture: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf
9	DOD	DOD	Department of Defense Cloud Computing Strategy

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
10	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
11	OMB	OMB M-08-05, Implementation of Trusted Internet Connections (TIC)	This initiative establishes TIC to optimize and standardize the security of external network connections for Federal agencies. There are three strategic components: • Reduce and consolidate external access points • Manage security requirements for NOC/SOC • Establish compliance program to monitor adherence to TIC policy
12	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. It does so by requiring agencies to evaluate safe, secure, cloud computing options before making any new investments.
13	Federal	U.S. CIO, 25 Point Implementation Plan to Reform Federal Information Technology Management	This 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.
14	Federal	FIPS 199 FIPS 200	FIPS 199 (Federal Information Processing Standard Publication 199) is a standard that establishes Minimum Security Requirements for Federal Information and Information Systems.

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.