Department of Veterans Affairs Enterprise Cloud (VAEC) Technical Reference Guide

V2.0

10 November 2022

VA/OIT/DSO/IO/Enterprise Cloud Solutions Office

Providing Veterans improved services through cloud-based data and computing capabilities

Table of Contents

1 Introduction 1
Purpose 1
Audience 1
Document Update Policy 1
Overview of Content 1
2 Environment Overview 2
VAEC Overview 2
ECSO Overview 3
3 VAEC Architecture 4
VAEC-AWS Architecture 5
VAEC-Azure Architecture 7
VAEC Enterprise Development Environment 8
VA Platform One 9
VAEC Research and Analytics Super Platform 9
4 VAEC Network Topology 11
VAEC-AWS Network Topology 13
VAEC-Azure Network Topology 14
5 VAEC Cyber Security 15
Shared Responsibility Model 16
Inheritable Security Controls 17
Authority to Operate 18
Other VAEC Cybersecurity Resources 18
6 Available Services and Tools 18
ECSO Core Services 18
Additional ECSO Services 19
CloudKey 20
VAEC General Support Services 20
Other VAEC Tools 29
Available VAEC Services 29
7 VAEC Relevant Policies and Procedures 30
VAEC Software Installation Policy 31
Elevated Privileges Policy 31
VAEC Lifecycle Management Framework 31
Product Line Change Request Process/Policy 34
Obtaining a VAEC Application Code 34
Enterprise Security External Change Council Process 34
Obtaining a VA Application ATO 35
VAEC Health Assessment Process 36
8 VAEC Points of Contact 37
Appendix A: References 38
Appendix B: Acronyms 39

Table of Figures/Tables

Figure 1. Overall VA IT Architecture 3
Figure 2. ECSO Organizational Structure 4
Figure 3. VAEC-AWS Component Layout 6
Figure 4. VAEC-Azure Component Layout 7
Figure 5. VAPO Architectural Layers 9
Figure 6. RASP Architectural Layers 10
Figure 7. RASP Pre-established Connectivity 10
Figure 8. VAEC to VA Network Overview 11
Figure 9. VAEC Application View of Network Topology 13
Figure 10. VAEC-AWS Network Connections 14
Figure 11. VAEC-Azure Network Connections 15
Figure 12. Inheritable Security Controls Model 17
Figure 13. GSS Categories vs DevSecOps Phases 22
Figure 14. Other Available VAEC Tools by DevSecOps Phase 29
Figure 15. VAEC Support Models 30
Figure 16. VLMF Overview 31

Table 1. Shared Security Responsibility Model 16
Table 2. Tool Usage Key 20
Table 3. GSS Tool Responsibility 21
Table 4. Asset Management GSS Tools 22
Table 5. Capacity and Performance Management GSS Tools 23
Table 6. Information Security GSS Tools 23
Table 7. Monitoring and Event Management GSS Tools 25
Table 8. Service Configuration/Deployment Management GSS Tools 26
Table 9. Service Desk/Service Request Management GSS Tools 27
Table 10. Service Financial Management GSS Tools 28

1 Introduction

The Department of Veterans Affairs (VA) is committed to the use of cloud computing, which treats IT services as commodities with the ability to dynamically increase or decrease capacity to match usage needs. VA understands that cloud computing can provide significant benefits to developers and users through leveraging shared computing services and taking advantage of economies of scale.

VA has established an overall cloud ecosystem including the VA Enterprise Cloud (VAEC), managed by the Enterprise Cloud solutions Office (ECSO), providing cloud services (Infrastructure as a Service, or IaaS) for hosting applications, cloud-based development platforms (Platform as a Service, or PaaS), and Software as a Service (SaaS) solutions. The VAEC is the only standard, approved VA enterprise-level cloud service. Cloud computing is a business enabler that efficiently provides Veterans, their dependents, VA employees and contractors, and VA partners with innovative, Veteran-focused services, applications, and access to information on demand using Veteran-preferred devices and technologies. The VA has the foundation of an agile, interoperable, scalable, and secure cloud computing environment that can adapt to evolving business needs. It offers elastic, metered data storage and computing capability to support new approaches for the delivery of integrated services to Veterans. The benefits of an enterprise cloud environment, and software services characterized by costs shared across a broad customer base and supported by leading, external technology providers, is improving the VA's ability to target its efforts toward key mission areas focused on the Veteran. This will result in more efficient and responsible stewardship of taxpayer dollars.

Purpose

The purpose of the *VAEC Technical Reference Guide* (TRG) is to provide information to help readers to understand the VAEC environment so that they can assess, plan, design and implement cloud-based migration, modernization, and new projects.

Audience

The intended audience for this document is primarily contractors and VA development teams, who need to understand the VAEC concepts, architecture, related services, and tools. Other readers, including new ECSO staff and developer teams looking to migrate to the VAEC, may also find information helpful to advance their general understanding of the VAEC services.

Document Update Policy

The TRG will be updated at least annually to ensure it has the latest information. This will provide the best value to contractors, VA development teams, and new ECSO team members.

Overview of Content

This TRG provides information about the VAEC in the following areas:

- Overview/Introduction
- Architecture (overview and details)
- Network topology
- Cybersecurity introduction
- Services and tools introduction
- Service Catalog
- Relevant procedures
- ECSO point of contact (POCs)

Detailed architectural information will only be provided after contract award and/or during project provisioning. It is important to note that all information in this Guide is therefore simply a snapshot of available information that is to be considered accurate as of the date on the title page. Any more recent updates are available on the VA ECSO web site: https://dvagov.sharepoint.com/sites/OITECSO that will be made accessible to all with VA accounts.

2 Environment Overview

The VA Enterprise Cloud (VAEC) is the VA-approved, standard, enterprise-level, multi-vendor platform for the development and deployment of VA applications hosted in the cloud. The VAEC provides a set of common, General Support Services (GSS) such as authentication and performance monitoring which each application can leverage, speeding and simplifying the development of new applications in or migration of existing applications to the cloud. The VAEC also implements many of the NIST-, FedRAMP- and VA-required security controls reducing the time each application should take to obtain a VA Authority to Operate (ATO). VAEC uses the two leading commercial cloud platforms: Amazon Web Services (AWS) and Microsoft Azure.

VAEC Overview

The VAEC implements the VA cloud use policy described in VA Directive 6517, *Cloud Computing Services*, updated in the OMB "Cloud Smart" strategy (see: *From Cloud First to Cloud Smart*, Federal Cloud Computing Strategy, OMB/Office of the Federal Chief Information Officer, URL: https://cloud.cio.gov/strategy/), and amplified in the joint Strategic Sourcing and Demand Management Office's *Use of the VA Enterprise Cloud (VAEC) to Host Applications* memorandum, as well as the *Use of Cloud Native Technologies and Approaches* memorandum (*see Appendix A: References* for a list of applicable policies). These authoritative sources respond to mandates issued by the White House, Congress, the Federal Chief Information Officer (CIO), and the Secretary of Veterans Affairs. VA envisions the VAEC as a business enabler that will efficiently provide Veterans, their dependents, VA employees and contractors, and VA partners with innovative, Veteran-focused services, applications, and access to information on demand using Veteran preferred devices and technologies.

Figure 1 shows how the VAEC fits within the overall VA compute architecture.

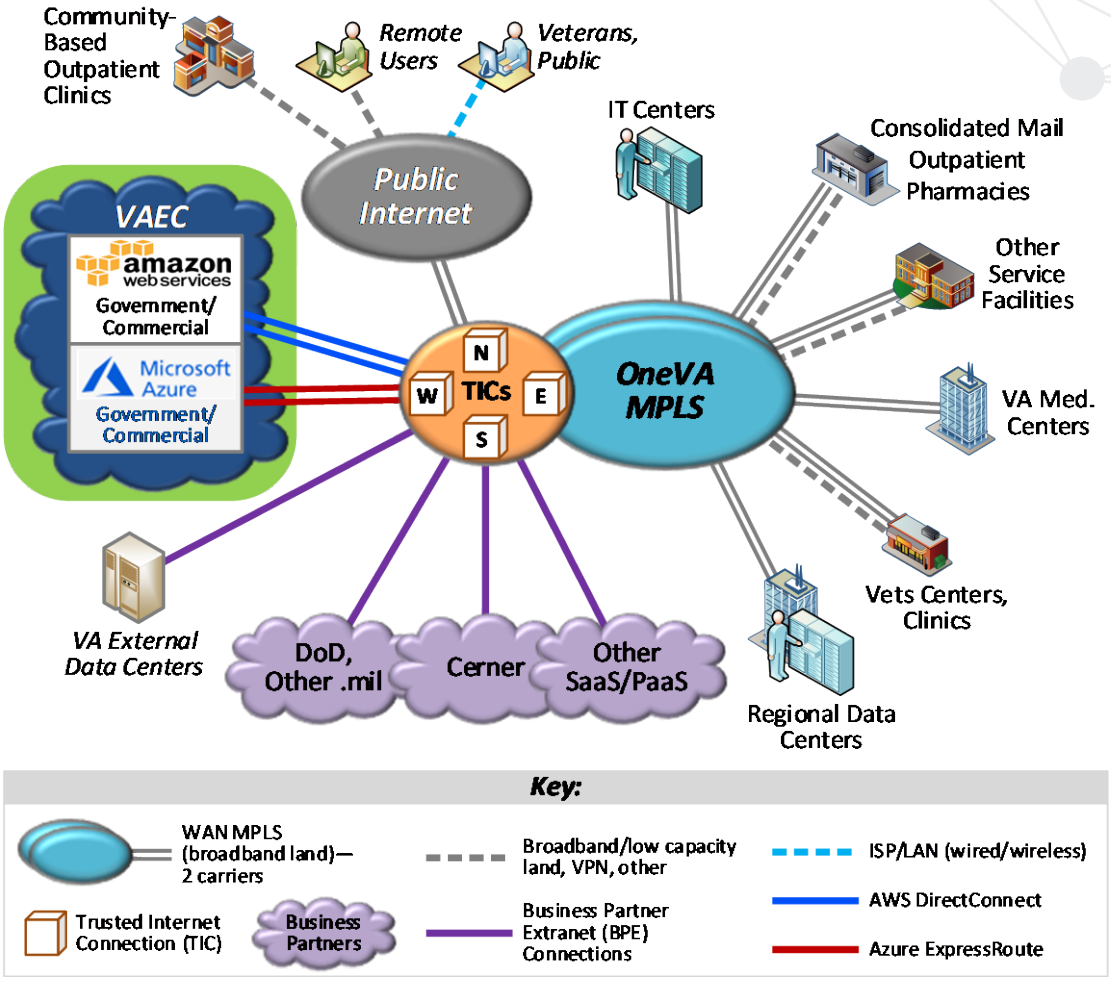

Figure 1. Overall VA IT Architecture

VA also uses various Platform as a Service/Software as a Service (PaaS/SaaS) capabilities provided by a set of VA business partners connected through Business partner Extranet (BPE) gateways. All services are connected to the central VA dual-carrier Multiprotocol Label Switching (MPLS) network through Trusted Internet Connection (TIC) gateways.

ECSO Overview

The VAEC is supported by the ECSO, organizationally part of the Application hosting, Cloud and Edge Solutions (ACES) organization under OIT/Development Security and Operations (DevSecOps)/Infrastructure Operations (IO). The Enterprise Program Management Office (EPMO) Senior Executive for VA Enterprise Cloud established the ECSO in April 2018. ECSO serves as the focal point for coordinating enterprise cloud initiatives and assists components to coordinate and facilitate cloud service adoption within the VA. ECSO is staffed by multidisciplinary IT subject matter experts (SMEs), supported by contract personnel. ECSO assists the VA enterprise with identifying, acquiring, migrating, and managing cloud services. An overview of the ECSO organizational structure is shown in Figure 2 below.

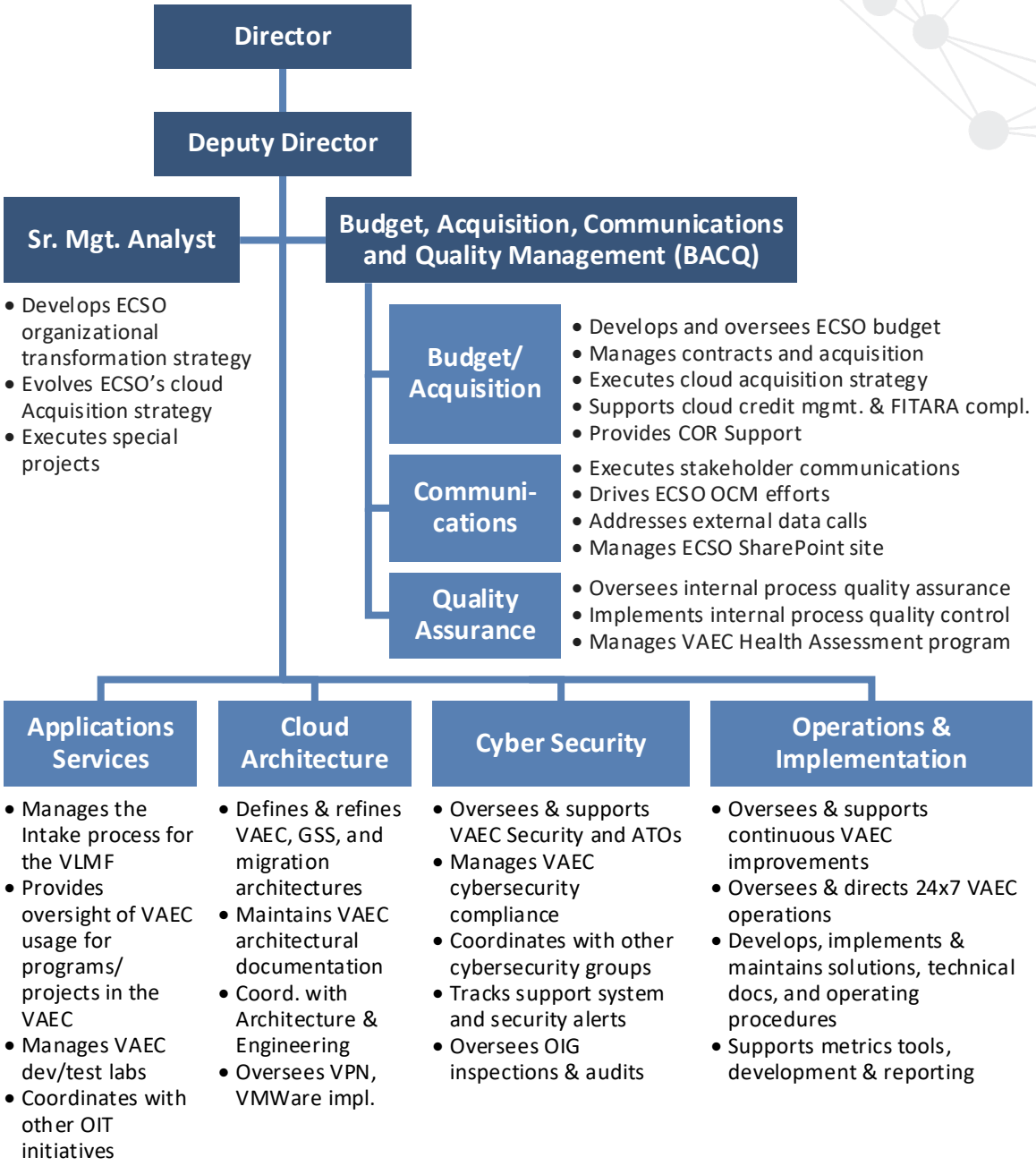

Figure 2. ECSO Organizational Structure

3 VAEC Architecture

VAEC runs on commercial Cloud Service Providers (CSPs), specifically Amazon Web Services (AWS) commercial offerings and their GovCloud environment (spread over two regions) and Microsoft Azure commercial and Government offerings (spread over five regions). VAEC currently hosts over 250 VA mission applications, plus various development environments. Since major components of VAEC are provided by the CSPs, they are deployed outside of the VA

enterprise network. Trusted Internet Connections (TICs) are used to route network traffic between VAEC (and other external entities) and the rest of VA network.

VA currently uses numerous commercial and government PaaS and SaaS platforms, including Microsoft Office 365 (O365), and Salesforce. The externally hosted Cerner Electronic Health Records (EHR) system is also treated as a SaaS platform.

VA applications execute in these environments and can take advantage of standard tools and services. These applications are used by all VA staff and Veterans. They are managed and maintained by VA and contractor developers and administrators. Finally, VA OIT policies, governance, and organizations such as ECSO provide guidance to all parts of the VA cloud effort, including the VAEC.

VAEC-AWS Architecture

The VAEC-AWS environment uses both the AWS GovCloud and AWS Commercial components. The VAEC-AWS is connected to the VA network via AWS Direct Connect (see Section 4 for details). Projects are provisioned, as part of the VAEC Lifecycle Management Framework (VLMF—see Section 7 for details), one or more Virtual Private Clouds (VPCs) for their production, development, and any other required environments. The VAEC-AWS offers common services described in Section 6. VAEC-AWS also provides access to the full suite of FedRAMP Certified AWS GovCloud Services by default. Access to Non FedRAMP Certified AWS GovCloud services may be provisioned upon request.

The VAEC-AWS environment consists of environments within two (2) geographic regions (AWS East and AWS West) with multiple availability zones provided by AWS GovCloud. A simplified view of the VAEC-AWS architecture is provided below. Detailed architectural information will only be provided post contract award and/or during project provisioning.

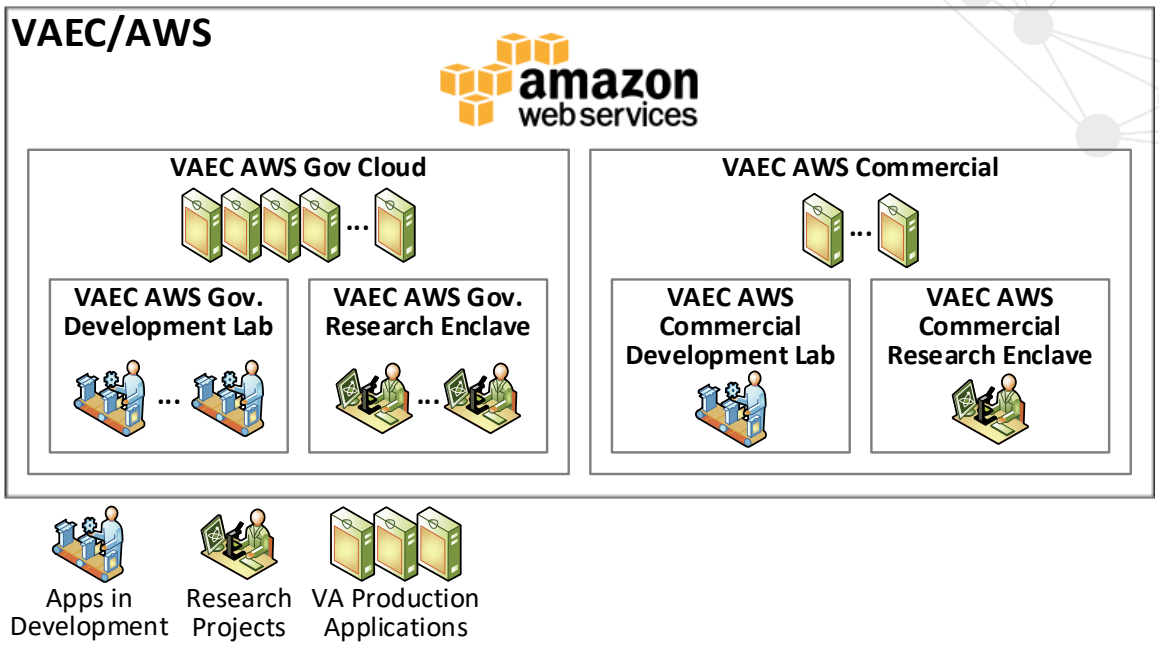

Figure 3. VAEC-AWS Component Layout

VAEC-AWS Components include:

- VAEC-AWS GovCloud (US) enables customers to adhere to International Traffic in Arms Regulation (ITAR) regulations, the FedRAMP requirements, Defense Federal Acquisition Regulation Supplement (DFARS), DoD (SRG) Impact Levels 2 and 4 and 5, and several other security and compliance requirements. It can protect sensitive unclassified data files with server-side encryption in Amazon S3. Projects/customers can store and manage security keys with AWS CloudHSM or the AWS Key Management Service (AWS KMS). ***This is the default location for all hosted applications using the VAEC-AWS production environment.***
- VAEC-AWS Commercial is composed of the AWS public cloud computing platform. In the rare situation (adjudicated on a case-by case basis) that a project/customer cannot use the AWS GovCloud component (if, for example, they absolutely require an AWS service not available in AWS GovCloud), they will be provisioned in the Commercial space. ***The default VAEC-AWS hosting location is the AWS GovCloud.***
- VAEC-AWS Development Labs include both Government Labs (GLabs) hosted in VAC-AWS GovCloud with connection to the VA Network and Commercial Labs (CLabs) hosted in the VAEC-AWS Commercial component. GLabs have all guard rails in place as a VAEC enclave, including Active Directory (AD), Single Sign On (SSO), Personal Identity Verification (PIV), Non-Mail Enabled Account (NEMA) capabilities, and use of the VA electronic Permission Access System (ePAS). GLabs are considered technically an extension of VAEC. CLabs have no VAEC guard rails built in. They use the VAEC-AWS Commercial component environment, with no connection to VA network, and will be provisioned in the cases where GLabs will not work. See the VAEC Enterprise

Development Environment (EDE) and VA Platform One (VAPO) architecture information below for further details.

- VAEC-AWS Research Enclaves are provisioned for VA projects/customers where VA Researchers need timely access to leading edge cloud research tools and institutional data sources; they should not be expected to become infrastructure or cloud experts. See the VAEC Research and Analytics Super Platform (RASP) architecture information below for further details.

VAEC-Azure Architecture

The VA connection into VAEC-Azure end point is via a Virtual Private Network (VPN) into the Azure Government GovCloud. Projects are provisioned one or more VPCs for their production, development/test and any other required environments. The VAEC-Azure offers common services and specific services and access to the full suite of Azure GovCloud Services as well as the ability to leverage the VAEC-Azure ATO.

The VAEC-Azure environment consists of three (3) geographic regions environments, one in Texas, one in Arizona, and one in Virginia. A simplified view of the VAEC-Azure architecture is provided below. Detailed architectural information will only be provided post contract award and/or during project provisioning.

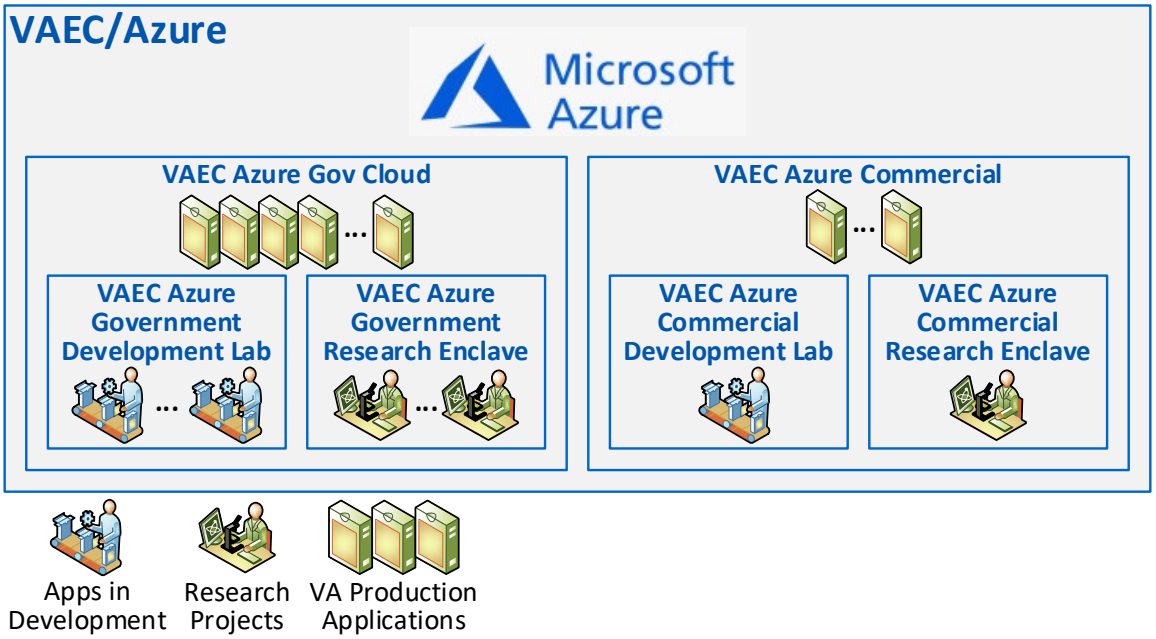

Figure 4. VAEC-Azure Component Layout

VAEC-Azure Components include:

- VAEC-Azure Gov Cloud is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant IaaS and PaaS

that has now received a FedRAMP JAB P-ATO. All Azure services are available immediately for supporting secure US government workloads, including CJIS, IRS 1075 FTI, HIPAA, DoD, and federal agency data. ***This is the default location for all hosted applications using the VAEC-Azure production environment.***

- VAEC-Azure Commercial is composed of the MS Azure public cloud computing platform. In the rare situation (adjudicated on a case-by case basis) that a project/customer cannot use the Azure Gov Cloud component (if, for example, they absolutely require an Azure service not available in Azure Gov Cloud), they will be provisioned in the Commercial space. ***The default VAEC-Azure hosting location is the Azure Gov Cloud.***
- VAEC-Azure Development Labs include both Government Labs (GLabs) hosted in VAC Azure Gov Cloud with connection to the VA Network and Commercial Labs (CLabs) hosted in the VAEC-Azure Commercial component. GLabs have all guard rails in place as a VAEC enclave, including Active Directory (AD), Single Sign On (SSO), Personal Identity Verification (PIV), Non-Mail Enabled Account (NEMA) capability, and use of the VA ePAS. GLabs are considered technically an extension of VAEC. CLabs have no VAEC guard rails built in. They use the VAEC-AWS Commercial component environment, with no connection to VA network, and will be provisioned in the cases where GLabs will not work. See the VAEC Enterprise Development Environment (EDE) and VA Platform One (VAPO) architecture information below for further details.
- Research Enclaves are provisioned for VA projects/customers where VA Researchers need timely access to leading edge cloud research tools and institutional data sources; they should not be expected to become infrastructure or cloud experts. See the VAEC Research and Analytics Super Platform (RASP) architecture information below for further details.

VAEC Enterprise Development Environment

The VAEC Enterprise Development Environment (EDE) test labs (also referred to as “Sandboxes”) were established in 2016, for Proof of Concept and VA applications/systems project development and testing. These labs are customer funded and a way to develop software applications, explore tools, and for cloud design pattern prototyping.

The development and lab environments are consumption based so you only pay for what you use. They are kept small in scope but are rapidly scalable and the labs are isolated development and test environments that allow VA projects to focus on their work and not on setting up a test environment.

As noted in Section 3 above, these are available in both VAEC-AWS and VAEC-Azure components, and in either the government community or public/commercial environments. As noted above, the government cloud labs are connected to the VA network, while commercial lab spaces are stand-alone, allowing for contractor access without VA credentials. VA applications/systems projects can get provisioned development lab space during the VLMF process (see Section 7 for details).

VA Platform One

VA Platform One (VAPO) is an enterprise-level turnkey development platform built using containerized technology and hosted in the VAEC. VAPO focuses on agility, ability to scale, and development project autonomy. It enables development teams, Product Managers, ISSOs, and IT Operations to work together with end-to-end visibility using a DevSecOps approach. It provides ready-to-use functionality for hybrid and multi-cloud systems development and includes innovative ways to reduce cost, increase efficiency and stabilize operations.

VAPO support the Cloud Smart migration initiative and is fully integrated into the VAEC intake process. VA Platform One utilizes commercial vendor-supported secure products (no open-source components) operating in both VA Data Centers and the VAEC government clouds (no commercial or public cloud presence). The core toolset is the TRM-approved RedHat OpenShift that has been VA security baselined, providing a positive impact towards achieving the system-level ATO.

VAPO also provides a platform for VA custom application systems, COTS applications, and (potentially) platform services. It currently hosts five custom applications and four COTS implementations.

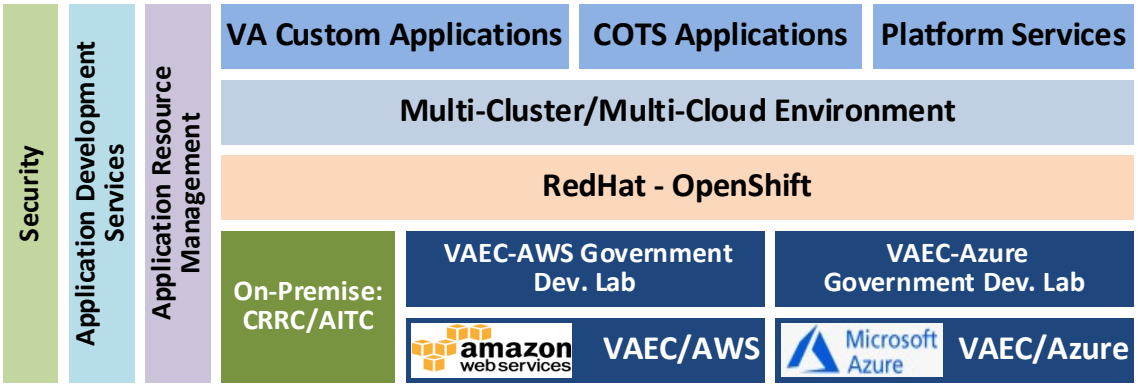

Figure 5. VAPO Architectural Layers

VAPO uses commercially available, vendor-supported secure products. The core component is the VA TRM-approved RedHat OpenShift Container Platform (RHOCP) with VA security baseline. VAPO contains no Open-Source upstream components. Developing in VAPO allows for expedited an ATO process. VAPO is available in in two VA Data Centers and the VAEC government cloud environments and is not locked into a particular hardware or cloud vendor. It is not, however, available in either VAEC-AWS or VAEC-Azure commercial/public clouds.

VAEC Research and Analytics Super Platform

The Research and Analytics Super Platform (RASP) is called a “super platform” as it sits as a layer above existing VAEC research platforms. RASP provides enforcing governance requirements around the use of non-IT funding in a standard way, ensures cloud services are used in accordance with VA policy, provides standardized enterprise monitoring and reporting, and provides easy inheritance of existing VAEC infrastructure- and platform-level security

controls speeding the ATO approval process. RASP includes a suite of tools to support VA research. It enables project teams to leverage pre-established capabilities to become productive quickly.

RASP includes access to native VAEC-AWS or VAEC-Azure CSP services, the VAEC-standard GSS toolkit and provides a platform for custom research code and data. RASP leverages existing, proven ECSO intake and support processes.

An overview of the RASP architecture is provided in Figure 6 below:

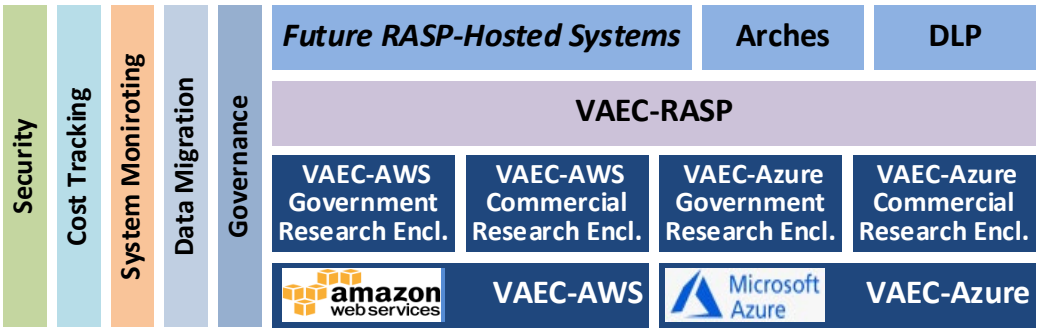

Figure 6. RASP Architectural Layers

RASP is built as a layer atop the VAEC-AWS and VAEC-Azure research enclaves—VA researchers can use whatever environment that provides the best value. It provides built-in support for security, cost tracking, performance monitoring. RAPS also includes resources for data migration technical support and a common set of governance controls ensuring funds are spent appropriately. Currently, two research-oriented systems are hosted in RASP, with more to come.

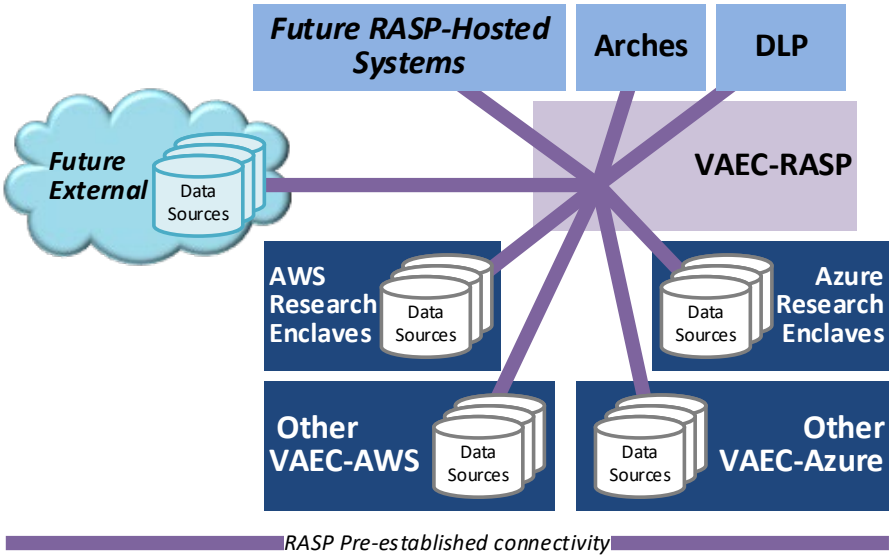

Figure 7. RASP Pre-established Connectivity

RASP includes pre-plumbed data connections which can be shared across users of RASP and pre-plumbed integrations to enterprise tools (e.g., API gateways, VDI tools, VAPO). It offers a place to host common/standard VHA/Office of Research & Development (ORD) data sources and services which can be shared across RASP users.

4 VAEC Network Topology

The VAEC environments use a common Trusted Internet Connections (TIC) compliant connection mechanism as shown in Figure 8 to connect back to the VA internal network. The connections are high bandwidth, fully redundant, encrypted connections with load balancers and firewalls as necessary to the respective endpoints. This section reflects the current state but changes will need to be made to reflect the future use of the TIC 3.0 architecture.

During onboarding (see the VLMF process overview in Section 7 for details), the VAEC team works with the project team to determine IP addressing requirements for each project environment and issue the required VA public and private IP addresses. Public inbound connectivity is blocked by default. Inbound public interfaces require VA approval. All inbound traffic must traverse the VA TIC. The VAEC team assists with the approval process.

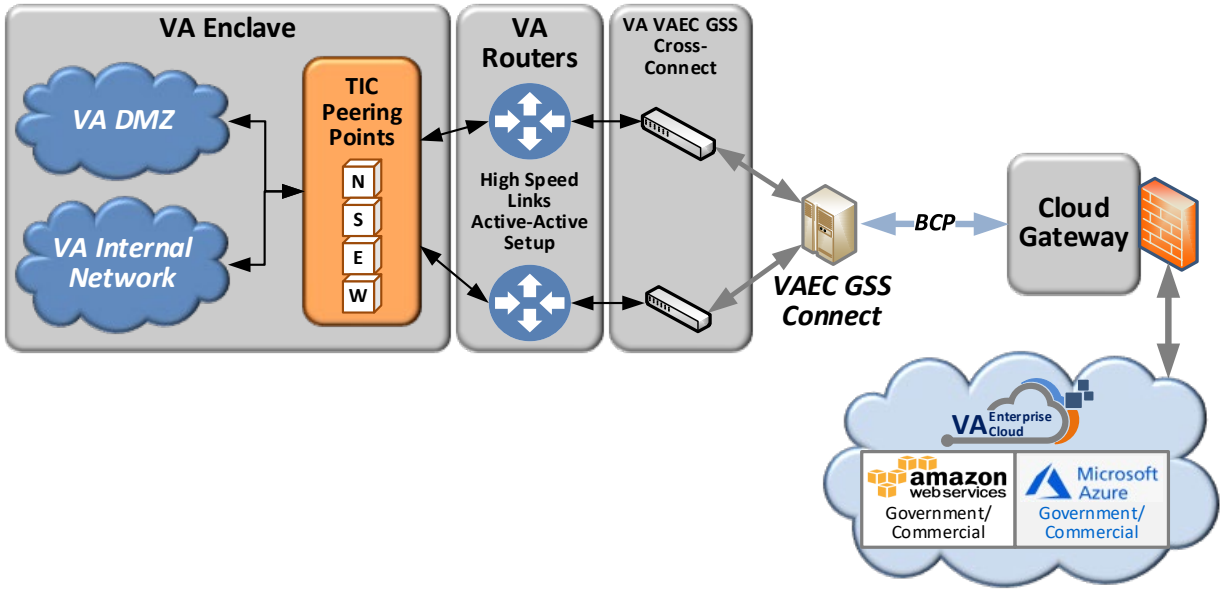

Figure 8. VAEC to VA Network Overview

The key feature for developers is that all VAEC-to-VA network traffic ***must*** go through the TIC, while intra-cloud traffic does not. The following describes applications/systems connectivity under several possible scenarios:

- **Both systems in same VPC**. Use direct addressing using virtual IP addresses.
- **Cross-FedRAMP boundaries**. Connectivity will have to be moderated through firewalls/gateways at each FedRAMP level.

- **Cross CSP Region**. Systems will be able to connect using virtual IP addresses provided during onboarding and will not have to traverse the VA TICs.
- **Cross-CSP Environments**. For connecting to systems that are hosted in a different VAEC CSP component, the interface will be go through the TIC infrastructure.
- **Cloud to/from VA On-Premises**. Any connection to a system/service hosted in a VA data center will need to pass though the VA TIC infrastructure.

This basic connectivity is reflected in the application view of network topology shown in Figure 9 below.

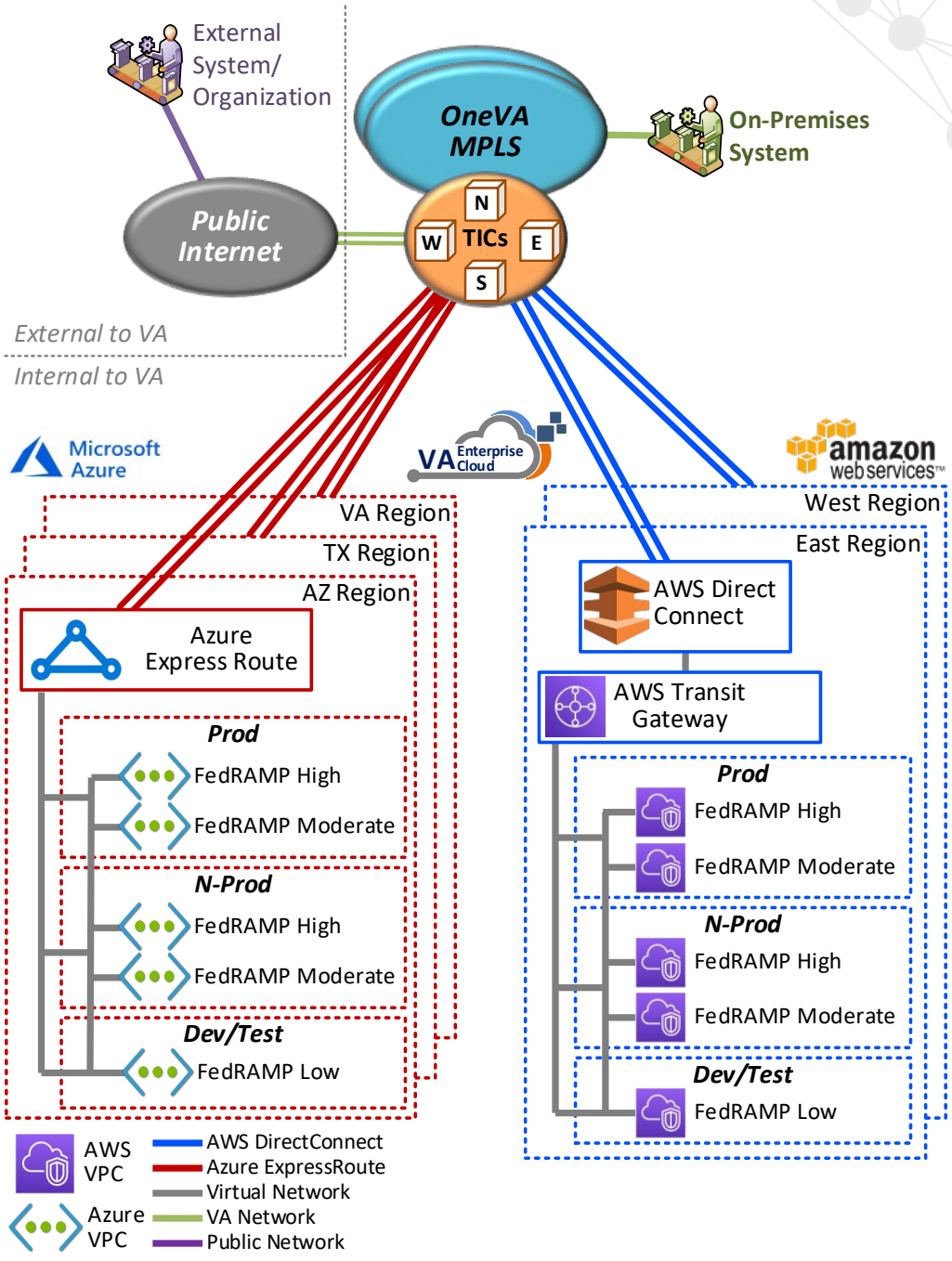

Figure 9. VAEC Application View of Network Topology

VAEC-AWS Network Topology

From the VA TICs, access to the VAEC-AWS components is via a set of redundant AWS Direct Connection links, mediated by the firewalls and routers provided by VAEC Network Services. Connectivity within and between VAEC-AWS regions is provided by the AWS Transit Gateway service. In each region, separate virtual environments are provided for production applications/systems, various pre-production (shown as “N-Prod” in the diagrams below)

environment use (as required by the project teams), and for applications/systems development/test. These are further segregated by virtual firewalls by FedRAMP levels. An overview of the VAEC-AWS network topology is shown in Figure 10 below.

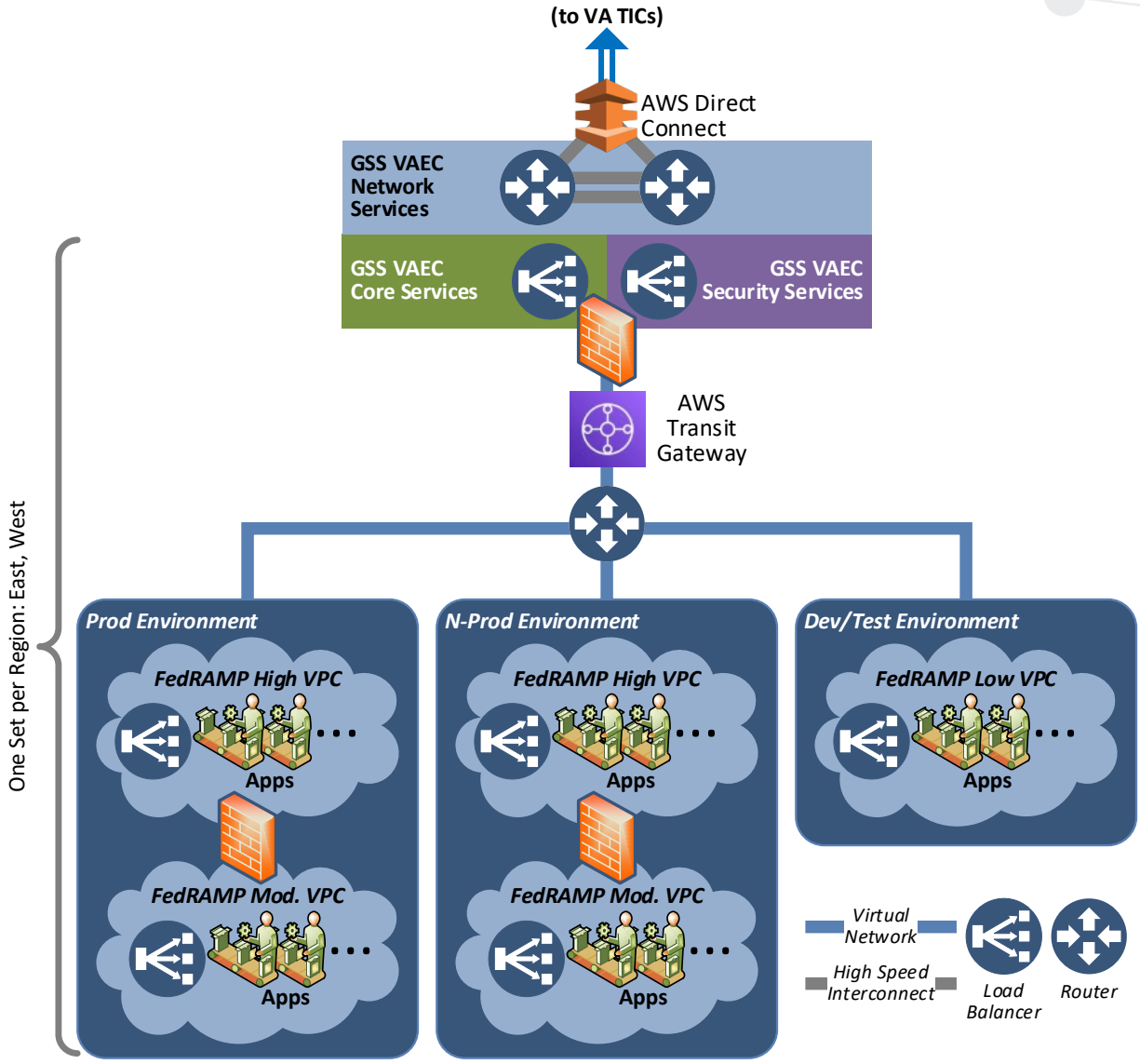

Figure 10. VAEC-AWS Network Connections

VAEC-Azure Network Topology

Similarly to VAEC-AWS, access to the VAEC-Azure components is via a set of redundant Azure Express Route links to VA TICs, mediated by the firewalls and routers provided by VAEC Network Services. Connectivity within and between VAEC-AWS regions is provided directly as part of the Azure Express Route service. In each region, separate virtual environments are provided for production applications/systems, various pre-production (shown as "N-Prod" in the diagrams below) environment use (as required by the project teams), and for

applications/systems development/test. These are further segregated by virtual firewalls by FedRAMP levels. An overview of the VAEC-Azure network topology is shown in Figure 11 below.

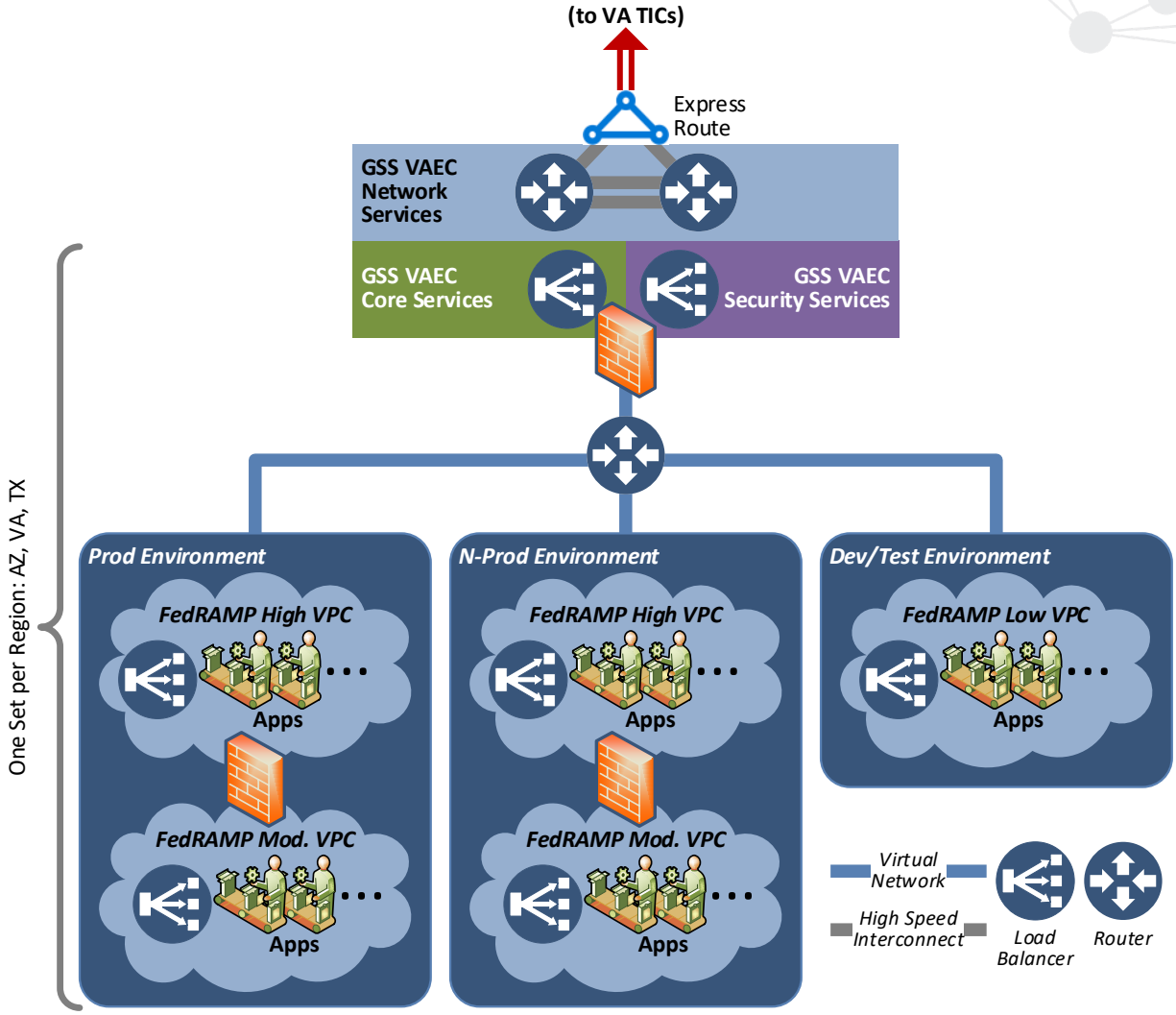

Figure 11. VAEC-Azure Network Connections

5 VAEC Cyber Security

Ensuring that sensitive Veteran data is secure, available, and safe from cyber threats is among the highest priorities of VA OIT. For that reason, applications hosted in any of the VAEC environments must meet the same rigorous cybersecurity requirements as any other VA IT system. These requirements are defined by the VA Handbook 6500 (Feb. 24, 2021), the VA Directive and Handbook 6517, Risk Management Framework for Cloud Computing Service (Nov. 15, 2016), and the National Institutes of Standards and Technology (NIST) 800 series, particularly Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 5, September 2020.

Shared Responsibility Model

In a typical on-premises application hosted in a VA-owned data center, the IT and Operations Services (ITOPS) team is typically responsible for security from the networking components through application-level security. Cloud-hosted systems use a shared responsibility model where the accountability for security is split among the Cloud Service Provider (CSP), the VAEC team, and the project team. This has two benefits. First, VA can take advantage of the billions of dollars of investments in security made by CSPs to build secure applications faster. Second, VA project teams can obtain an application-level ATO more quickly since their applications are only reviewed for the security controls that they are responsible for. The remaining security controls are inherited from the lower layer components which have already by tested by the Federal Risk and Authorization Management Program (FedRAMP) or VA OIT.

Table 1. Shared Security Responsibility Model

Security Level	On-Premises Responsibility	IaaS Responsibility
User Access	**Project Team**	**Project Team**
Data	**Project Team**	**Project Team**
Applications	**Project Team**	**Project Team**
Operating System	**Project Team**	VAEC/CSP
Network Traffic	ITOPS	VAEC/CSP
Hypervisor	ITOPS	VAEC/CSP
Infrastructure	ITOPS	VAEC/CSP
Physical	ITOPS	VAEC/CSP

User Access and Data is always the responsibility of the Project Team/cloud customer. The CSP/VAEC is responsible for security OF the cloud while the project team/ customer is responsible for security IN the cloud.

The VAEC adds another layer of inheritable controls at the GSS level. This architecture speeds up the ATO process even when compared with a more general cloud-hosted application.

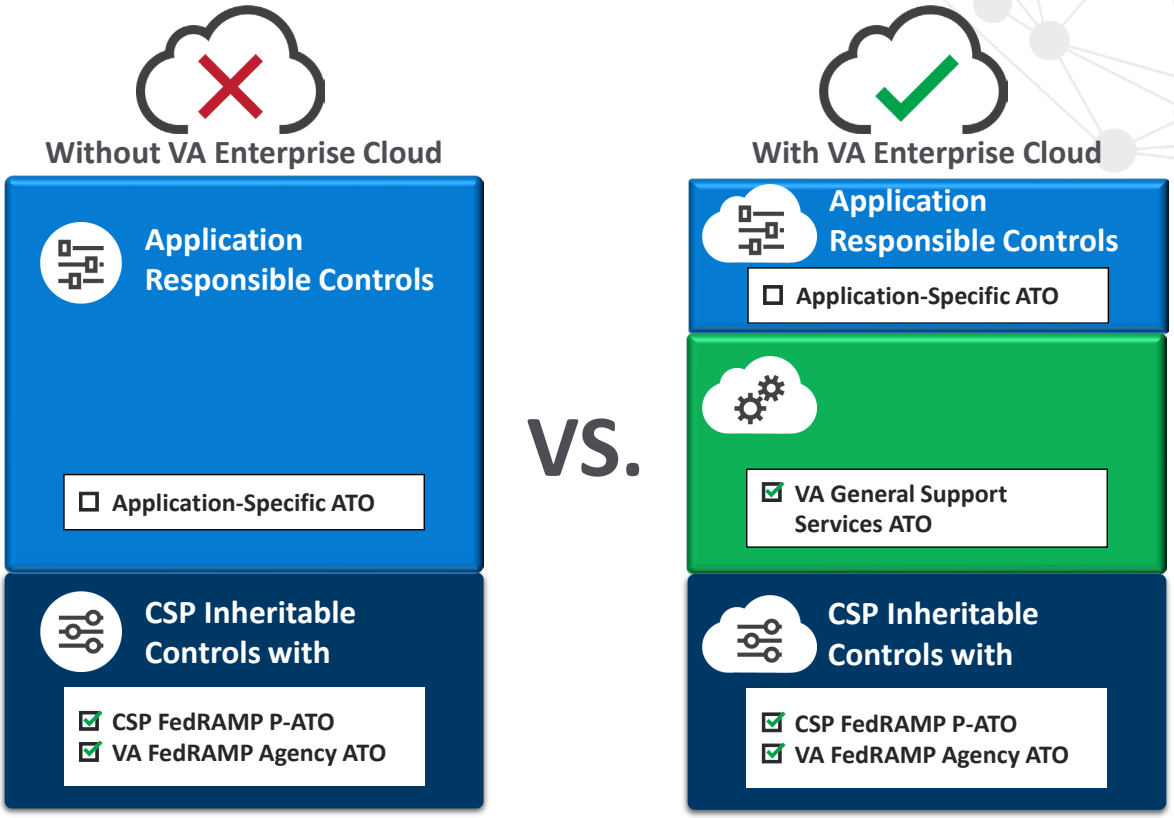

Figure 12. Inheritable Security Controls Model

Inheritable Security Controls

Both VAEC-AWS and VAEC-Azure currently provide 119 inheritable security and privacy controls. They fall into the following categories/families (based on the NIST 800-53 standard):

- Access Control (AC)
- Accountability, Audit, and Risk Management (AR)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Identification and Authentication (IA)
- Individual Participation and Redress (IP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Planning (PL)
- Program Management (PM)

- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- Security (SE)
- System and Information Integrity (SI)
- Transparency (TR)

For VAEC-hosted (using VAEC IaaS capabilities), the customer/project team can inherit these controls using the Management/Associates interface and simply select the appropriate VAEC environment as the source. Specific details will be provided when the project has been provisioned.

Authority to Operate

The VAEC currently has an ATO for both the AWS and Azure components. The ATO allows environments to be added at anything up to the FedRAMP high level of security. Any VAEC-hosted system/application that intends to move into a production status is required to obtain a VA ATO at the appropriate FedRAMP level. See *Obtaining a VA Application ATO* in Section 7 below for details on this process.

Other VAEC Cybersecurity Resources

The "Cybersecurity Resources" section from ECSO/VAEC SharePoint page with additional details will be available when VA account access has been provided.

6 Available Services and Tools

Each VAEC CSP environment (AWS and Azure) provides GSS tools to be leveraged by application/solutions developed and hosted within the environment. These tools and services simplify development, migration, and hosting of applications in the VAEC. Some tools are available in both VAEC environments (VAEC-AWS and VAEC-Azure) while others are exclusive to one CSP. In those cases, comparable tools exist in both environments. Other DevSecOps-oriented tools are also available in both VAEC CSPs.

ECSO Core Services

Core Services are provided to all VAEC customers. The only prerequisite to receive ECSO Core Services is having a Workflow Manager (WFM) ticket submitted. Core Services include basic cloud support from ECSO's six support teams. See Figure 2 for details on the ECSO organizational structure and the functions provided by ECSO teams.

Core services include:

- **Process Support**: Includes support for the VASI/VIPR processes, funding process, the application-level ATO process, and guidance on how to obtain an App code (required by the VA Business Office). Also includes an ECSO Customer Service & Support Manager (CSSM) to guide future support.

- **Application Development Support**: Includes applications architecture SME support, current and proposed design reviews, access to CSP architectural documentation, help in determining the target CSP, access to training, webinars, etc.
- **Documentation Support**: Includes project artifact templates and samples, artifact/documentation (intake, project plan, etc.) support and review.
- **Knowledge Management (KM) Support**: Includes the creation of a project-level SharePoint library and provides a VA policies and practices SharePoint site.
- **Project Management Support**: Includes general project/product management SME support, acquisition/procurement SME support, assistance in schedule development, strategic communications SME support, support for the development of the project migration and communications plans, full access to VAEC Service Catalog, Workflow Manager, and Maintenance Calendar, provide ROMs for predicted capacity and services, and helps to verifies funding/credits.
- **Migration and Installation Support**: Includes the development of environment provisioning plans and schedules, creation of required Virtual Private Cloud (VPCs) & Resource Groups per environment, access to backup and GSS tools (including GSS training, support, and troubleshooting), the provisioned cloud environments (development, test, and/or production as needed), assistance with procurement and licenses as needed, implementation of the Identity and Access Management (IAM) Framework per environment, assists in obtaining Enterprise Security External Change Control (ESECC) approval for proposed application connections, maps VAEC IP addresses and assists in obtaining TIC connection approval. Executes the actual migration or installation and ensures the application-level ATO is approved.
- **Operations Support**: Includes IOSS, Security, and Architecture support, CSP performance and availability reporting/tracking capabilities, assistance in CSP-level backup and restore, Infrastructure Operations Services Support (IOSS) SME availability, and applications security and architecture support as needed.

Note that the VAEC operates under a self-service model by default, whereby the working assumption is that each application team migrating to or operating in the VAEC provides the necessary support personnel to migrate and sustain their application.

Additional ECSO Services

ECSO Professional Services is a mechanism by which VAEC customers can get additional non-core cloud support services for their applications or systems. ECSO personnel will work directly with the VAEC customers providing SME support. The ECSO Application Services team can refer customers with non-core requirements to ECSO.

CloudKey

CloudKey serves as the ECSO solution for streamlining the data collection process for migrating systems to the VAEC. ECSO uses CloudKey to capture technical requirements and information that facilitates completion of the VLMF. Upon completion of the record, ECSO generates feedback which identifies the preferred VAEC environment that is eligible to host the system, along with the Criticality and Complexity of those systems. It also provides rough orders of magnitude (ROM) that reflect representative migration and hosting costs for the application in those target environments.

VAEC General Support Services

The VAEC GSS Toolkit is a collection of tools and services that are available in the VAEC that are either:

- Required for using cloud service provider (CSP) services,
- Mandated for usage by VA/ECSO policy, or
- Recommended for use to support typical project development and operations.

It is intended for use by Project Managers, System Architects, Information System Security Officers (ISSOs), VA Project Team Cloud Coders/Developers, Business Owners, and Budget staff (primarily for cost reporting).

Some GSS tools are required to be used by all hosted applications/systems, while others are those the project teams could or should use. For purposes of this document, the categories are defined below in Table 2 below.

Table 2. Tool Usage Key

Use Type	Definition
M: Must Use	Required use based on VA or ECSO policy
S: Should Use	Strongly recommended for use for most projects. Project may use other tools but may be liable for the additional cost
C: Could Use	Important but not necessary for all projects
W: Won't Use (at present)	Tools are not needed for most projects, not recommended for use due to policy or gaps in functionality or not yet available but planned for future use
F: Future	In the process of implementation—added for informational purposes

GSS tools are owned, paid for, and supported in three different ways. The responsibility information in the following table should be considered a general guideline only. Exceptions exist, so project teams should verify (with ECSO) the status and support responsibility of any desired tool or service before using it on a VA project. For purposes of this document, the responsibility categories are defined in Table 3 below.

Table 3. GSS Tool Responsibility

Tool Type	Description	Who Typically Pays
GSS-I	GSS Internal tool/service • Third-party tools that ECSO owns and operates • Provided as part of the VAEC-GSS environment	ECSO
GSS-E	GSS External tool/service • Owned by another VA group not ECSO • May provide limited support, in conjunction with support from the VA owner • In most cases, these are licenses procured by VA and are available to project teams	VA Owner
GSS-C	GSS-C: Cloud-Native (CSP, ECSO or Customer Operated) • Primarily services that are provided by the CSP and paid for by individual VA projects just as these projects pay for typical cloud services • ECSO may provide limited support for some of these services	ECSO or Project Team

The GSS tools are organized categories based on those from the Information Technology Infrastructure Library (ITIL) management practice areas. Figure 13 below shows these superimposed on the corresponding DevSecOps phases.

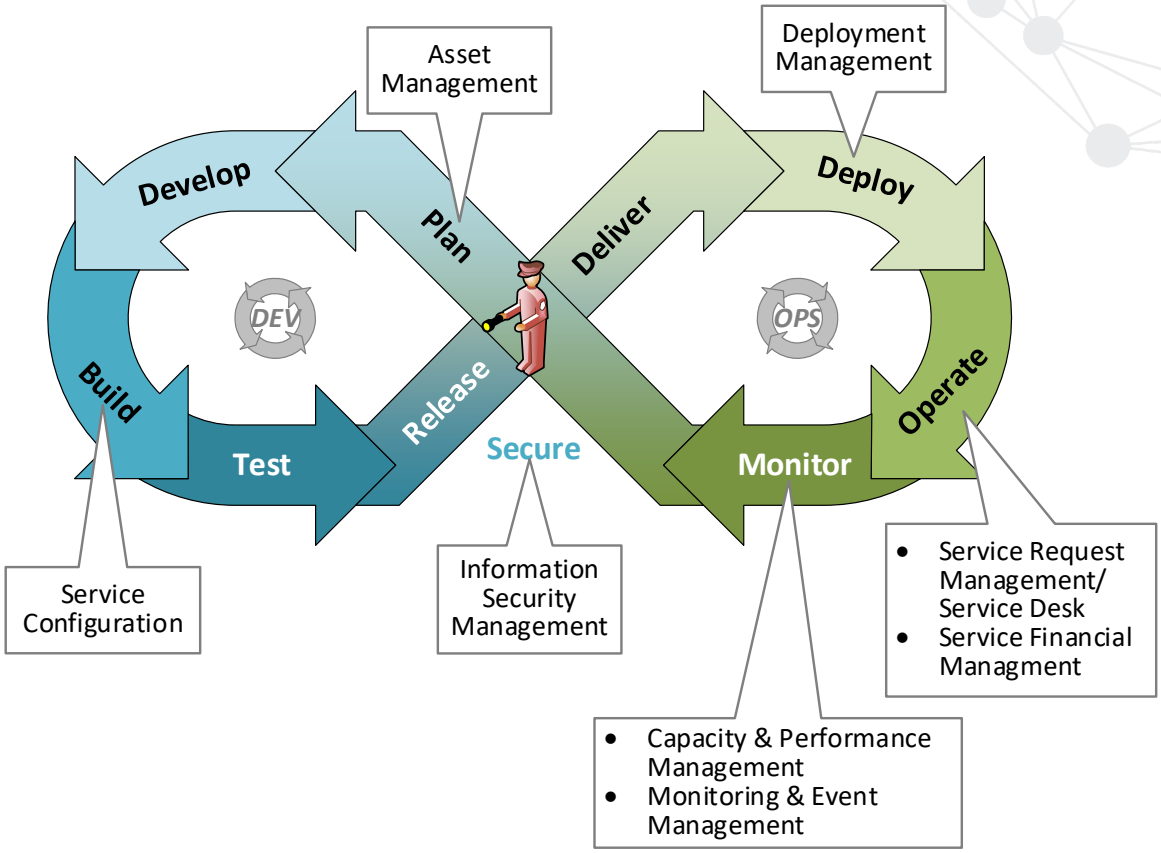

Figure 13. GSS Categories vs DevSecOps Phases

It is strongly recommended that project teams review their tools strategy with ECSO as part of their migration/development plan.

The following tables provides details on the available GSS tools organized by category. A tool is marked as "Initial?" if it is included as part of initial provisioning of an VAEC-AWS or VAEC-Azure account/project as part of the VAEC Lifecycle Management Framework (VLMF) process.

Table 4. Asset Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
BigFix	Provides system administrators with compliance checking and reporting. Enterprise-wide tool for both on-prem and cloud environments. **Required for ATO**. "All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix".	Both	M	GSS-E	X	

Table 5. Capacity and Performance Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Dynatrace	Preferred tool for application performance management. **Currently not charged back to project teams—but this may change.**	Both		GSS-E	X	
AppDynamics	Supports application performance management. ECSO supports the infrastructure platform, but ECC supports the application and user onboarding.	Both		GSS-E		

Table 6. Information Security GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Centrify (Linux only)	Handles privileged access management (PAM). Verifies who is requesting access, the context of the request, as well as the risk of the access environment.	Both	M	GSS-E	X	
eMass	Supports Information Assurance (IA) program management and supports the ATO process. Helps VA to maintain IA situational awareness, manage risk, and comply with the Federal Information Security Management Act (FISMA).	Both	M	GSS-E		Project security lead must use eMass
McAfee	Acts as VA's Host Intrusion Prevention System (HIPS) on all VA IT components based on host-based boundaries. Includes McAfee Data Loss Prevention Endpoint, which safeguards sensitive data and verifies compliance. **Being replaced by Microsoft Defender for Endpoints (MDE).**	Both	M	GSS-E		
Nessus	An open-source network vulnerability scanner. **A credentialed Nessus vulnerability scan is required for an ATO.** Projects can request a scan from the CSOC	Both	M	GSS-E		

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Turbot	Agentless tool which searches for and reports on vulnerabilities based on governance rules including enforcing tagging for billing. **Active on all VAEC-Azure and VAEC-AWS accounts.**	Both	M	GSS-I	X	
AWS GuardDuty	A continuous security monitoring service which can help to identify unauthorized or malicious activity in your AWS environment.	AWS	M	GSS-C	X	
AWS Identity and Access Management (IAM)	Controls access to AWS services through the use of security credentials (e.g., PIV cards) and permissions. **Not used directly by project teams.**	AWS	M	GSS-C	X	
AWS Inspector	Assesses resources for vulnerabilities or deviations from best practices, and then produces a detailed list of security findings prioritized by level of severity. AWS Inspector has been activated for select customers	AWS	M	GSS-C		
AWS Systems Manager	Provides a unified user view of operational data from multiple AWS services and enables you to automate operational tasks across AWS resources. Subcomponents used in VAEC: OpsCenter, Explorer, Inventory, Patch Manager and Parameter Storage. **See the VAEC Compliancy Tools guide for more info on which Systems Manager capability should not be used or not planned.**	AWS		GSS-C	X	Must be installed by projects on their EC2 instances/ virtual machines
Azure Active Directory (AD)	Provides single sign-on and multi-factor authentication. Projects are given instructions on how to connect users and systems to Azure AD during the VLMF process	Azure	M	GSS-C		
Azure ADFS (Active Directory Federated Service)		Azure	M	GSS-E		
Azure Policy	Used primarily by VAEC system administrators to identify and flag policy violations. Projects may receive notices from Azure Policy if issues are found.	Azure	M	GSS-C	X	

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Azure Resource Manager	Simplifies how projects manages your application's resources. Has scripting supporting infrastructure as code.	Azure		GSS-C		
Azure Role-Based Access Control (RBAC)	Provides fine-grained access management of Azure resources. Helps projects manage who has access to Azure resources, what they can do with those resources, and what areas they can access. Works with Azure AD and Azure ADFS. Elevated permissions are managed using the ePAS system.	Azure		GSS-C		
Azure Security Center	Set of tools for monitoring and managing the security of virtual machines and other cloud computing resources. Fed by Azure Monitor.	Azure	M	GSS-C		

Table 7. Monitoring and Event Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
AWS CloudTrail	Monitor/reports all application program interface (API) calls including calls from the AWS Management Console, AWS software development kits (SDKs), command line tools, and higher-level AWS services.	AWS		GSS-C		
AWS CloudWatch	Collects monitoring and operational data in the form of logs, metrics, and events, and visualizes it using automated dashboards providing a unified view of AWS resources, applications, and services. **Should be used by application teams who need custom monitoring & alerting of their application.**	AWS	S?	GSS-C		
AWS Elastisearch / LogStash / Kibana	Family of open-source tools often referred to as ELK which includes AWS Elasticsearch (search & analytics engine), AWS LogStash (data collection engine with real-time pipelining capabilities) and AWS Kibana (data visualization and exploration tool).	AWS	M	GSS-C		Collectively referred to as *Centralized Logging Solutions*

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
ScienceLogic (SL)	Infrastructure monitoring and Artificial Intelligence for Operations (AIOps) platform to predict, detect, and resolve IT problems faster. Performs discovery, dependency mapping, monitoring, alerting, ticketing, workflow automation, dashboarding, and reporting. In the process of being rolled out...	Both	MF	GSS-I	X	
Splunk	Collects and analyzes data on VA's technology infrastructure. Also support monitoring, alerting, and reporting. Used by CSOC and Enterprise Command Operations (ECO).	Both	M	GSS-E		
Azure Monitor	A cloud-native tool for monitoring VAEC-Azure infrastructure that is in the control of the project team. Log Analytics is also required on all Azure virtual machines, which feeds Azure Security Center (ASC).	Azure	M	GSS-C	X	
Azure Log Analytics	Provides to ability to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results. Used for reporting cloud compliance.	Azure	M	GSS-C	X	

Table 8. Service Configuration/Deployment Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
AWS Virtual Private Cloud (VPC)	A virtual, isolated network for every VA AWS account which enables access to AWS services such as VPMs, storage, etc. Changes to the virtual network are done by submitting a request to the ECSO WorkFlow Manager.	AWS	M	GSS-C	X	Network Configuration
AWS Direct Connect	Provides direct connectivity to the VA network. **Projects pay for outbound network costs.**	AWS	M	GSS-C	X	Network Configuration
Azure ExpressRoute	Provides direct connectivity to the VA network. **Projects pay for outbound network costs.**	Azure	M	GSS-C	X	Network Configuration

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Azure Virtual Network	A virtual, isolated network for VA Azure projects which enables access to Azure services such as VMs, storage, etc. Changes to the virtual network are done by submitting a request to the ECSO WorkFlow Manager.	Azure	M	GSS-C	X	Network Configuration
AWS Cloud Formation	Enables projects to create and provision AWS infrastructure deployments (infrastructure as code). Supports Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing, and Auto Scaling services.	AWS		GSS-C		System Configuration/ Deployment Management
AWS Configuration Manager	Ensures no unauthorized changes occurs for any resources in an account and logs the changer ID; projects will be alerted if a configuration changes based on the rule set.	AWS	M	GSS-C		System Configuration/ Deployment Management
Ansible Tower	Graphical user interface for Ansible, an open-source tool which enables software provisioning, configuration & orchestration management, and application-deployment tool enabling infrastructure as code.	Both		GSS-I		System Configuration/ Deployment Management

Table 9. Service Desk/Service Request Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
ServiceNow (SNOW)	VA's Enterprise Service Desk tool which is used to request equipment, services, software, incident resolution and other help services. **All non-VAEC service requests should be submitted to SNOW.**	Both	M	GSS-E		

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Workflow Manager	ECSO's work management system by which projects can request support such as implementing configuration or service changes, getting access to GitHub, or getting assistance for cloud viability assessment and planning, deployment, migration, and operational sustainment. Depending on their security and scope, Workflow Manager requests may generate a ServiceNow ticket	Both	M	GSS-I		

Table 10. Service Financial Management GSS Tools

Tool	Description	AWS/ Azure?	Usage	Support Type	Initial?	Notes
Apptio	A powerful reporting and dashboard tool to help VA project managers track VAEC spending and credits. VA project managers must use the tool to ensure that their project has sufficient cloud credits to pay for projected usage. Apptio will also provide project managers with an estimate of the number of months left given available funds for a project.	Both	M	GSS-I	X	
AWS Trusted Advisor	Provides real time guidance to help your project provision resources following AWS best practices. Trusted Advisor Helps optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Trust Advisor recommendations results are captured in Apptio.	AWS		GSS-C		
Azure Advisor	Analyzes your project's configurations and usage telemetry and offers customized, actionable recommendations to help optimize Azure resources for reliability, security, operational excellence, performance, and cost. Azure Advisor recommendations results are captured in Apptio.	Azure		GSS-C		

Other VAEC Tools

VAEC and the component CSPs provide other tools and services available to VA project teams. Development and operational tools are shown in Figure 14 below. The tools are organized by overall availability—those that are considered enterprise-level and other available tools

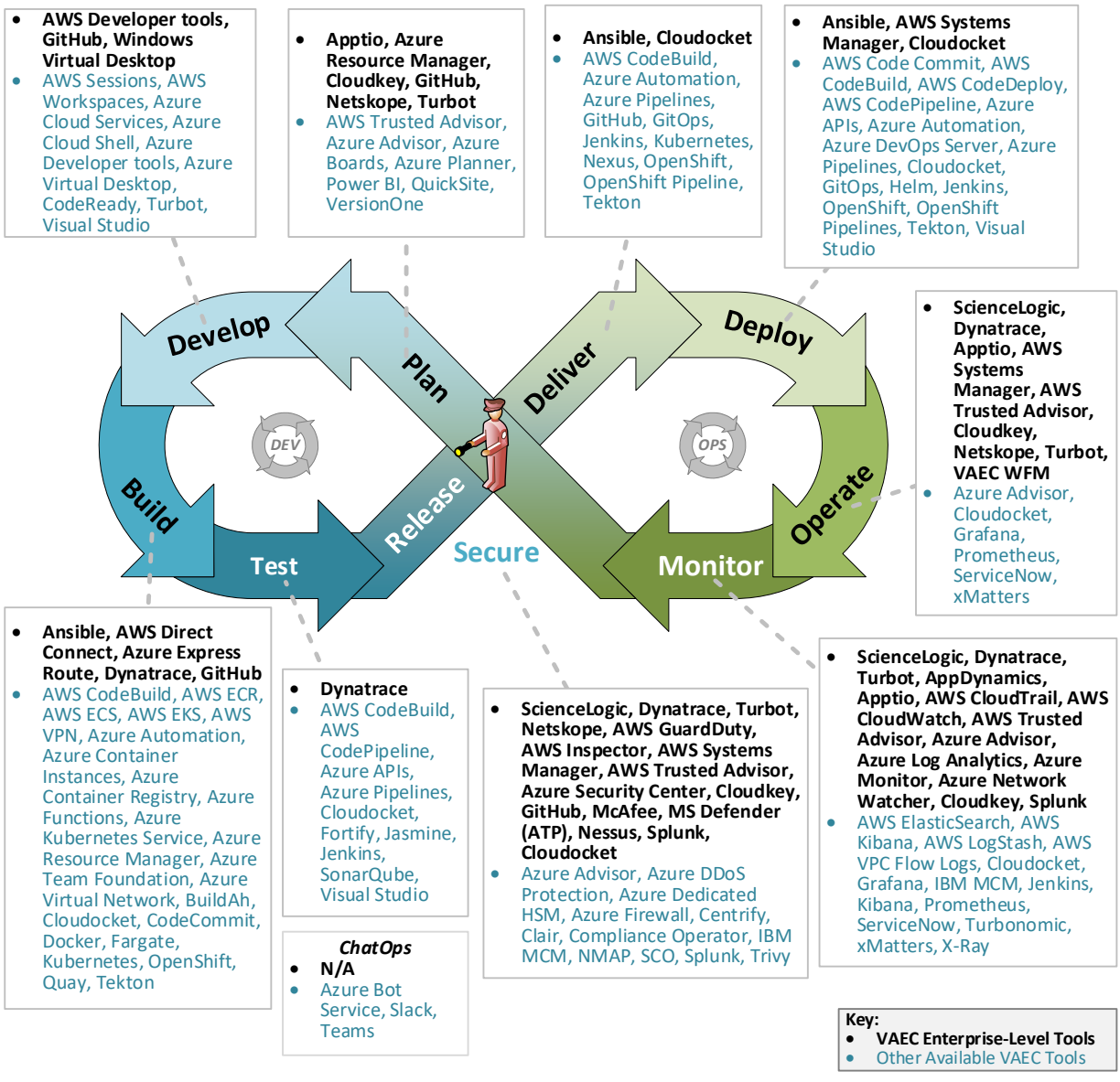

Figure 14. Other Available VAEC Tools by DevSecOps Phase

An interactive version of this diagram will be made available when the project team receives VA network access.

Available VAEC Services

Generally, all services provided by the underlying VAEC component CSPs will be available to the VA projects teams. Note that these are different in the commercial and government

environments. A listing of these services can be found on the publicly available AWS and Azure web sites.

In addition, several levels of support services are available through ECSO for production applications/systems hosted in the VAEC. Customer projects can manage all the aspects of a production system (the "Core" model), contract with ECSO and contractor staff to manage all but the actual application level (the "Gold" model) or some combination of the two (the "Mixed Managed" model). These will be negotiated as part of the VLMF process. Each of these models involves some level of on-going project resources to execute. An overview of cloud support models can be seen in Figure 15 below.

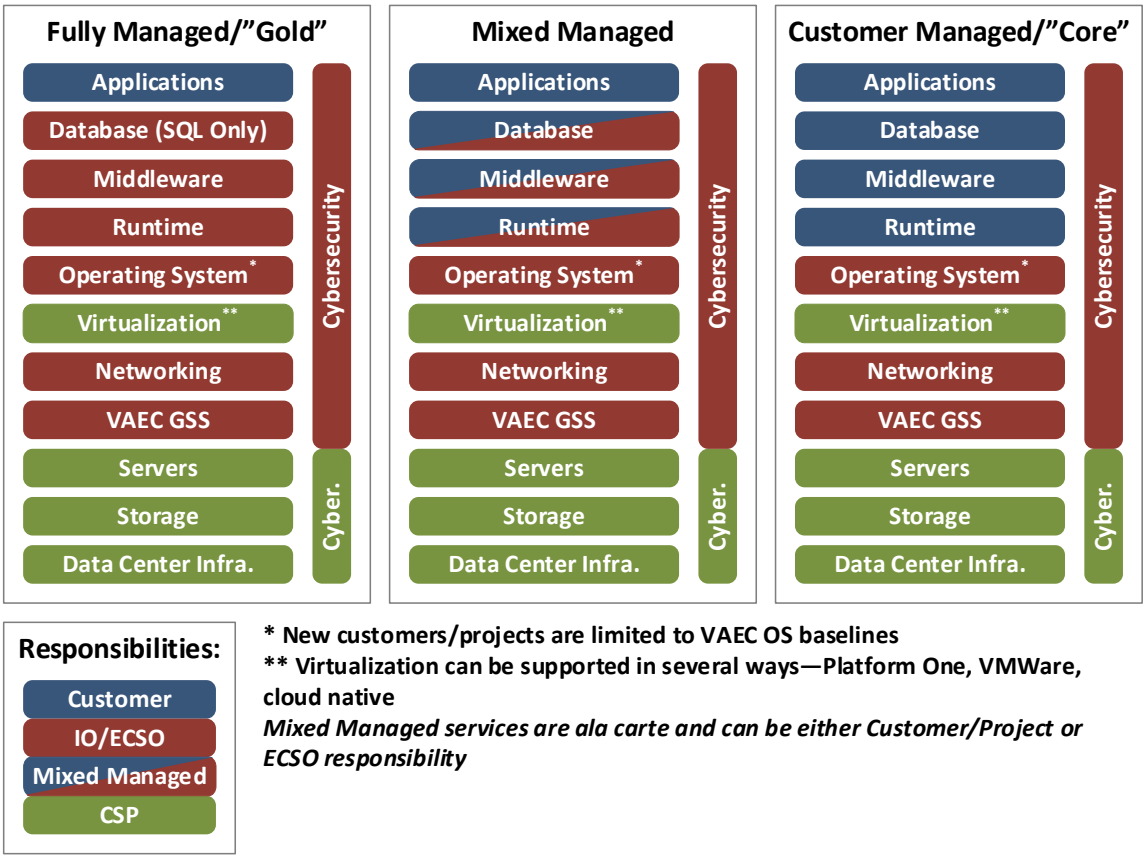

Figure 15. VAEC Support Models

7 VAEC Relevant Policies and Procedures

The VA cloud strategy identifies and describes goals, objectives, cloud development and migration strategies, and derived actions to implement and operate the VAEC. Together, these goals, objectives, and actions form the VAEC foundation for future roadmaps, concepts of operations, and standard operating procedures. The VA cloud strategy aligns with mandates issued by the White House, Congress, the Federal Chief Information Officer, and VA OIT, including:

- The Federal Chief Information Officer's (CIO's) "Cloud Smart" strategy

- The VA OIT Comprehensive Plan
- The VA Digital Transformation Strategy
- The VA Enterprise Roadmap

VA cloud-specific policies responding to these mandates include the joint Strategic Sourcing and Demand Management Division's Use of the VA Enterprise Cloud (VAEC) to Host Applications memorandum (29 October 2019), the Enterprise Program Management Office (OIT) memorandum, Use of Cloud-Based Native Technologies and Approaches (29 October 2019), and the Principal Deputy Assistant Secretary for Office of Information Technology (OIT) memorandum, Use of the VA Enterprise Cloud (VAEC) for New Development, 7 Jan 2019 .See Appendix A for details.

Specific policies and procedures relating to the TRG are included below.

VAEC Software Installation Policy

Any software installed on virtual machines (VM) operating in the VAEC at the IaaS or PaaS levels must be VA Technical Reference Model (TRM) compliant or have an approved waiver.

Elevated Privileges Policy

A VA account is required for read-only access to the AWS Console and/or Azure Portal. Elevated privileges are required for administrator access to the AWS console and/or Azure Portal. Please submit an Elevated Privileges request through ePAS early to avoid delays in accessing your account or subscription.

VAEC Lifecycle Management Framework

The Enterprise Cloud Solutions Office (ECSO) established the VAEC Lifecycle Management Framework (VLMF), a step-by-step methodology to planning, migration, and operation of VA applications in the VAEC. ECSO customers understand that cloud migration or deployment are multi-faceted efforts and completing these activities while staying on schedule, on budget, and in compliance with VA policy can be a balancing act. VLMF organizes cloud migration or deployment activities into nine steps. The nine-step process is a step-by-step approach to intake, provisioning, deployment, and sustainment of Veterans Affairs (VA) applications in the VAEC.

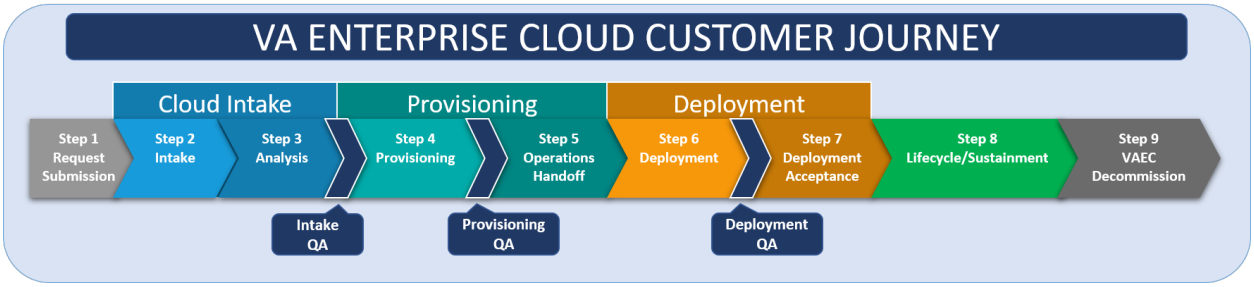

Figure 16. VLMF Overview

An overview of VA project team responsibilities in each phase is included below:

Phase 1: Request Submission

- **Objective**: Validate that an application team meets the basic requirements for VAEC hosting.
- **Project team Responsibilities**:
    - Initiate the project through Veteran -Focused Integration Process (VIP) Request (VIPR) or WFM ticket. VIP is the VA-standard systems lifecycle.
    - Initiate Step 1 of VIPR process.
    - Initiate VA funding request.
    - Complete VA Systems Inventory (VASI) process and obtain a VASI ID for the system.
    - Submit Product Line Change Request
    - When VASI is complete, start the Business Office (BO) App Code process.

Phase 2: Intake

- **Objective**: Gather detailed business, technical, and project data to support upcoming analysis efforts for provisioning and deployment.
- **Project team Responsibilities**:
    - Provide the project information to the ECSO Intake Analyst and ECSO/COMS Service and Support Manager (CSSM). Information required includes an As Is Architecture Diagram, Initial Operating Capability (IOC) Memorandum of Understanding (MOU), and other relevant server, storage, and POC details.

Phase 3: Analysis

- **Objective**: Provide guidance for the cloud implementation approach for the application.
- **Project team Responsibilities**:
    - Review the completed documentation set with the ECSO Intake Analyst and provide any missing information.
    - Obtain the link to the relevant credit transfer request.
    - Provide a signed Cloud Credit Management MOU.
    - Identify the ECSO Sustainment Manager for technical support after the application has gone into production.

Phase 4: Provisioning

- **Objective**: Allocate CSP resources for the application, grant access, and obtain accessibility to the environment.
- **Project team Responsibilities**:
    - Obtain a signed VA Form 2237, allocating funding for the agreed services/cost.

- Meet with the CSSM to determine what (if any) ECSO Professional Services will be needed during the project, based on the VAEC deployment support required. Obtain funding and a signed Professional Services Agreement if needed.

Phase 5: Operations Handoff

- **Objective**: To hand off the respective environment to support deployment efforts.
- **Project team Responsibilities**:
  - Review the provisioned environment and next steps with the CSSM.
  - Review credit management procedures with the ECSO CSP Lead.

Phase 6: Deployment

- **Objective**: Deploy and/or migrate the application, along with its virtual machines, data stores, network access, and related software into the CSP/ provisioned environments.
- **Project team Responsibilities**:
  - Submit ePAS requests for environment(s) to the Enterprise Security Engineering Change Council (ESECC), establish CSP Console access, and provide access to consumption reporting.
  - Track the target deployment completion date.
  - Track the high-level status of the build efforts.
  - Provide the tool(s) that will be used for monitoring and logging of the application.
  - Obtain a VA ATO for the application/system.
  - Provide the completed deployment Go/No Go checklist.

Phase 7: Deployment Acceptance

- **Objective**: Validate all ECSO requirements have been met and approve the final deployment effort.
- **Project team Responsibilities**:
  - Track final deployment Go/No Go decision and take necessary corrective action.

Phase 8: Lifecycle/Sustainment

- **Objective**: Operate and maintain the system to provide end user functionality.
- **Project team Responsibilities**:
  - Ensure all operations and maintenance (O&M) activities are completed unless engaged in a Professional Services Agreement. If a Professional Services Agreement is procured, ECSO/COMS will perform all agreed upon O&M work in this VLMF step.

Phase 9: VAEC Decommissioning

- **Objective**: Perform migration or end-of-life activities for an application leaving its VAEC environment.
- **Project team Responsibilities**:
    - Initiate WFM ticket to begin decommissioning process.
    - Support decommissioning planning session with CSSM.
    - Turn off and remove all resources within their account or subscription.
    - Initiate a cloud credit transfer either into or out of the account for a zero balance.
    - Notify VASI team to deactivate VASI entry.
    - Notify Franchise Fund Business Office to deactivate app code.

Product Line Change Request Process/Policy

Product line and portfolio alignment is critical to VLMF. If a VA application/system project team does not know which product line to align to through the VASI process, then the VA PM needs to submit a Product Line Change Request (PLCR) intake form as soon as possible to avoid delays within VLMF.

The PLCR Intake Form is a tool used for product line changes. This tool provides continuous a feedback loop to stakeholders. Requests approved through the PLCR process only will be updated in VASI.

For questions regarding the PLCR process contact the ACOE Metrics and Analytics office: ACOEMetricsAnalytics@va.gov.

Obtaining a VAEC Application Code

The three-digit application (App) code is a system/application identifier issued by the Franchise Fund Business Office (FFBO) Customer Agreement Management (CAM) group. This identifier is used for billing purposes. Any system/application billing in the VAEC must have an app code. Systems in lab environments will share the app code of the lab environment.

To obtain an app code, please submit an App Code Request Form to the Infrastructure Operations (IO) Business Office via an VA intranet on-line form. This will be available when VA Project Teams have VA access.

Enterprise Security External Change Council Process

The VA Enterprise Security External Change Council (ESECC) was established to ensure all proposed changes to the VA network are reviewed to ensure viability and will not adversely impact the operation of the existing system or subsystem. ESECC process notes include:

- All changes to the VA's network infrastructure must be submitted to the ESECC for evaluation and approval.
- Review and disposition of proposed modifications to current baselines and recommend resources for system security maintenance and/or enhancements.
- Ensure that proposed change will not have a negative impact on current operations.

- Approve updated baselines and documentation.
- Approve deviations from standards and schedules on a case-by-case basis.
- Inform the appropriate services in the Office of Cyber Security (OCS) and Administrations, Information & Technology Field Security Operations (FSO) of any VA hardware/software configuration changes that affect the current system security configuration standards and/or affect other organizations.

Change requests are requested and managed via an VA intranet on-line form. This will be available when VA Project Teams have VA access.

Obtaining a VA Application ATO

Prior to receiving application-level ATO, an information system must progress through each of the first five of the six steps in the Risk Management Framework (RMF), as described in NIST SP800-37. These are:

1. **Security Categorization.** Categorize the security level required by the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
2. **Control Selection**. Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. **Control Implementation**. Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
4. **Control Assessment**. Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. **Authorization**. Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. At this point the application/system will receive the official ATO.
6. **Continuous Monitoring**. Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. This phase will continue through the life of the production application/system.

These steps are supported in the VA by the Enterprise Mission Assurance Support System (eMASS) tool. For further details, see the *Enterprise Mission Assurance Support System (eMASS) Implementation Guide*, which includes a sample ATO process, and will be available when VA account access has been provided.

ECSO has available templates (on the VA network) for the following required ATO documents:

- VAEC AWS/Microsoft Azure Government (MAG) Incident Response Plan
- VAEC AWS/MAG Disaster Recovery Plan
- VAEC AWS/MAG Configuration Management Plan
- VAEC AWS/MAG Information System Contingency Plan
- ITOPS CP Test Script
- ITOPS DRP Test Script
- ITOPS Test Results
- ITOPS IRP Test Script

The ECSO OPS team can run an ***unofficial*** pre-ATO Nessus scans for your environment to aid in assessing your security posture. The VAEC OPS Team will run one unofficial scan for your ATO to determine your vulnerability remediation and one unofficial scan once you have done your remediation. Your application must be installed on your virtual VAEC servers before the team runs the initial scan. Once your ATO is received, any subsequent Nessus scans must be requested from the Cyber Security Operations Center (CSOC).

PLEASE NOTE: These scans cannot be submitted as evidence with your ATO. Only official CSOC scans can be submitted with your ATO package.

VAEC Health Assessment Process

The VAEC Health Assessment (VAEC HA) is a 4-phase evaluation process for production applications hosted in the VAEC. The VAEC HA process is performed for all VAEC-hosted applications/systems once they are considered in production. Areas where reliability, performance, security, and compliance with VA and VAEC policy can be improved are identified. Application Project Teams are then advised of available resources, services, and training to improve application health.

An overview of the VAEC HA process is described below.

Phase 1: Intro and Data Collection

- Introduction to Health Assessment Process
- System Documentation and Data Collection

Phase 2: System Assessment

- System Security Assessment Conducted
- System Architecture Assessment Conducted

Phase 3: Deliverable

- HA Report reviewed by ECSO Leadership
- HA Report provided to application project team

Phase 4: Implementation

- HA findings entered CloudKey (see Section 6, *Available Services and* Tools) for Implementation Tracking
- Project Teams review, update, and track status of implementation of findings in CloudKey

8 VAEC Points of Contact

General ECSO or VAEC Questions: ECSOInfo@va.gov

Migration questions, needs or support: VAITECIntakeMailbox@va.gov

VAEC Cloud Security questions, concerns, or needs: VAECSecurityTeam@va.gov

General question about Cloud Operations & Migration Services (COMS) and the

VAEC Workflow Manager: Comsrequests@va.gov

VAEC Cloud Management Requests, including inquiries for cloud credit requests, cloud migration services and sustainment support requests, Out of Cycle Federal Technology Acquisition Reform Act (FITARA) approvals, and other VAEC cloud management questions: VAECCloudManagement@va.gov

Acquisitions (Purchasing cloud credits for either the VA Enterprise Cloud Capacity contract or the Microsoft (MS) Enterprise License Agreement): VAECAcquisition@va.gov

Technology Acquisition Center (TAC) (for questions about cloud acquisitions): VAECAcquisitionAssist@va.gov

Testing and Development Environment/Sandbox: ECSODevTest@va.gov

Facilitate a ServiceNow Request or Support Incident: Call (855) 255-1854 for production VAEC incidents or outages.

Appendix A: References

1. Department of Veterans Affairs Memorandum, Subject: *Use of Cloud Native Technologies and Approaches*, B. James, 10 Apr 2018
2. Department of Veterans Affairs Memorandum, Subject: *Use of Cloud-Based Native Technologies and Approaches*, J. Everett, Associate Deputy Assistant Secretary, Enterprise Program Management Office (OIT), 29 October 2019
3. Department of Veterans Affairs Memorandum, Subject: *Use of VA Enterprise Cloud (VAEC) to Host Applications*, John P. Everett, Associate Deputy Assistant Secretary, EPMO, OIT, 29 October 2019
4. Department of Veterans Affairs Memorandum, Subject: *Use of VA Enterprise Cloud (VAEC) for New Development (VIEWS 00124536)*, D. Cussat, Principal Deputy Assistant Secretary for OIT, 7 Jan 2019, URL: https://vaww.portal.va.gov/sites/ECS/Shared Documents/Cloud 101/VAEC First Policy Memo 07-Jan-2019.pdf
5. Department of Veterans Affairs Memorandum, Subject: *Use of VA Enterprise Cloud (VAEC) to Host Applications*, J. Everett and L. Jones, 16 Jan 2018
6. Department of Veterans Affairs, *VA Directive 6517, Risk Management Framework for Cloud Computing Services*, Department of Veterans Affairs, Washington, DC, 15 Nov 2016
7. *From Cloud First to Cloud Smart*, Federal Cloud Computing Strategy, OMB/Office of the Federal Chief Information Officer, URL: https://cloud.cio.gov/strategy/
8. NIST Special Publication 800-145*, The NIST Definition of Cloud Computing*, National Institute of Standards and Technology (NIST), September 2011
9. *VA Enterprise Cloud Solutions Office (ECSO) Portal*, URL: https://dvagov.sharepoint.com/sites/OITECSO/SitePages/VA-Enterprise-Cloud-VAEC.aspx , accessed January 2021

Appendix B: Acronyms

Acronym	Definition
ACOE	VA/OIT/DSO/BO/Agile Center of Excellence
APM	Applications Performance Monitoring
ATO	Authorization to Operate
BO	VA/OIT/DSO/Business Office
CI/CD	Continuous Integration/Continuous Delivery
CIO	Chief Information Officer
CISO	Cyber and Information Security Officer
COTS	Commercial off-the-Shelf
CSOC	Cyber Security Operations Center
CSP	Cloud Service Provider
CSSM	ECSO/COMS Service and Support Manager
DevSecOps	Development/Cybersecurity/Operations (combined)
DSO	DevSecOps Organization
ECSO	Enterprise Cloud Solutions Office
EDE	Enterprise Development Environment
ePAS	Electronic Permission Access System
EPMO	Enterprise Program Management Office
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSS	General Support Services
IaaS	Infrastructure as a Service
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITAR	International Traffic in Arms Regulation
MPLS	Multiprotocol Label Switching
NCA	National Cemetery Administration
OCM	Organizational Change Management
OIS	Office of Information Security
OIT	Office of Information and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
SLO	Service Level Objective
TIC	Trusted Internet Connection
VA	Department of Veterans Affairs
VAEC	VA Enterprise Cloud

Acronym	Definition
VAPO	VA Platform One
VBA	Veterans Benefits Administration
VBMS	Veterans Benefits Management System
VHA	Veterans Health Administration
VistA	Veterans Health Information System and Technology Architecture
VLMF	VAEC Lifecycle Management Framework
WFM	Workflow Manager