

**OFFICE OF  
VA ENTERPRISE  
ARCHITECTURE**

**VA EA Enterprise Technical  
Architecture Compliance Criteria**

**Version 8.0**

**Configuration Item: 5.2.5-2002AF-2016-8-24-230**

**September 30, 2016**

## Revision History

Change Number	Date of Change	Individual Making Change	Description of Change
1.0	8/12/2012	VA EA	Initial Version Published
2.0	9/30/2013	VA EA	Published
3.0	3/31/2014	VA EA	Published
4.0	6/30/2014	VA EA	Published
5.0	10/31/2014	VA EA	Published
6.0	4/30/2015	VA EA	Published
7.0	9/30/2015	VA EA	Published
8.0	9/30/2016	VA EA	Published

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Executive Summary .....	1
1.2	Overview .....	1
1.2.1	VA EA Global Principles .....	1
1.2.2	VA EA Purpose.....	2
1.2.3	Enterprise Architecture: Technical Layer .....	3
1.3	Scope.....	5
1.3.1	Relationship to Other Related Processes.....	5
1.3.2	Solution Types.....	6
1.4	Purpose.....	6
1.5	Document Conventions .....	7
1.6	Audience .....	7
<b>2</b>	<b>Compliance Criteria .....</b>	<b>8</b>
2.1	Mission Alignment.....	8
2.1.1	Veteran-Centric Solutions .....	8
2.1.2	Business Architecture.....	10
2.1.3	Mission Criticality .....	11
2.2	Data Visibility and Accessibility .....	12
2.2.1	N-Tier Architecture .....	12
2.2.2	Data Independence.....	14
2.2.3	Common Look and Feel.....	15
2.2.4	Data Persistence.....	16
2.2.5	Test-Driven Development .....	17
2.2.6	Exception Handling .....	18
2.2.7	Scalability .....	19
2.2.8	Stateless Business Logic .....	20
2.2.9	Accessibility Requirements .....	21
2.3	Data Interoperability .....	22
2.3.1	Data Standards.....	22
2.3.2	Authoritative Information Sources .....	23
2.3.3	Enterprise Logical Data Model .....	24
2.3.4	Local Copies of Authoritative Information Sources .....	26
2.3.5	VA Data Inventory .....	27
2.4	Infrastructure Interoperability .....	28
2.4.1	Cloud First .....	28
2.4.2	Standard Operating System Images.....	30
2.4.3	Standard Databases .....	31

2.4.4	Virtualization .....	32
2.4.5	Infrastructure Capacity .....	33
2.4.6	Storage .....	34
2.4.7	Network Configurations.....	35
2.4.8	Transmission Control Protocol/Internet Protocol v6.....	36
2.4.9	System Monitoring.....	37
2.4.10	Disaster Recovery.....	38
2.4.11	Backup and Restore .....	40
2.4.12	Thin Client .....	41
2.5	Information Security.....	42
2.5.1	Security Regulations.....	42
2.5.2	External Hosting.....	44
2.5.3	Secure Access Paths .....	45
2.5.4	Secure Information Sharing .....	47
2.5.5	Personally Identifiable Information and Protected Health Information .....	49
2.5.6	Homeland Security Presidential Directive 12 .....	51
2.6	Enterprise Capabilities.....	53
2.6.1	Messaging Standards – Simple-Object Access Protocol-Based Services .....	53
2.6.2	Messaging Standards – Healthcare Information Exchange .....	55
2.6.3	Service Registry .....	57
2.6.4	Service Reuse .....	58
2.6.5	Service Architecture Layering .....	59
2.6.6	Service Types.....	61
2.6.7	Service Design .....	62
2.6.8	Extensible Markup Language Standards.....	64
2.6.9	External System Access .....	65
2.6.10	Service Access .....	66
2.6.11	Service Documentation.....	67
2.6.12	ESS Governance Approval .....	68
2.6.13	Identity and Access Management (IAM) Service .....	70
2.6.14	Service-Enabled Information Sharing .....	72
2.6.15	Technical Reference Model .....	74
2.6.16	COTS Products.....	76
2.6.17	VA Systems Inventory (VASI).....	78
2.6.18	Enterprise Message Infrastructure .....	79
2.6.19	Open Source Software .....	81
2.6.20	Standardized National Software .....	82
<b>Appendix A</b>	<b>Acronyms and Abbreviations .....</b>	<b>A-1</b>
<b>Appendix B</b>	<b>Terms and Definitions.....</b>	<b>B-1</b>
<b>Appendix C</b>	<b>References.....</b>	<b>C-1</b>
<b>Appendix D</b>	<b>ETA Compliance Criteria Frequently Asked Questions.....</b>	<b>D-1</b>

D1 Purpose of FAQs ..... D-1  
D2 Frequently Asked Questions..... D-2  
**Appendix E PMAS Milestone Artifacts .....E-1**

## Table of Figures

Figure 1-1: VA EA..... 3  
Figure 1-2: VA ETA Compliance Criteria..... 4

## Table of Tables

Table 1-1: Solution Types..... 6

# 1 Introduction

## 1.1 Executive Summary

The Department of Veterans Affairs (VA) is transforming in an effort to improve its support to Veterans. To achieve a level of seamless support for VA, a more efficient and better-integrated enterprise is required. The envisioned enterprise creates the alignment of strategic direction, business operations, technology and data, and is methodically designed, aggregated, and managed to deliver the right information to the right place at the right time.

At the core of this transformation is the VA Enterprise Architecture (EA). The VA EA is the strategic planning and management tool that supports operations execution and management accountability, and equips leadership to execute change across the Department. The VA EA provides the enterprise-level line-of-sight needed to support informed decision-making. As an authoritative reference, the VA EA provides an integrated view of the different domains of enterprise data across all levels of VA: VA-wide, Segment, and Solution levels.

The combination of intent, resources, methodology, and execution aligned through the VA EA enables a VA enterprise that provides a consistent and seamless experience for accessing information, and delivering improved services to U.S. Veterans and their families.

The VA EA Compliance Criteria Report serves to support the VA EA vision and mission in providing valuable products, services, and capabilities for the VA. Specifically, this report establishes minimum compliance criteria to assist both program developers and VA investment decision-makers in ensuring alignment of VA programs, projects, initiatives, or investments with the technical layer of the VA EA. This layer, named the VA Enterprise Technical Architecture (ETA), details rules and standards for use and configuration of VA networks as well as standards for information security and application design. These rules and standards apply to all VA information technology (IT) solutions and investments.

## 1.2 Overview

The VA EA is a strategic, enterprise-wide, information asset base that identifies and aligns critical business factors, information, and technologies necessary to perform the VA mission and the transitional processes for implementing new capabilities in response to changing mission needs. VA EA is guided by a set of global principles that have been vetted by the VA Enterprise Architecture Council (EAC). These principles direct VA capabilities to adopt enterprise approaches and services to the greatest extent possible in delivering capabilities to Veterans and employees. This not only eliminates wasteful duplication of services and capabilities, but also ensures better interoperability of capabilities and services rendered to Veterans and VA employees.

### 1.2.1 VA EA Global Principles

The VA EA Global Principles are:

1. Mission Alignment – VA information, systems, and processes shall be conceived, designed, operated, and managed to address the Veteran-centric mission needs of the Department.

2. Data Visibility and Accessibility – VA Application, Service, and Data Assets shall be visible, accessible, available, understandable, and trusted to all authorized users (including unanticipated users).
3. Data Interoperability – VA Information shall be made interoperable through data standardization, including the identification, designation, and utilization of authoritative sources.
4. Infrastructure Interoperability – VA IT Infrastructure shall be made interoperable through definition and enforcement of standards, interface profiles, and Implementation guidance.
5. Information Security – VA shall provide a Secure Network and IT environment for collaborative sharing of information assets (information, services, etc.) with Veterans and other partners, including (among others) federal agencies, third-party service providers, academia, researchers, and businesses.
6. Enterprise Services – VA solutions shall use enterprise-wide standards, services, and approaches to deliver seamless capabilities to Veterans, facilitate IT consolidations through reuse, and simplify the use of Veteran functions.

### 1.2.2 VA EA Purpose

The VA EA details VA's full operations. As such, it includes both business and technical layers. The business layer depicts the functional operations of VA's Administrations and corporate business services. Enterprise architecture for the business layer is model-based, depicting the functions and services provided across the Department and their linkages and relationships to VA strategies, initiatives, and the IT applications that service them. A heavy emphasis on information flows across capabilities and services is embedded across all enterprise architecture supporting business capabilities. Figure 1-1 shows the VA EA.

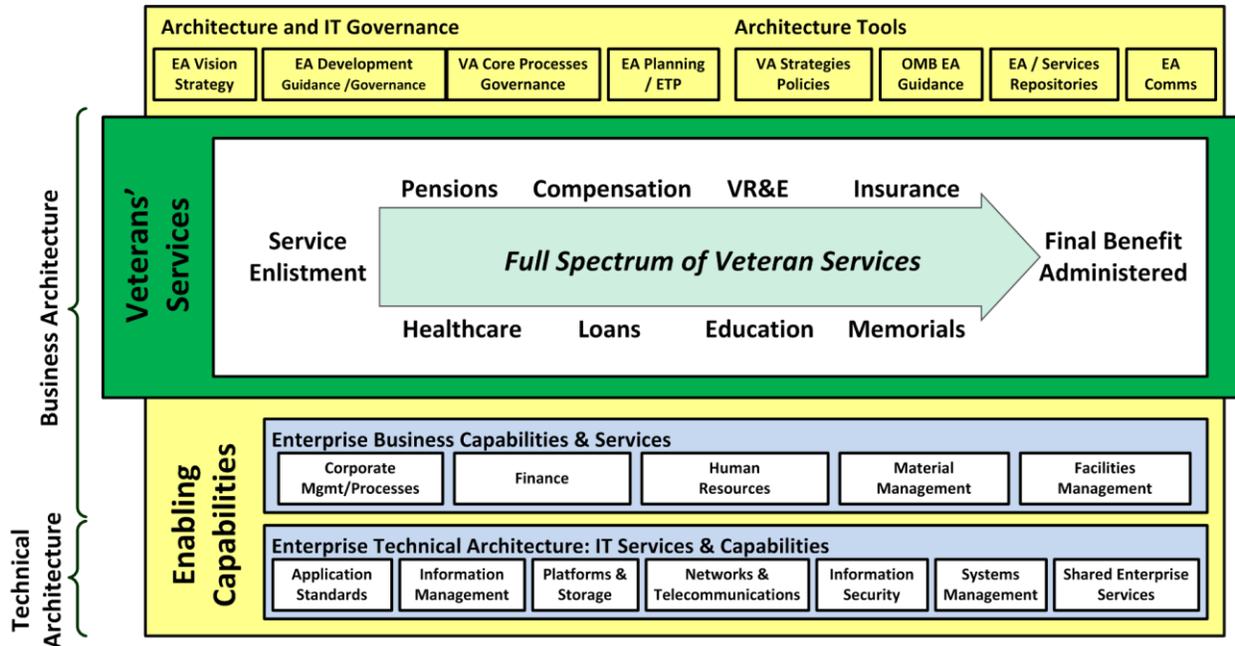


Figure 1-1: VA EA

### 1.2.3 Enterprise Architecture: Technical Layer

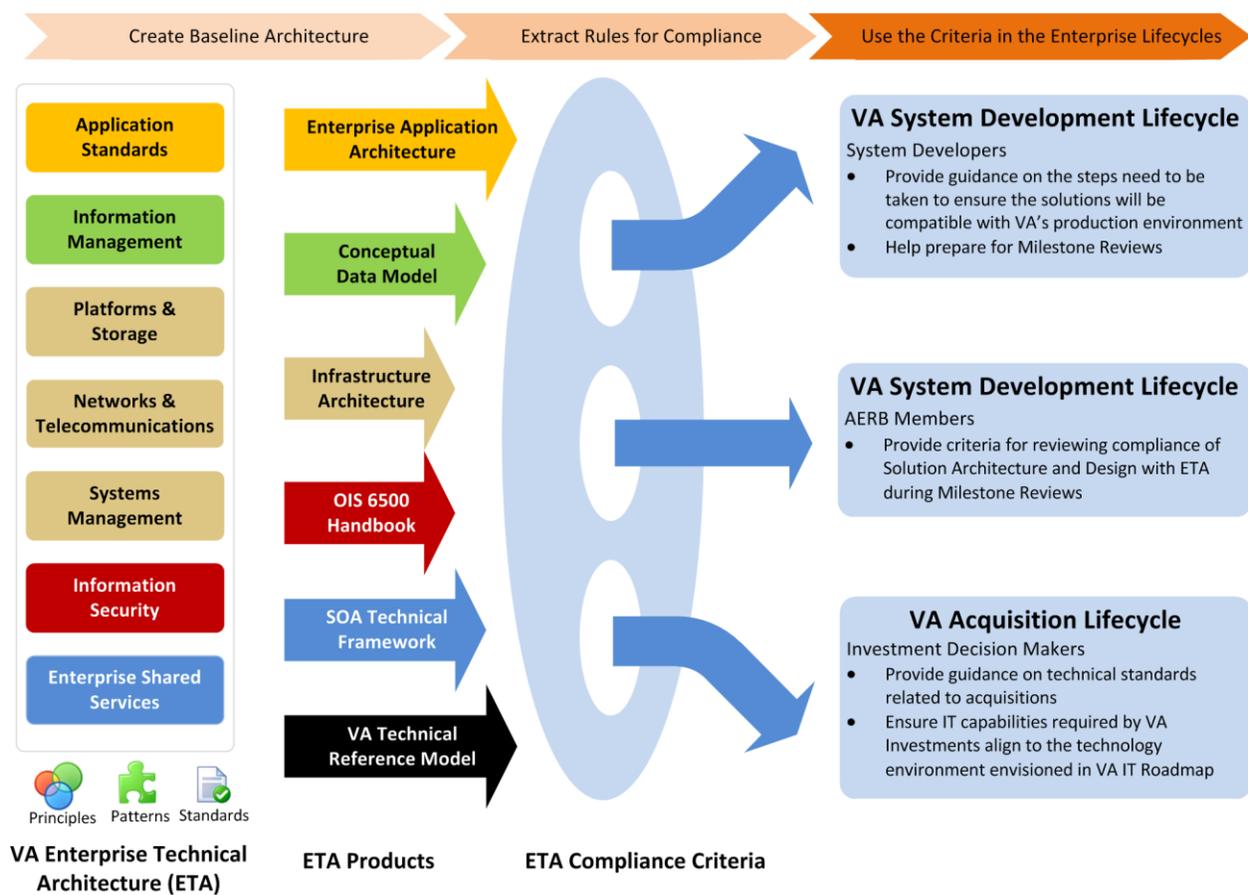
The enterprise architecture for the technical layer of the VA EA, or the VA ETA, is largely based on rules and standards. These rules and standards cover a wide range of topics, including use of VA's infrastructure (including networks, platforms, and data storage), information security standards, and standards for application design. These rules are influenced by both today's needs and an understanding of where and how VA needs to evolve its technology future as described in the VA Enterprise Technology Strategic Plan (ETSP).

Over the last year, VA's Office of Information & Technology (OI&T) has developed a variety of policies and architecture products to document these necessary rules and standards of the ETA. Many of these documents have been formally published; several (noted as "Pending") are currently going through the Department's coordination process. These documents, which can be found on the VA EA Intranet along with other VA EA products, include the following:

1. VA Enterprise Target Application Architecture v1.0, June 2012, Office of Product Development (PD)
2. VA Service-Oriented Architecture (SOA) Layer Implementation Guide v0.1, January 2012, Office of Product Development (PD)
3. OI&T Infrastructure Architecture V2.0, Service Delivery and Engineering (SDE)
4. VA Enterprise Architecture Vision and Strategy, Office of Architecture, Strategy, and Design (ASD)
5. [VA Policy 6500, Handbook 6500, and other 6500 appendices](#)
6. [VA Technical Reference Model \(TRM\), ASD](#)

7. VA Enterprise Technology Strategic Plan (ETSP), Fiscal Year 2017–2021, ASD
8. Enterprise Shared Services (ESS) Reference Documentation
9. Enterprise Design Patterns, ASD<sup>1</sup>

These documents collectively contain more than 2,000 pages of rules, standards, and configuration information that are applicable to IT resources within VA. The full breadth of this information represents a huge challenge to both developers trying to understand exact requirements and investment decision-makers and program evaluators trying to determine if solutions are being designed and constructed appropriately, with the proper eye for both network interoperability and use of enterprise approaches and capabilities. Thus, the need for this compliance criteria document arose. Figure 1-2 depicts how the ETA rules are derived and envisioned for use in enterprise lifecycles for ensuring compliance.



**Figure 1-2: VA ETA Compliance Criteria**

<sup>1</sup> Enterprise Design Patterns, developed by the ASD Office of Technology Strategies (TS), are documents that provide a generalized, vendor-agnostic framework to guide all VA IT programs to develop standardized solutions in accordance with the VA Enterprise Technical Architecture (ETA). These documents will aid programs in developing solutions that also align with the ETSP. The ETSP provides the goals and objectives for implementing the enterprise’s long-term strategic technical vision, leveraging best-of-breed technologies to maximize the effectiveness, efficiency, and security of VA’s IT assets. Use of VA Enterprise Design Patterns is mandatory based on [VA Directive 6551](#), [VA Enterprise Design Patterns](#), dated March 17, 2016.

## 1.3 Scope

This document has been crafted as a direct response to the need for stakeholders to be able to easily navigate the full array of ETA rules and standards detailed in the documents listed above and to ask (and answer) the questions necessary to gauge alignment of solutions with this collective guidance.

The VA EA team reviewed the full array of ETA documentation and developed an initial set of questions, which, if answered “YES,” will ensure compliance and alignment with the vast majority (more than 90 percent) of all ETA rules and standards. The EA team worked closely with the owners of each related ETA document to ensure that the equities of their individual rule sets were adequately covered.

The convention of “Can you answer ‘YES?’” to each of these questions was used throughout. It is intended that, where a “YES” answer is not possible, a program or investment may have to request a waiver from the Architecture and Engineering Review Board (AERB) to move forward.

Waivers granted are often conditional on a program or investment having a plan (and budget) in place to achieve the necessary “YES” answer at a defined and agreed-on future date.

The VA EA global principles are used as an organizing framework under which these rules are binned and categorized. As these represent core values and principles that underlie the entire VA EA, it was determined that aligning questions to them would serve as a check to ensure coverage of all VA enterprise equities. For each question starting in Section 2.1.1: Veteran-Centric Solutions, context is provided along with a reference to specific places in the underlying ETA documents where additional detail can be found. (This detail is often needed, particularly by developers, to understand the precise configurations and/or criteria applicable in a given situation.)

These questions were written to be applicable throughout the lifecycle of a program or investment. It is fully recognized that the meaning of a specific question may vary based on where in the lifecycle a program or investment is. To account for this, each question provides additional context as to how it can and should be applied at each Project Management Accountability System (PMAS) milestone (M0 through M3), including how one may use existing documentation to demonstrate a “YES” answer. As of today, only PMAS milestones are documented. As EA compliance is extended to other lifecycle processes, this guidance will be revised to reflect what compliance and alignment mean at these additional stages.

To assist program integrated project teams (IPT) with VA EA compliance, a set of frequently asked questions (FAQ) has been developed and is attached as an appendix (to this document). The focus of these FAQs is to assist program IPTs on how to use ETA compliance criteria in ensuring alignment of VA programs, projects, initiatives, or investments with the technical layer of the VA EA.

### 1.3.1 Relationship to Other Related Processes

This document is not intended to layer an additional requirement on developers or system maintainers above and beyond what is required by other processes, but rather to help draw focus

and organize critical points in those processes. It should serve not only as a compliance checklist, but also as a navigation tool to ETA, PMAS, Operational Analysis (OA), and other requirements. The use of the ETA Compliance Criteria by PMAS project teams and the AERB governance process is a well-recognized and mature review mechanism. However, these same criteria have not been well applied to system-level maintenance and sustainment lifecycle phases.

The EA team recognizes that current VA software lifecycle processes are not fully integrated, and state transitions often result in duplicative work for project and systems teams. In addition, gauging the best way to integrate these criteria into the process is difficult until they are actually being used. As the OA process and other system-level reviews across VA mature, the ETA content and related processes will also evolve. The teams will assess and continuously update the Compliance Criteria based on feedback provided during ongoing implementation of these criteria in oversight reviews.

### 1.3.2 Solution Types

It is recognized that not all compliance questions are applicable to every solution being developed. For example, most of the rules related to application architecture may not be applicable to a solution that involves infrastructure-level changes only. To assist the IPTs in identifying the criteria applicable to them, a set of commonly developed solution types has been identified; these are listed in Table 1-1.

**Table 1-1: Solution Types**

Sl. No	Solution Type	OI&T Pillar/Working Group	
1	Software Solutions	PD SDE: COTS only	Office of Information Security (OIS), SDE, ASD
2	Infrastructure Interoperability	SDE	
3	ESS	ESS WG	

These solution types should not be considered mutually exclusive. For example, although a software solution may not also be considered an infrastructure solution, it will still impact the infrastructure and must be interoperable with it. As such, the Infrastructure Interoperability questions still apply. When completing the ETA Compliance Checklist, the IPT must ensure that all IPT Compliance Assertions are completed and that any non-applicable criteria are marked as N/A with corresponding comments.

## 1.4 Purpose

This document serves as an entry point into the comprehensive architecture documentation developed by OI&T to describe how its IT environment must be designed and configured to do the following:

- Ensure interoperability of solutions
- Transition IT capabilities to the technology environment envisioned in the VA ETSP

The criteria contained herein will be assessed in alignment with milestone review processes that solutions must pass. Application developers should use this document to ensure that solutions they develop are in alignment with enterprise-wide technical guidance and help prepare for mandatory milestone reviews. VA investment decision-makers can use this guidance to better gauge the alignment of solutions being evaluated with VA's enterprise capability and technology environment.

All VA solutions and investments are required to comply with the business and technical layers of the VA EA. Note that the ETA represents only the technical layer of VA EA; therefore, compliance and/or alignment with the criteria in this document does not represent full VA EA compliance. Although this document simplifies compliance with the technical layer that is required by all solutions and investments, business architecture compliance is defined by the relevant VA Administration or Corporate Staff Office.

## 1.5 Document Conventions

To keep the compliance criteria generic for all applicable lifecycles (i.e., Acquisition versus System Development), this document uses the term "Solution" in the compliance questions to refer to the effort (investment, project, application, or program) that is being measured for compliance.

This document follows the conventions that conform to RFC2119.<sup>2</sup> The specific architecture guidelines described in this document fall into two categories:

- **Mandatory Compliance** – These guidelines are identified by the key words "MUST," "MUST NOT," "REQUIRED," "SHALL," and "SHALL NOT." Exceptions require a waiver and a transition plan.
- **Recommended Use** – These guidelines are identified by the key words "SHOULD," "RECOMMENDED," "SHOULD NOT," and "NOT RECOMMENDED." These guidelines describe a preferred alternative as judged by VA. Deviations should be limited and justified by the circumstances.

## 1.6 Audience

This document is primarily written for the following audience to ensure alignment with EA rules and standards:

- VA Project Managers (PM) and Technical Stewards (Solution Architects, Developers, and Engineers) who will be architecting, designing, and developing the VA Solutions
- VA investment decision-makers, AERB members, and others reviewing solutions for compliance and alignment
- VA System-level maintainers, Operations Managers, and Federal Information Security Management Act (FISMA) Systems Owners responsible for the day-to-day operations and maintenance of VA IT business systems

---

<sup>2</sup> [Internet Engineering Task Force \(IETF\) Standard.](#)

## 2 Compliance Criteria

### 2.1 Mission Alignment

*VA information, systems, and processes shall be conceived, designed, operated, and managed to address the Veteran-centric mission needs of the Department.*

#### 2.1.1 Veteran-Centric Solutions

##### Criterion

Solution should support Veteran-centric mission needs and/or capabilities.

##### Rationale

VA Solutions should enable coordination and integration across programs and organizations, measuring performance by the ultimate outcome for the Veteran, and putting the Veteran in control of how, when, and where they want to be served. The solution needs to identify the primary mission capability being served.

The VA has documented its mission needs and priorities in a set of integrated strategic goals, strategic objectives, and performance goals in the VA FY 2014–2020 Strategic Plan. The solution must identify the primary mission capability being served with linkage to the strategic direction contained in the VA FY 2014–2020 Strategic Plan.

This Compliance Criteria document is specific to Technology (not Business) compliance with the VA EA. IT professionals, however, should never lose sight of their ultimate mission.

##### Sources

- VA EA Vision and Strategy, Section 1.3: Guiding Principles, pp. 5–6
- VA FY 2014-2020 Strategic Plan, Chapter VI: VA FY 2014-2020 Strategic Goals, pp. 21–37

**Solution Development Compliance**

PMAS Milestone	Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
0-3	Does the business need support integrated strategic goals and objectives defined in VA FY 2014–2020 Strategic Plan? Does the solution support Veteran-centric mission needs and/or capabilities?	Project Charter: Business Need

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Does this system continue to meet business and customer needs and contribute to meeting strategic goals and objectives defined in VA FY 2014–2020 Strategic Plan?	VA FY 2014–2020 Strategic Plan

## 2.1.2 Business Architecture

### Criterion

Solution should be compliant with appropriate business architecture.

### Rationale

The solution needs to identify high-level Business Functions or Business Processes it supports and illustrate that the business owner(s) have vetted the business processes to ensure To-Be Business Process Flows are up-to-date with the solution's business objectives.

ETA compliance is only part of VA EA compliance. In addition to Technical (ETA) compliance, all VA IT solutions are also subject to Business EA compliance.

### Sources

- VA EA Vision and Strategy, Section 2: Strategic Goals/Purposes, pp. 7-10

### Solution Development Compliance

PMAS Milestone	Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
0-3	Has the leaf-level business subfunction of the VA EA Business Architecture that the solution aligns to been identified?	Specifics of Business Architecture compliance is beyond the scope of this document.

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Have the leaf-level business subfunctions of the VA EA Business Architecture supported by this system been captured? If captured, does this system continue to support the documented business functions?	VA EA Business Reference Model (BRM) VASI

### 2.1.3 Mission Criticality

#### Criterion

All VA IT Systems shall be assigned application levels of Mission Criticality.

#### Rationale

Identification of mission criticality of Systems based on Business Impact Analysis (BIA) is important for business continuity planning to assess potential impacts of business disruptions resulting from uncontrolled, non-specific events in meeting VA's mission needs.

#### Sources

- OIS Information Systems Continuity Planning (ISCP)

#### Solution Development Compliance

- Not applicable

#### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Has BIA been conducted for this system and an applicable system criticality level assigned?	VASI

## 2.2 Data Visibility and Accessibility

*VA Application, Service, and Data Assets shall be visible, accessible, available, understandable, and trusted to all authorized users (including unanticipated users).*

### 2.2.1 N-Tier Architecture

#### Criterion

- Application shall be partitioned into logical layers (i.e., presentation layer, business logic layer, and data access layer) with each layer containing functionality specifically related to that layer.
- The application layers shall use interface components to provide loose coupling between layers.

#### Rationale

The layered architecture reflects the well-established software engineering principle of separation of concerns. Application code shall be functionally organized into layers, and such layering shall be reflected in the dependency structure of the application code. For example, the Presentation Layer<sup>3</sup> should depend on the Business Logic layer,<sup>4</sup> but business logic code must not depend on presentation code. Furthermore, application layers shall be determined independent of the runtime infrastructure. The layered structure facilitates a logical way to divide the application development tasks.

#### Sources

- VA Enterprise Target Application Architecture v1.0, Section 4: Application Architecture Layers, p. 49
- Enterprise Application Design Patterns: VistA Evolution

---

<sup>3</sup> See Appendix C: References.

<sup>4</sup> Ibid.

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the application design functionally organized into Presentation, Business Logic, and Data Access Layers? Does the application design ensure that secure communication between the layers happens through loosely coupled interface components?	System Design Document (SDD): Conceptual Application Design
<b>2</b>	Has a VA-recommended application framework, as identified by the VA Enterprise Technology Strategic Plan (ETSP), been selected for the application development?	SDD: Software Detailed Design
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are the source code of the VA custom-developed application components and the configuration baselines of this system available? If available, have they been captured in a Version Control Repository?	Version Control Repository

## 2.2.2 Data Independence

### Criterion

Application logic shall be fully decoupled from the data that it manages or processes.

### Rationale

There shall be a complete separation between business processing and data access and delivery services, such that the business logic has no visibility into the physical structure of the data. Any data stored locally at the application level presents barriers to information sharing across the enterprise and should not be permitted.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 5.1.4.5: Separation of Business Logic and Data Logic, p. 99
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Does the application logic access and manage data through a Data Access Layer <sup>5</sup> or established services instead of directly accessing the database?	SDD: Conceptual Application Design
2	Is the application logic free from the database implementation details (e.g., data base URLs, internal file formats, schema information)?	SDD: Software Detailed Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is the application logic of the VA custom-developed software of this system free from the database implementation details (e.g., data base URLs, internal file formats, schema information)?	Version Control Repository

<sup>5</sup> See Appendix B: Terms and Definitions.

## 2.2.3 Common Look and Feel

### Criterion

Application user interface (UI) shall follow the enterprise common UI templates and style guidelines.

### Rationale

The solution should provide UIs that have a consistent “look and feel,” following enterprise templates and style guidelines.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 4.1.2.1.2: End-User Interface, p. 51

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Not applicable	
2	Have the applicable enterprise conventions and standards (enterprise templates and style guidelines) been applied in the design of the UI(s)?	SDD: Overview of the Technical Requirements
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable until enterprise conventions and standards are published.

## 2.2.4 Data Persistence

### Criterion

Data used by the solution stored on enterprise servers shall be stored without being saved on end-user devices or user workstations.

### Rationale

Using enterprise resources to store permanent data lessens the burden on an application to be a proper data custodian (including concerns about security, privacy, etc.). It also promotes consistency in how data custodianship is executed and isolates changes to common services when policies are modified.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.1: OI&T Architecture Principles, p. 21
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Has required analysis been performed to ensure the permanent storage of sensitive data (PII/PHI) will not happen on the end-user devices?	SDD: Conceptual Application Design
2	Is the transient application data stored temporarily on end-user devices (through mechanisms such as cookies) purged periodically or when the user session expires?  Is the relational/non-relational data used by the solution stored on enterprise servers?	SDD: Data Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are procedures in place to ensure the permanent storage of sensitive data (PII/PHI) will not happen on the end-user devices of this system?	N/A

## 2.2.5 Test-Driven Development

### Criterion

Unit tests shall be developed for all application functions and publicly exposed methods.

### Rationale

Any major application component is a potential candidate for use as an enterprise service. Components should be tested not only in the context of the local application, but also as a stand-alone capability. This facilitates reuse and makes reliable enterprise components available. Increased testability arises from having well-defined, layered interfaces, and the ability to switch between different implementations of the layer interfaces. Separate architectural patterns allow building mock objects that mimic the behavior of concrete objects such as the Model, Controller, or View during testing.

### Sources

- VA Enterprise Target Application Architecture: SOA Layer Implementation Guide, Section 3.1: Architecture Considerations, p. 32

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Does the solution leverage automated unit testing (i.e., <a href="#">JUnit</a> for Java-based testing or <a href="#">Nunit</a> for .Net-based testing)?	SDD: Conceptual Application Design
2	Have unit tests been defined for all solution functions and publicly exposed methods?  Have the designed unit tests been automated for execution during the build and deployment process?	SDD: Software Detailed Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.2.6 Exception Handling

### Criterion

Procedures shall be in place for communicating and resolving unhandled exceptions.

### Rationale

Systems and shared services may encounter usage that was unexpected in its original development. It is not possible to anticipate all potential causes of failure. Production operation processes must be designed to properly react to and resolve unexpected system errors, which includes communicating the status of system errors to system users.

### Sources

- VA Enterprise Target Application Architecture: SOA Layer Implementation Guide, Section 3.1: Architecture Considerations, p. 32

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Is there a strategy for processing unhandled exceptions and associated security considerations? Is there a strategy for communicating unhandled exceptions to system users?	Project Management Plan (PMP): Testing Plan
1	Has the development of a Production Operations Manual, which includes error handling, been identified and properly resourced in the IPT Integrated Master Schedule (IMS)?	Production Operations Manual
2	Has the IPT completed development of the Production Operations Manual? Have the error handling procedures documented in the Production Operations Manual been validated through a quality assurance (QA) and/or testing process?	SDD: Software Detailed Design Production Operations Manual
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is the Production Operations Manual available and up-to-date for this system? If so, have the exception handling procedures been documented in Production Operations Manual?	Production Operations Manual

## 2.2.7 Scalability

### Criterion

- Application shall be designed to scale out (rather than scale up) and designed to operate on a series of loosely coupled commodity platforms.
- Application shall scale-out without requiring code changes.

### Rationale

The solution needs to be designed to scale out (i.e., run on larger numbers of small systems). To scale horizontally (or scale out) means to add more nodes to a system, such as adding new virtual machines (VM) spread across physical server farms or adding a new computer to a distributed software application. To scale vertically (or scale up) means to add resources to a single node in a system, typically involving the addition of Central Processing Units (CPU) or memory to a single server or computer.

### Sources

- OI&T Infrastructure Architecture v2.0, System Availability/Performance: Scalability, p. 9
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Is the application designed to scale out and operate on a series of loosely-coupled commodity platforms? [Applicability: Infrastructure Interoperability]  Can the application scale-out without requiring code changes? [Applicability: Software Solutions]	SDD: Conceptual Application Design  SDD: Hardware Detailed Design
2	Not applicable	SDD: Software Detailed Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are the application components of this system designed to scale out and to operate on a series of loosely-coupled commodity platforms?	N/A

## 2.2.8 Stateless Business Logic

### Criterion

Application business logic shall be “stateless” (i.e., user session information is not stored within the business logic).

### Rationale

The solution should not store the user session information within the business logic to ensure the same business logic is exposed for user interaction (through presentation layer) and system interaction (through integration layer using enterprise messaging).

### Sources

- Enterprise Application Design Patterns: Vista Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Has required analysis been performed to ensure user session information is not stored within the business logic?	SDD: Conceptual Application Design
2	Is the application business logic “stateless” (i.e., user session information is not stored within the business logic)?	SDD: Software Detailed Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.2.9 Accessibility Requirements

### Criterion

Solution shall comply with Electronic and Information Technology Accessibility (EITA) Standards (specifically accessibility requirements in accordance with Section 508 of the Rehabilitation Act of 1998, as amended, 29 USC 794(d)).

### Rationale

The solution shall meet accessibility requirements.

### Sources

- [Section508.gov](#)
- [VA Section 508 Standards Checklist](#)
- VA Enterprise Target Application Architecture v1.0, Section 4.1.2.1.2: End-User Interface, p. 51

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Does the solution comply with Section 508 of the Rehabilitation Act of 1998, as amended, 29 USC 794(d)?	SDD: Overview of Significant Functional Requirements PMP: Testing Plan
<b>2</b>	Does the solution comply with required EITA accessibility standards?	SDD: Overview of the Technical Requirements
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Does this system comply with Section 508 of the Rehabilitation Act of 1998, as amended, 29 USC 794(d)?	VASI

## 2.3 Data Interoperability

*VA Information shall be made interoperable through data standardization, including the identification, designation, and utilization of authoritative sources.*

### 2.3.1 Data Standards

#### Criterion

Solution shall adhere to all applicable data standards published by VA Enterprise Data Architecture.

#### Rationale

The use of common data standards (e.g., National Information Exchange Model [NIEM], HL7, Logical Observation Identifiers, Names, and Codes [LOINC], Systematized Nomenclature of Medicine [SNOMED], Veteran Information Model [VIM], and Healthcare Information Technology Standards Panel [HITSP]) will foster consistently defined and formatted data elements and sets of data values, and provide enterprise access to more meaningful data.

#### Sources

- VA EA Vision and Strategy, Section 2.1: Principle #5 – Seamless Capabilities
- Enterprise Application Design Patterns: VistA Evolution

#### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Have the required analysis and conceptual design been performed to identify the applicable Data Standards?	SDD: Conceptual Data Design
1	Not applicable	
2	Have the data elements and values been defined and formatted in accordance with the VA EA Data Standards?	SDD: Data Design
3	Not applicable	

#### IT Operational Analysis/System Sustainment

- Not applicable

## 2.3.2 Authoritative Information Sources

### Criterion

Authoritative information sources (including user identity data) shall be identified and leveraged for data retrieval and manipulation.

### Rationale

A single instance of each data element (attribute in an entity) needs to be designated as “Authoritative” and should serve as a unique and unambiguous source of data to be shared operationally across all systems in the enterprise with the approval of the responsible data stewards.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.2: Data Management Principles, p. 32
- Interoperability and Data Sharing Design Patterns: Data as a Service
- IT Service Management (ITSM) Design Patterns: ITSM Increment 1
- [VA Directive 6518](#) – Enterprise Information Management (EIM)

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Has required analysis been performed to identify authoritative information sources?	
<b>1</b>	Not applicable	
<b>2</b>	Have authoritative information sources been leveraged for data retrieval and manipulation wherever authoritative sources have been identified by the enterprise?	SDD: Data Design
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

### 2.3.3 Enterprise Logical Data Model

#### Criterion

Information captured by the proposed solution shall be syntactically and semantically harmonized with the VA Enterprise Logical Data Model (ELDM).

#### Rationale

Promote usage of a VA Enterprise Logical Data Model that will identify each “enterprise” entity that contains at least one attribute (data element) that may be of use outside the system in which it is created or stored. Any data that enters or leaves a system is considered data used outside that system.

The data exchange between systems needs to be based on harmonized, standard definitions of all entities and attributes as defined in the Enterprise Logical Data Model. The solution must ensure conversion of its internal data definitions to the enterprise definitions for communication with enterprise services or other systems with the approval of responsible data stewards.

#### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.2: Data Management Principles, p. 30; Section 4.6: Layer 6 – Data Layer, p. 81; Section 4.5.3.1: Information Integration, p. 70; Section 5.6.4: Data Harmonization, p. 108

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Has the required analysis been performed to identify alignment with the VA EA ELDM?	
<b>1</b>	Not applicable	
<b>2</b>	<p>Has alignment with the VA EA ELDM been reviewed and approved by the responsible data stewards?</p> <p>Have translations between enterprise data and internal system data been reviewed and approved by the responsible functional and technical enterprise data stewards for both data production and consumption?</p> <p>Has information captured by the proposed solution been syntactically and semantically harmonized with the VA EA ELDM?</p> <p>Has the VA EA ELDM been updated with the new enterprise entities introduced by the solution?</p>	SDD: Data Design VA EA ELDM
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.3.4 Local Copies of Authoritative Information Sources

### Criterion

Solution shall function optimally without using local copies of authoritative information source instances.

### Rationale

In general, the use of local copies of the authoritative instance is not recommended. If performance requirements of the solution dictate usage of local copies, permission of the responsible data steward must be obtained for such use. In addition, any update to such a copy or the creation of new records in such a copy shall be considered to be effective only unless and until the authoritative instance has been successfully updated.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.2: Data Management Principles, p. 33; Section 5.1.4.4: Single Authoritative Instance of all Data, p. 117
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Not applicable	
2	<p>Has the logical data design identified the need for using local copies of authoritative data instances?</p> <p>Are security controls in place for accessing authoritative data?</p> <p>Has approval/authorization been granted to store local copies of authoritative data instances?</p> <p>Are change management procedures in place to ensure that no authorized data modifications are permitted on copied authoritative data, unless performed on the authoritative sources first?</p>	SDD: Data Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable until authoritative sources have been identified

### 2.3.5 VA Data Inventory

#### Criterion

Data gathered and generated by this system shall have its definitions registered in the VA Data Inventory (VADI).

#### Rationale

Metadata registries (MDR) store the data schemas/domain vocabularies and manage the semantics of data independent of the subject matter area. The MDR should act as a central source of authoritative schemas or vocabularies for use within VA. The solution should ensure that the metadata related to the information it receives and disseminates is stored in the VA MDR to promote harmonization, standardization, use, reuse, and interchange.

#### Sources

- VA Enterprise Target Application Architecture v1.0, Section 4.5.3.2: Enterprise Service Bus (ESB) Functions, p. 72

#### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Have the related authoritative data schemas/domain vocabularies in the VADI been identified?	SDD: Conceptual Data Design
2	Have the physical data schemas generated or maintained by this system been registered in the VADI?	SDD: Data Design
3	Not applicable	

#### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Have the physical data schemas related to this system been registered in the VADI?	VADI

## 2.4 Infrastructure Interoperability

*VA IT Infrastructure shall be made interoperable through definition and enforcement of standards, interface profiles, and Implementation guidance.*

### 2.4.1 Cloud First

#### Criterion

Solution shall adhere to VA Cloud First Policy.

#### Rationale

Promote usage of secure cloud services across VA to provide highly reliable, innovative services quickly despite resource constraints. Cloud computing<sup>6</sup> has the potential to play a major part in improving VA service delivery.

#### Sources

- [VA Directive 6517, Cloud First Policy](#)

---

<sup>6</sup> Ibid.

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	<p>Does the project plan on performing required analysis to identify the pertinent cloud delivery model (i.e., Infrastructure as a Service [IaaS], Platform as a Service [PaaS], or Software as a Service [SaaS])?</p> <p>Has the required analysis been performed to leverage Enterprise Identity and Access Management (IAM) Capabilities for the solution's authentication, authorization, and auditing needs?</p>	<p>Project Charter: Project Dependencies</p> <p>SDD: Application Locations</p>
<b>1</b>	<p>Has the required analysis been performed to identify the pertinent cloud delivery model (i.e., IaaS, PaaS, or SaaS)?</p> <p>If so, have relevant policies and procedures been established to ensure delivery of effective and secure cloud computing services to support VA's infrastructure, information systems, and data repositories?</p>	SDD: System Architecture
<b>2</b>	<p>Have the security control requirements been evaluated and tested following VA Network and Security Operations Center (NSOC) procedures?</p> <p>Have recommendations for continuous monitoring, implementation, and maintenance of cloud services at VA Network and NSOC been provided?</p>	<p>Operational Acceptance Plan (OAP): C&amp;A SMART Status</p> <p>SDD: Security and Privacy</p>
<b>3</b>	<p>Does the VA cloud service meet Federal Risk and Authorization Management Program (FedRAMP) and National Institute of Standards and Technology (NIST) requirements before adoption of the service to ensure compliance and adherence with VA regulatory authority and NIST standards?</p>	OAP: C&A SMART Status

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
<p>Has the "Cloud Readiness" of this system been assessed and the applicable Cloud Service Model, Deployment Model, or the exception if deemed not ready for cloud been documented?</p>	<p>Cloud guidance for Product Planning</p>

## 2.4.2 Standard Operating System Images

### Criterion

End-user devices and servers shall use standard system images, as published in the current VA Infrastructure Architecture.

### Rationale

Reduce complexity by standardizing Platform<sup>7</sup> that include hardware, operating system (OS), middleware, databases, and supporting system software. Ensure the solution conforms to the VA Standard OS.

### Sources

- OI&T Infrastructure Architecture v2.0, Platforms, p. 8

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Are end-user devices and servers used by the solution configured using the standard system images published in the current OI&T Infrastructure Architecture?	Requirements Specification Document (RSD): Applicable Standards SDD: Software Architecture OAP: Physical Support Requirements, Architecture/Dependencies
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are end-user devices and servers used by this system configured using the standard OSs published in the current OI&T Infrastructure Architecture?	OI&T Infrastructure Architecture

<sup>7</sup> Ibid.

## 2.4.3 Standard Databases

### Criterion

Solution shall use Relational Databases and Object-Oriented Databases, as published in the current VA Infrastructure Architecture.

### Rationale

Reduce complexity by standardizing platforms that include hardware, OS, middleware, databases, and supporting system software. Ensure the solution conforms to the VA Standard Databases.

### Sources

- OI&T Infrastructure Architecture v2.0, VistA Platforms, p. 10; Database Products, p. 14.
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Are the Relational Databases and Object-Oriented Databases published in the current OI&T Infrastructure Architecture sufficient to meet solution needs?	SDD: Database Information
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Does this system use all standard Database Management Systems published in the current OI&T Infrastructure Architecture?	OI&T Infrastructure Architecture

## 2.4.4 Virtualization

### Criterion

Solution shall be designed for operation in the standard OI&T-defined virtual environments.

### Rationale

The solution shall be independent of the underlying physical infrastructure and leverage virtualized environments that provide flexibility of system development and stability for the production system by incorporating cloud architecture. Hardware-specific applications limit the hosting options and, thus, potentially limit scalability and opportunities for reusing existing hardware resources. Virtualization provides the ability to run more workloads and provide higher utilization and capitalization on a single server and facilitates VM mobility without downtime.

### Sources

- Server Virtualize First Policy (VAIQ 7266972), dated 8/27/2012

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the solution designed to run in virtual environments without the need for modification?	SDD: Conceptual Infrastructure Design
<b>2</b>	Is the current solution-hosting infrastructure based on the standard OI&T-defined virtual environments?	SDD: Detailed Design
<b>3</b>	Is the system hosted by the standard OI&T Virtual Environment?	OAP

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is the system capable of running in virtual environments without a need for modification?	

## 2.4.5 Infrastructure Capacity

### Criterion

Capacity analysis shall be performed and detailed capacity requirements shall be based on workload analysis, simulated workload benchmark tests, or application performance models.

### Rationale

Good understanding of infrastructure capacity (throughput and processing) helps determine the infrastructure’s ability to meet future workload changes and plan for future growth.

### Sources

- OI&T Infrastructure Architecture v2.0. Background. p. 6
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Have infrastructure capacity requirements been assessed and has an infrastructure impact analysis been performed?	RSD: Performance Specifications SDD: System Criticality and High Availability SDD: Overview of Functional Workload/ Performance Requirements
2	Have appropriate load testing and impact analysis been performed to leverage the VA infrastructure to host the solution?  Have performance baselines been established during load testing that may be used for comparison when future functionality changes or enhancements are made?	OAP: Physical Support Requirements OAP: Service Level Requirements OAP: Architecture/ Dependencies
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Have Service Level Agreements (SLA) been established for this system? If so, has this system been provisioned to meet the established SLAs?	

## 2.4.6 Storage

### Criterion

Storage capacity requirements shall be based on detailed capacity analysis and/or models.

### Rationale

Storage requirements help to drive the infrastructure need for storage capacity. This further supports the current and future needs of storage within the infrastructure.

### Sources

- OI&T Infrastructure Architecture v2.0, Storage Capacity, p. 11

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Are storage capacity requirements based on detailed capacity analysis and/or models?	SDD: Data Design SDD: Hardware Detailed Design
<b>2</b>	Is the solution storage infrastructure based on the standard OI&T storage provisioning model?	OAP: Physical Support Requirements OAP: Service Level Requirements OAP: Architecture/Dependencies
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.4.7 Network Configurations

### Criterion

Solution shall be designed to operate within the current VA Local Area Network (LAN) and Wide Area Network (WAN) configurations.

### Rationale

The network should be able to support connectivity (latency and bandwidth) and security requirements of the solution in establishing internal and external communications with VA Data Centers, VA Medical Centers (VAMC), Community-Based Outpatient Clinics (CBOC), and VA facilities. In addition, remote management of the solution must be incorporated into the overall system design.

### Sources

- OI&T Infrastructure Architecture v2.0, Network, p. 12

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Is the solution designed to operate within the current VA LAN and WAN network configurations?	SDD: Network Detailed Design SDD: External System Interface Design
2	Have the current VA LAN and WAN configurations been evaluated against the solution's planned network traffic profile?  Have the effects of the solution's estimated additional network traffic been considered against current VA LAN and WAN bandwidth capabilities?	OAP: Physical Support Requirements OAP: Service Level Requirements
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.4.8 Transmission Control Protocol/Internet Protocol v6

### Criterion

Solution shall be designed to support Transmission Control Protocol/Internet Protocol (TCP/IP) v6.

### Rationale

The solution should be IPv6 compliant. An IPv6-compliant product or system must be able to receive, process, and transmit or forward (as appropriate) IPv6 packets and should interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation.

### Sources

- OI&T Infrastructure Architecture v2.0, Network, p. 13
- “Adoption of IPv6 at VA” Memorandum, dated March 24, 2011
- “IPv6 Transition Guide,” dated January 11, 2013

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the solution designed to comply with VA’s guidance on IPv6 policy and guidelines as specified in the current OI&T Infrastructure Architecture? [Applicability: Infrastructure Interoperability]  Is the application code free of hard-coded IP addresses? [Applicability: Software Solutions]	SDD: Network Detailed Design SDD: External System Interface Design
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is this system assessed for compliance with VA’s guidance on IPv6 policy and guidelines as specified in the current OI&T Infrastructure Architecture?	OI&T Infrastructure Architecture

## 2.4.9 System Monitoring

### Criterion

Solution deployment environment must be able to meet the performance, downtime, and security monitoring requirements.

### Rationale

Ensure the solution is monitored vigilantly for performance and security. Continuous monitoring of operational workload and failure data across all infrastructure components is crucial to discovering issues and alerting operational personnel for remediation to prevent outages that impact end users.

Also, build health checks into the solution. Solution health checks will augment monitoring and provide a means for load balancers to redistribute traffic.

### Sources

- OI&T Infrastructure Architecture v2.0, Instrumentation/Monitoring Products, p. 16
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Does the deployment environment meet the performance, downtime, and security monitoring requirements of the solution?	RSD: Reliability Specifications SDD: Overview of System Criticality and High Availability Requirements SDD: System Criticality and High Availability
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is this system monitored end-to-end for performance and security?	OI&T SDE Configuration Database

## 2.4.10 Disaster Recovery

### Criterion

A disaster recovery (DR) strategy and plan, which includes multiple (physical) locations of critical infrastructure components (including data), must be developed.

### Rationale

DR comprises the process, policies, and procedures related to recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Proper DR requires several components to create an overall functional solution. Some technologies that may be leveraged for DR include storage replication, backups, point-in-time copies, and virtualization. Ensure critical data and application components are not collocated.

### Sources

- OI&T Infrastructure Architecture v2.0, System Availability, p. 9
- VA Enterprise DR Service Tiers Standard Version 1.0, dated 9/4/2012

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Has the applicable DR Service Tier been identified based on the business continuity requirements? Has a DR plan been developed and provisioned? Are critical infrastructure components (including Data) located at multiple (physical) locations?	RSD: Disaster Recovery Specification SDD: Overview of System Criticality and High Availability Requirements SDD: System Criticality and High Availability
<b>2</b>	Does the DR plan maximize use of OI&T infrastructure capabilities?	OAP: Physical Support Requirements OAP: Service Level Requirements
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Has BIA been performed for this system? If yes: Has the applicable DR Service Tier been identified based on the BIA and the associated Recovery Point Objective (RPO) and Recovery Time Objective (RTO) been documented for this system? Has a DR plan been developed and provisioned for this system?	OI&T SDE Configuration Management Database

## 2.4.11 Backup and Restore

### Criterion

Backup and restore Solution shall meet data recovery requirements (RPO and RTO).

### Rationale

Infrastructure users help to determine the amount or the period of data that needs to be backed up and the amount of data that needs to be restored. Recovery requirements help to determine the backup and restore capabilities.

### Sources

- OI&T Infrastructure Architecture v2.0, Storage Technologies, p. 11

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Will the backup and restore solution meet objective data recovery requirements (RPOs and RTOs)?	RSD: DR Specification SDD: Overview of System Criticality and High Availability Requirements SDD: System Criticality and High Availability
<b>2</b>	Does the backup and restore plan maximize use of OI&T infrastructure capabilities?  Does the security of data backups comply with VA requirements?	OAP: Physical Support Requirements  OAP: Service Level Requirements
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is there a backup and restore plan and a solution in place for this system?  Will the backup and restore solution meet objective data recovery requirements (RPOs and RTOs)?	OI&T SDE Configuration Management Database

## 2.4.12 Thin Client

### Criterion

Solution must be designed for a browser or “thin client”-based UI.

### Rationale

The use or implementation of standalone thick clients on the client tier is not permitted. An exception would be if a solution has special requirements such as the need for device integration where an applet (e.g., functionality) will not be sufficient; in such cases, a thick client may be considered in the architecture. The goal is to minimize the client footprint and target web-based client interfaces whenever possible. Acceptable [thin client](#)<sup>8</sup> technology is cited in the source. See the TRM for browser standards.

### Sources

- OI&T Infrastructure Architecture v2.0, Client, p. 13
- VA Enterprise Target Application Architecture v1.0, Section 2.1: OI&T Architecture Principles, p. 21

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the solution either browser or “thin client”-based? Has the required analysis been performed to leverage Enterprise IAM Capabilities for the solution's authentication, authorization, and auditing needs?	SDD: Conceptual Data Design
<b>2</b>	Is the UI designed with device- and browser-independent technologies such as HyperText Markup Language (HTML), Extensible HTML [XHTML], HTML5, Cascading Style Sheet (CSS), and JavaScript?	SDD: Software Detailed Design
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

---

<sup>8</sup> Ibid.

## 2.5 Information Security

*VA shall provide a Secure Network and IT environment for collaborative sharing of information assets (information, services, etc.) with Veterans and other partners, including (among others) federal agencies, third-party service providers, academia, researchers, and businesses.*

### 2.5.1 Security Regulations

#### Criterion

Solution design shall include all applicable Information Security rules.

#### Rationale

Ensure the solution adheres to and is in compliance with established federal laws and regulations as per the policy provided in VA Policy 6500, Handbook 6500, and other 6500 appendices.

#### Sources

- [Information Security Program – VA Directive and Handbook 6500](#), Section 3: Utilization of This Handbook and Appendices, p. 7
- ESS SOA Policy 238 (*Security tab*)
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Has the solution identified all potential information security and privacy requirements, risks, and vulnerabilities that will need to be addressed? Will this solution be included in another application’s C&A and privacy documentation?	RSD: Security Specifications SDD: Overview of the Security or Privacy Requirements SDD: Security and Privacy
<b>1</b>	Has the required security and privacy documentation addressing specific security requirements, applicable controls, potential vulnerabilities, and risks been developed and approved? Have all applicable Information Security rules been adhered to?	Risk Log RSD: Security Specifications SDD: Overview of the Security or Privacy Requirements SDD: Security and Privacy
<b>2</b>	Have the procedures for monitoring, assessing, and testing for security been documented? Has the solution passed the C&A?	OAP: C&A SMART Status
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is this system covered under an active Authority to Operate (ATO) issued by OIS? If so, has the system information been updated or validated in VASI to include correct ATO information?	OIS Governance Risk and Compliance (GRC) Risk Vision VASI

## 2.5.2 External Hosting

### Criterion

If hosted externally, solution must follow all guidelines for using commercial partners.

### Rationale

Ensure the solution follows the external hosting guidelines and VA security policy for using such hosted solutions.

### Sources

- OI&T Infrastructure Architecture v2.0, p. 4
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Do security requirements include information on the requirements for certification of the external site under NIST when VA data is exchanged, transmitted, or otherwise hosted on an external system?	OAP: C&A SMART Status OAP: Anomaly/Risk Summary
<b>1</b>	Have all guidelines for using commercial partners been communicated to the hosting provider? Have all guidelines for using commercial partners been followed?	OAP: C&A SMART Status OAP: Anomaly/Risk Summary
<b>2</b>	Do agreements for contracted information services include provisions for monitoring security control compliance? Are externally hosted VA sites registered with VA Web Operations (WebOps), which provides website and enterprise-based application hosting services for all VA facilities and programs, including the VA's primary internal (vaww.va.gov) and external (www.va.gov) sites?	OAP: C&A SMART Status OAP: Anomaly/Risk Summary
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
If this system is hosted externally, have all guidelines for using commercial partners been followed?	

### 2.5.3 Secure Access Paths

#### Criterion

Solution design shall follow established secure access paths for application and database access.

#### Rationale

Access Paths define the physical and logical access to a computer resource (application, data, or the underlying infrastructure) and provide the ability to use, change, or view such resource.

Ensure that only approved message paths will be used for application and data access. No direct user access is permitted to the internal databases and applications that bypass VA security infrastructure.

#### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Architecture Application Principles, p. 35
- [VA Handbook 6500](#) – External Business Partner Connections, p. 66
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Are established secure access paths followed for application and database access?	SDD: Security and Privacy
<b>2</b>	<p>Do access controls ensure that only authorized individuals gain access to information system resources, are assigned an appropriate level of privilege, and are individually accountable for their actions?</p> <p>Do moderate- and high-impact systems validate and ensure that the flow of information between endpoints is appropriate, documented, and approved by the designated officials?</p> <p>Are data communication pathways from VA facilities to non-VA business partners that cannot pass through the VA EA Internet gateways fully documented and have the Information Security Officer (ISO) approvals?</p> <p>Are these connections managed and coordinated with and by the VA NSOC?</p>	<p>SDD: Security and Privacy</p> <p>OAP: Architecture/ Dependencies</p> <p>SDD: Interface Detailed Design</p>
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are the required access controls in place to ensure that only authorized individuals gain access to information system resources, are assigned an appropriate level of privilege, and are individually accountable for their actions?	

## 2.5.4 Secure Information Sharing

### Criterion

Specific reasons for all limited, external access to data, including the need to know along with security, privacy, or other legal restrictions, shall be documented.

### Rationale

Using enterprise resources to store permanent data lessens the burden on an application to be a proper data custodian (including security and privacy concerns). It also promotes consistency in how data custodianship is executed and isolates changes to common services when policies are modified.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.1: OI&T Architecture Principles, p. 28
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Does the solution document specify reasons for all (or limited) external access to data, including the need to know along with security, privacy, or other legal restrictions?  Will the solution employ automated audit logs for external data access?	SDD: Security and Privacy
<b>2</b>	Does the solution employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process?  Will system audit logs record sufficient information to establish what events occurred, the sources, and outcomes of the events?  Will additional details such as type, location, and subject be recorded for moderate and high risk systems?  Will audit logs have sufficient detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred?  Will audit logs be treated as restricted information and protected from unauthorized access, modification, or destruction?	SDD: Security and Privacy OAP: Architecture/ Dependencies SDD: Interface Detailed Design
<b>3</b>	Are operational procedures in place to ensure audit logs are reviewed periodically for action?	OAP: Anomaly/Risk Summary

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Are operational procedures in place to ensure system audit logs record sufficient information to establish what events occurred, the sources, and outcomes of the events?  Are operational procedures in place to ensure audit logs are reviewed periodically for action?	System Audit Logs

## 2.5.5 Personally Identifiable Information and Protected Health Information

### Criterion

Appropriate controls to prevent the unwarranted disclosure of sensitive, Personally Identifiable Information (PII), or Protected Health Information (PHI) shall be implemented.

### Rationale

The solution should ensure all access to PII and PHI is logged and subjected to audits.

Ensure appropriate controls are implemented and enforced to prevent storing sensitive, PII, or PHI in exception messages, log files, or persistent cookies.

ESS Services shall comply with VA Directive 6502 like all other VA software.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.1: OI&T Architecture Principles, p. 29
- [VA Directive 6502, VA Enterprise Privacy Program](#)
- [VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment](#)
- ESS SOA Policy 436 (*Privacy tab*)

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Has required analysis been performed to identify the PII or PHI the solution/service needs to handle? If the solution/service handles PII or PHI, can the solution/service log the details of PII and PHI access?	SDD: Overview of the Security or Privacy Requirements
<b>2</b>	If the solution/service handles PII or PHI, does the solution/service employ automated mechanisms to log details of the access of PII and PHI data, including the “who, what, where, when, and why” of the person and/or application that accessed the data? Have appropriate controls been implemented to prevent storing sensitive, PII, or PHI in exception messages, log files, or persistent cookies?	SDD: Overview of the Security or Privacy Requirements
<b>3</b>	If the solution/service handles PII or PHI, are operational procedures in place to ensure audit logs of access to PII and PHI data are reviewed periodically for action?	OAP: Anomaly/Risk Summary

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Has the usage of PII and PHI within this system been identified and recorded in VASI? If this system handles PII or PHI, does the system employ automated mechanisms to log details of the access of PII and PHI data, including the “who, what, where, when, and why” of the person and/or application that accessed the data?	System Audit Logs VASI

## 2.5.6 Homeland Security Presidential Directive 12

### Criterion

Solution design shall be smartcard-enabled to handle logical logon using Public Key Infrastructure (PKI).

### Rationale

Homeland Security Presidential Directive 12 (HSPD-12) is a strategic initiative intended to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials, including a standardized background investigation to verify employee and contractor identities. Each agency is to develop and issue an implementation policy by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.

### Sources

- [Office of Management and Budget \(OMB\) M11-11: HSPD-12 Directive](#)
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Has the project planned to perform the required analysis to identify the solution’s readiness to handle logical logon based on PIV cards?  Has the project planned to perform the required analysis to identify the solution’s readiness to support PIV-based authentication (smartcard-enabled or integrated with Enterprise IAM Single Sign-on Interval [SSOi])?	SDD: Overview of the Security or Privacy Requirements
<b>1</b>	Has the solution been smartcard enabled to handle logical logon using PKI?  Has the solution designed to support PIV-based authentication (smartcard enabled or integrated with Enterprise IAM SSOi)?	SDD: Overview of the Security or Privacy Requirements  SDD: Security and Privacy
<b>2</b>	Has the solution been smartcard enabled to handle logical logon of the internal VA users using PKI?  Has the solution been implemented to support PIV-based authentication (smartcard-enabled or integrated Enterprise IAM SSOi) of VA internal users?	SDD: Security and Privacy
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Has an e-Authentication risk assessment been completed for this system to identify the appropriate Level of Assurance (LOA) as defined in NIST SP 800-63-1 and OMB M-04-04?  Has the system fully implemented one of the approved authentication mechanisms based on LOA, as recommended by the Enterprise design patterns for Authentication and Authorization, or received an approved waiver from OIS?	

## 2.6 Enterprise Capabilities

*VA solutions shall utilize enterprise-wide standards, services, and approaches to deliver seamless capabilities to Veterans, facilitate IT consolidations through reuse, and simplify the use of Veteran functions.*

### 2.6.1 Messaging Standards – Simple-Object Access Protocol-Based Services

#### Criterion

All Simple-Object Access Protocol (SOAP) -based implementations of a Service must comply with The Web Services-Interoperability Organization (WS-I) Standards. In particular, Services must comply with WS Interoperability Basic Profile and WS Interoperability Basic Security Profile.

#### Rationale

Many combinations of technologies are possible within the Web Services suite of specifications, some of which are not interoperable with each other. Adherence to WS-I standards provides a better foundation for interoperability.

#### Sources

- VA Enterprise Target Application Architecture v1.0, Section 5.6.4.3: Format Harmonization, p. 109
- [WS Interoperability Basic Profile](#)
- [WS Interoperability Basic Security Profile](#)
- Message Exchange Guide, v1.0
- ESS SOA Policy 43 (*Architecture tab*)
- Enterprise Application Design Patterns: VistA Evolution
- Interoperability and Data Sharing Design Patterns: Enterprise Messaging Capabilities and Message Exchange

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	For SOAP-based Service implementations, does the service design follow WS Interoperability Basic Profile and WS Interoperability Basic Security Profile standards?	SDD: Conceptual Application Design
<b>2</b>	For SOAP-based Service implementations, does the service design follow WS Interoperability Basic Profile and WS Interoperability Basic Security Profile standards?	SDD: External System Interface Design SDD: Software Detailed Design
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.2 Messaging Standards – Healthcare Information Exchange

### Criterion

Unless otherwise required, messages and protocol will follow the Health Level 7 (HL7) 2.x and/or 3.0 standards for the applicable domains.

### Rationale

Industry-standard messaging is required for interoperability among systems.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 5.6.4.3: Format Harmonization, p. 109
- [Health Level 7 \(HL7\) 2.x](#)
- [Health Level 7 \(HL7\) 3.0](#)
- Message Exchange Guide, v1.0
- ESS SOA Policy 20 (*Architecture tab*)
- Enterprise Application Design Patterns: VistA Evolution
- Interoperability and Data Sharing Design Patterns: Enterprise Messaging Capabilities and Message Exchange

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	If healthcare information is being exchanged through the service, are messages and protocol following the HL7 2.x and/or 3.0 standards?	SDD: Conceptual Application Design
<b>2</b>	If healthcare information is being exchanged through the service, are messages and protocol following the HL7 2.x and/or 3.0 standards?	SDD: External System Interface Design SDD: Software Detailed Design
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.3 Service Registry

### Criterion

Solution shall leverage existing services published in the VA Service Registry.

### Rationale

Ensure usage of ESS to increase return on investment (ROI), eliminate waste and duplication, improve the effectiveness of technology solutions, and reduce costs through shared approaches to program activities. Application Services need to be developed and made available for reuse by the enterprise and application. Development efforts should reuse registered services.

### Sources

- [OMB Shared First Policy](#)
- VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Application Architecture Principles, p. 34
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Has required analysis been performed to leverage applicable Shared Enterprise Services in the VA Service Registry?	SDD: Conceptual Application Design
1	Not applicable	
2	Have the services introduced/upgraded by the solution been published in the VA Service Registry?	VA Service Registry
3	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Not applicable until fully operational VA service registry is available for VA Enterprise Shared Service registration	

## 2.6.4 Service Reuse

### Criterion

ESS Services shall have an interface that expresses a well-defined functional boundary that does not duplicate functionality of other services. The boundaries will be judged as compliant through inception and design reviews.

### Rationale

To control costs and avoid unpredictable system behavior it is essential that software functions not be duplicated or reinvented. Further, services with redundant or overlapping functionality cause confusion for potential consumers during the service discovery process as to which service should be used to satisfy their need.

### Sources

- ESS Strategy, Section 2.1.1
- ESS SOA Policy 54 (*Architecture tab*)
- Enterprise Application Design Patterns: Vista Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Have service discovery procedures been followed to assure that the same service functionality is not being duplicated?  If there is overlap in function with an existing service, has a refactoring plan been established to remove the overlap?	SDD: Service Oriented Architecture (SOA)/ESS Detailed Design
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Have all system interfaces and the underlying information exchanges been registered in VASI?	VASI

## 2.6.5 Service Architecture Layering

### Criterion

The ESS SOA shall be organized as a series of layers, with each layer containing services of particular types. A service must belong to one of the following permitted layers: Presentation Logic Layer, Business Logic Layer, and Underlying Logic Layer.

### Rationale

Organizing architecture into a series of well-defined layers with specific areas of concern is a best practice (separation of concerns). Grouping services into functional layers reduces the impact of change. Most changes affect only the layer in which they are made, with few side effects that impact other layers. Restricting each layer to a particular functionality simplifies the design of the service and service maintenance. It also enhances the potential to reuse the service across the enterprise because their solution logic is independent of any particular business process or technology. The result is financial savings to the VA while providing a more useful suite of enterprise services.

### Sources

- ESS SOA Policy Set:
  - Service Architecture Layering: ESS SOA Policy 437 (*Architecture tab*)
  - Presentation Logic Layer: ESS SOA Policy 438 (*Architecture tab*)
  - Business Logic Layer: ESS SOA Policy 439 (*Architecture tab*)
  - Underlying Logic Layer: ESS SOA Policy 440 (*Architecture tab*)
- ESS SOA Design – How To Guide Document v5.10
- Enterprise Application Design Patterns: VistA Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Have the services being reviewed been organized by/assigned to one of the permitted layers? Do the characteristics of the service match those of the services in that layer?	SDD: SOA/ESS Detailed Design
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.6 Service Types

### Criterion

Services shall be assigned types consistent with and based on the Open Group SOA Reference Architecture.

### Rationale

Assignment of service types assists in effecting separation of concerns and the assignment of services to appropriate service layers. Grouping services by type provides clear, concise, and non-overlapping definitions to facilitate communication by providing a common and accepted language, allowing more effective communication between the various VA stakeholders.

### Sources

- Open Group SOA Reference Architecture
- ESS SOA Policy Set:
  - Service Types: ESS SOA Policy 441 (*Architecture tab*)
  - Presentation Layer: ESS SOA Policy 442 (*Architecture tab*)
  - Business Logic Sublayer: ESS SOA Policy 443 (*Architecture tab*)
  - Underlying Logic Layer: ESS SOA Policy 444 (*Architecture tab*)
- ESS SOA Design – How To Guide Document v5.10
- Enterprise Application Design Patterns: Vista Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Has the service been assigned a service type?	SDD: SOA/ESS Detailed Design
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.7 Service Design

### Criterion

Services (e.g., Interface and Implementation) must be reviewed for compliance with the ESS Guideline documents (e.g., Service Namespace, Exception Handling, Versioning, Security, and Messaging design guidelines).

### Rationale

Uniformity of service planning and specification artifacts (1) enables service designers to provide consistent behavior of services in their environments and interactions with other services, (2) facilitates the reuse of services by designers, thus lowering cost of development, and (3) facilitates the discovery of services for use by consumers.

### Sources

- ESS SOA Architecture
- ESS SOA Architecture – ESS Design Guidelines:
  - Service Namespace Guidance, v1.1
  - Exception Handling Guidance, v1.0
  - Service Versioning Guidance, v0.2
  - Security Design Guidance, v0.6
  - Message Exchange Guide, v1.0
- ESS SOA Policy Set:
  - ESS SOA Policy 349 (*Architecture tab*)
  - ESS SOA Policy 403 (*Architecture tab*)
  - ESS SOA Policy 404 (*Architecture tab*)
- Enterprise Application Design Patterns: Vista Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the service design consistent with the ESS Guideline Documents published on the ESS website?	SDD: SOA/ESS Detailed Design
<b>2</b>	Is the service design consistent with the ESS Guideline Documents published on the ESS website?	SDD: SOA/ESS Detailed Design
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.8 Extensible Markup Language Standards

### Criterion

- An Extensible Markup Language (XML) documents shall conform to an XML definition written in accordance with XML Schema v1.0, XML Schema v1.1, or Schematron [check latest DoD Information Technology Standards and Profile Registry (DISR) accepted version]. An XML document should not be defined using Document Type Definitions (DTD).
- The use of wild-cards, unstructured, or character data (CDATA) in schemas shall be avoided.
- Types shall be specified for all schema constructs.

### Rationale

The use of W3C XML and XSD standards as intended enhances the interoperability of messages based on XML. Ambiguous “exceptions” accommodated by the standard (such as CDATA for non-semantically differentiated data, and wild-cards for undifferentiated types and type specifications) may impair interoperability.

### Sources

- Message Exchange Guide, v1.0
- ESS SOA Policy Set:
  - Assertion 1: ESS SOA Policy 115 (*Architecture tab*)
  - Assertion 2: ESS SOA Policy 117 (*Architecture tab*)
  - Assertion 3: ESS SOA Policy 122 (*Architecture tab*)
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Have all uses of XML documents in the SDD been written to conform to these XML standards?	SDD: SOA/ESS Detailed Design
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.9 External System Access

### Criterion

External systems shall not be allowed direct access to VA internal functional services and will need to be processed through an interface layer that provides the security services.

### Rationale

External consumers have different security characteristics than internal consumers and, therefore, additional mechanisms must be put in place to address those issues.

### Sources

- ESS SOA Policy 39 (*Architecture tab*)
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	If a service is intended for external consumption, how has the design addressed the additional security issues associated with external consumers?	SDD: SOA/ESS Detailed Design
2	If a service is intended for external consumption, has an interface layer been implemented to address the additional security issues?	SDD: SOA/ESS Detailed Design
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.10 Service Access

### Criterion

Services shall be accessed only through the exposed, published interfaces. Exposed interfaces are the sole entry points into service logic and resources.

### Rationale

“Backdoor” access to services can result in system instability. The service’s contract for uniform behavior is at the published interface. Changes can be made to the execution details of the service, which can result in unexpected results from alternate, unpublished, and non-contracted access techniques.

### Sources

- ESS SOA Policy 52 (*Architecture tab*)
- Enterprise Application Design Patterns: VistA Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is all service usage specified to be approved and published through interfaces in the service environment?	SDD: SOA/ESS Detailed Design
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.11 Service Documentation

### Criterion

All Service documentation shall follow the templates defined in the ESS Architecture documentation guidelines.

### Rationale

Uniform documentation is necessary to provide uniform quality, the ability to review system design, and efficient provisioning of the service.

### Sources

- ESS SOA Service Artifacts Templates
- ESS SOA Policy 188 (*Architecture tab*)
- Enterprise Application Design Patterns: VistA Evolution

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Have the documents specified in the ESS Architecture Document Guidelines been created?	SDD: SOA/ESS Detailed Design
2	Have the documents specified in the ESS Architecture Document Guidelines been created?	SDD: SOA/ESS Detailed Design
3	Have the documents specified in the ESS Architecture Document Guidelines been created?	SDD: SOA/ESS Detailed Design

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.12 ESS Governance Approval

### Criterion

Documentation of service attributes will be approved through the appropriate ESS Governance processes and by the process-designated approver(s).

### Rationale

ESS Governance processes assure that services are documented to provide clear guidelines regarding the scope, lifecycle, description, and expected service levels to provide appropriate information and visibility to the user community to maximize the adoption and minimize the redundancy of the service architecture.

### Sources

- ESS SOA Service Artifacts Templates
- ESS SOA Policy Set:
  - ESS SOA Policy 431 (*Service Asset Mgmt tab*)
  - ESS SOA Policy 432 (*Service Asset Mgmt tab*)
  - ESS SOA Policy 433 (*Service Asset Mgmt tab*)
  - ESS SOA Policy 434 (*Service Asset Mgmt tab*)
  - ESS SOA Policy 435 (*Service Asset Mgmt tab*)
- Enterprise Application Design Patterns: VistA Evolution

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Does the ESS Service Charter clearly describe the appropriate scope for the service? Is the ESS Service Roadmap achievable? Has the ESS Service Roadmap been vetted against the roadmaps of planned consumers and other services upon which this service may depend? Has the Service Description been specified in sufficient detail to enable unambiguous consumption of the service and allow for subsequent internal design and provisioning to occur? Are the responsibilities of both the consumer and provider well defined? Are the service levels attainable for planned usage? Is there an SLA in place for each pair of providers/consumers? Have both business and technical owners of the consumer and provider “signed” the SLA?	ESS Service Charter ESS Service Roadmap ESS Service Description ESS Service Level Agreement
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.13 Identity and Access Management (IAM) Service

### Criterion

Solution shall use Enterprise IAM Services.

### Rationale

The Federal Identity, Credential, and Access Management (FICAM) Roadmap details additional rationales for adopting an identity and access services framework to support business and/or objectives. IAM services provide a framework for identity, credential, and access services. IAM services also provide compliance, increased security, improved interoperability, enhanced customer self-service, and increased protection of PII.

A significant part of VA's mission is to assure that information and systems are protected from unauthorized access. It is essential that it be designed into the infrastructure. Sensitive information must be protected on a need-to-know basis.

### Sources

- [VA Directive 6510, VA Identity and Access Management](#)
- [OMB Shared First Policy](#)
- VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Application Architecture Principles, p. 35
- ESS SOA Policy 239 (*Security tab*)
- Privacy and Security Design Patterns: User Identity Authentication
- Privacy and Security Design Patterns: External User Identity Authentication – Increment 2
- Enterprise Application Design Patterns: VistA Evolution

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Do the business requirements include IAM aspects (i.e., managing person identity, compliance, customer self-service, authenticating users, and enforcing entitlement/access decisions) that enable adequate integration of the solution with the IAM capabilities?	Business Requirements Document (BRD) RSD: Security Specifications
<b>1</b>	Has the required analysis been performed to leverage Enterprise IAM capabilities for the solution’s authentication, authorization, and auditing needs?  Have the integration RSD, consuming application SDD, and User Acceptance and Integration Test Plans been reviewed and approved by IAM (as signatory)?  Has the Consuming Application Project team provided the IAM Service Request recommendation from the Governance Review that provides guidance on when IAM capabilities will be ready for consumption?	SDD: Conceptual Application Design
<b>2</b>	Does the solution use the Enterprise IAM Service?  If the required IAM capabilities are not leveraged, has the IAM team been told the reasons for not leveraging IAM offered capabilities?  Are operational logs being monitored for unauthorized access attempts? Are operational logs being routinely monitored?	SDD: External System Interface Design SDD: Software Detailed Design Systems Operation Logs
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Has this system’s utilization of mandated Enterprise IAM Services been registered in VASI?  If the required IAM capabilities are not leveraged, have the reasons been documented and communicated to IAM Business Office?	VASI

## 2.6.14 Service-Enabled Information Sharing

### Criterion

Solution shall use enterprise information that is made available as services.

### Rationale

The goal is to disallow development of monolithic systems. The solution needs to share the business functionality for enterprise usage through [service](#)<sup>9</sup>-enabled design. Reusing enterprise-level services and making application services available to the enterprise saves money and resources. It also promotes continuity in processing.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.3. Enterprise Application Architecture Principles, p. 34
- Enterprise Application Design Patterns: VistA Evolution
- Enterprise Application Design Patterns: End-to-End Application Performance Management (APM) (August 2014)
- Interoperability and Data Sharing Design Patterns: Data as a Service

---

<sup>9</sup> Ibid.

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Has required analysis been performed to identify the available Shared Enterprise Services required for the solution in the VA Service Registry?	SDD: Application Context SDD: Data Design VA Service Registry
<b>1</b>	Not applicable	
<b>2</b>	Is the enterprise information used and produced by this solution available through services?  Are all services that are part of this system registered in the VA Service Registry and discoverable through the VA services portal?	SDD: External System Interface Design  SDD: Software Detailed Design
<b>3</b>	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.15 Technical Reference Model

### Criterion

All Products and Standards used by the solution shall be listed and identified as permissible for usage in the VA TRM.

### Rationale

Ensure the solution adheres to VA approved standards and products to leverage IT investments and an integrated technology framework (Clinger-Cohen Act).

### Context

Applicable to PD, Office of Responsibility (OOR) PMAS Projects

### Sources

- [VA TRM](#)
- [VA TRM Announcement \(WebCIMS 447341\), dated 7/1/2011](#)
- [VA TRM Compliance Enforcement and Announcement \(VAIQ 7110943\), dated 7/1/2011](#)
- Enterprise Application Design Patterns: VistA Evolution
- IT Service Management (ITSM) Design Patterns: ITSM Increment 1

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	<p>Has the required analysis been performed to determine that the solution will be supported by the permissible products and standards and their respective versions in TRM?</p> <p><b>[Note:</b> Any technology in use in VA's production operating environment that is non-compliant with the TRM or does not have a valid waiver will be removed from the production operating environment.]</p>	<p>SDD: Conceptual Infrastructure Design</p> <p>SDD: Enterprise Architecture</p> <p>OAP: Electronic Inventory List and Asset Management VA TRM</p>
<b>2</b>	<p>If the project needs new products that are not in the TRM:</p> <p>Have technology insertion requests been submitted for the required products early enough in the project lifecycle such that the products will be available when needed?</p> <p>Has a lifecycle cost estimate been performed for the candidate technologies?</p> <p>Have common cost-savings practices been taken into consideration for avoidance of additions to the TRM?</p>	Product Evaluation and Decision Analysis
<b>3</b>	Has a determination been made to retire older products from the TRM that were replaced by the new products?	VA TRM

**IT Operational Analysis/System Sustainment**

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
<p>Have all technologies used by this system been listed and identified as permissible for usage in the VA TRM?</p> <p>Have all critical technologies belonging to this system been validated and registered in VASI?</p>	<p>VA TRM</p> <p>VASI</p>

## 2.6.16 COTS Products

### Criterion

All commercial off-the-shelf (COTS) products used in the solution shall be from mature companies large enough to support those products over the expected life of the product at all locations at which they may be installed.

### Rationale

Ensure the COTS products used in the solution are supported by the vendor across the VA enterprise over its full lifecycle until it is removed from VA service.

### Sources

- VA Enterprise Target Application Architecture v1.0, Section 2.1: OI&T Architecture Principles, p. 25
- Enterprise Application Design Patterns: VistA Evolution

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	<p>Is the vendor company stable and likely to remain so to support the COTS product as long as VA needs it?</p> <p>Are all COTS products used in the solution from mature companies large enough to support those products for the entire expected life, at all locations at which they may be installed?</p>	Product Evaluation and Decision Analysis
<b>2</b>	<p>Are all IT products on the National Information Assurance Program (NIAP) Validated Product List (VPL) or accepted for NIAP evaluation?</p> <p>Are the employed COTS products not approaching the end of their life (i.e., the user base is no longer expanding, new versions of the product are only sold to previous customers, and companies using the product only use it to support legacy applications)?</p> <p>Does custom code interact with COTS products only through vendor-supplied Application Program Interfaces (API) or interfaces that the vendor guarantees will be supported through future versions?</p> <p>Where VA requires significant changes to a COTS product, did VA get the vendor to make the changes to the core product, incorporate those changes into the standard distribution, and support those changes through future releases of the product?</p>	Product Evaluation and Decision Analysis SDD: Software Detailed Design
<b>3</b>	Is a copy of COTS product's source code held in escrow by a third party for "code vaulting," ensuring that if a COTS product vendor goes out of business, VA will have a copy of the source code as a basis for future maintenance efforts?	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.17 VA Systems Inventory (VASI)

### Criterion

All VA IT Systems **must** be registered in VASI. In addition, the system information in VASI **must** be validated during all VA reviews associated with defining, building, enhancing, certifying, operating, or retiring VA IT Systems.

### Rationale

VASI is the authoritative data source for information used to identify and describe VA IT Systems. It provides a Department-wide inventory of systems and systems-related information that reflects the current state of the VA's information environment. Through the EA, VASI links systems information to other information about VA's business and IT environment, enabling analysis and decision support across a wide variety of topics.

### Sources

- [VA Directive 6404](#)
- VA EA: VASI

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
<b>0</b>	Not applicable	
<b>1</b>	Is the VA IT System being built or enhanced during this solution development registered in VASI and the associated system information validated?	VASI
<b>2</b>	Not applicable	
<b>3</b>	Not applicable	

### IT Operational Analysis/System Sustainment

Compliance Question(s)	Relevant Artifact for Demonstrating Compliance
Is the VA IT System for which the IT Operation Analysis is being conducted registered in VASI and the associated system information validated?	VASI

## 2.6.18 Enterprise Message Infrastructure

### Criterion

All VA IT ESS **must** utilize the Enterprise Message Infrastructure (eMI) capabilities and services.

### Rationale

The VA has elected to implement an eMI to provide an integrated messaging approach using a common service bus. This will allow the connections of legacy applications to modern services using standards-based methodology in a secure, reusable manner. The eMI includes native capabilities to transform, translate, aggregate, and distribute messages across the enterprise. The solution is implemented using Open Standards and brings centralized monitoring, management, and security control to the organization.

Through use of the eMI, applications can reduce their messaging complexity and leverage the native capabilities provided by eMI. eMI in conjunction with ESS (1) is designed to take advantage of VA infrastructure and other ESS investments, (2) provides end-to-end (E2E) environment monitoring through use of Enterprise Management Framework (EMF), (3) provides load balancing and fault-tolerance (99.999 percent uptime design), (4) is integrated with Identity Access Management (IAM) to provide both Person Entity (PE) and non-Person Entity (NPE) security controls, (5) uses VA Cloud infrastructure (both Production and Development and Test leverage Enterprise Operations Cloud/IaaS), and (6) supports capacity on demand, scalable, with proven ability to handle more transactions than National Association of Securities Dealers Automated Quotation (NASDAQ) (> 60,000 MPS).

### Sources

- ESS Directive 6000 (Draft), Policy Section: e. "The deployment of services shall be standardized to ensure that VA can efficiently scale services and reduce the time to field capabilities," p. 3
- ESS SOA Policy 239 (*Security tab*)
- Enterprise Application Design Patterns: VistA Evolution

**Solution Development Compliance**

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Do the business requirements include messaging aspects (i.e., service and application interface design, compliance, service registration decisions) that enable adequate integration of the solution with the eMI capabilities?	BRD
1	If messaging is required:  Has the required analysis been performed to leverage eMI capabilities for the solution’s messaging needs? Have the integration RSD, consuming application SDD, and User Acceptance and Integration Test Plans been reviewed and approved by eMI Integration Team (eMI-IT) (as signatory)?	RSD  SDD: Conceptual Application Design  User Acceptance and Integration Test Plans
2	Does the solution use the eMI capabilities? Specifically, use of eMI is mandated if the messaging design pattern includes:  Transformation of message type (e.g., HL7 2.x–3.x); translation of message format (e.g., Minimal Lower Layer Protocol [MLLP] to SOAP); mediation or orchestration (e.g., modifying information within a message by adding, changing the message); message routing requiring use of business rules (e.g., aggregating or sending to multiple users) or broadcast message, broadcast request/response, publish/subscribe, or store and forward; two or more consumers using the same service.  If the required eMI capabilities are not leveraged, has a waiver been obtained from the AERB not to use the eMI offered capabilities?  Additionally, if any message crosses an Information Assurance (IA) boundary, is it using an approved “gateway” (e.g., eMI, Data Access Service (DAS) or Virtual Lifetime Electronic Record [VLER] Health Exchange)?	SDD: Software Detailed Design  SDD: External System Interface Design  Metrics from monitoring agents
3	Not applicable	

**IT Operational Analysis/System Sustainment**

- Not applicable

## 2.6.19 Open Source Software

### Criterion

Open Source Software (OSS) shall be thoroughly evaluated when VA acquires software, and OSS development practices shall be considered when VA develops software.

### Rationale

VA recognizes that many potential advantages exist in to using and relying on OSS solutions in support of VA's mission. Potential advantages of OSS solutions include lower development costs, lower licensing costs, lower maintenance costs, faster introduction of community-developed innovations, higher software quality, and increased openness and transparency.

### Sources

- [VAIQ# 7532631](#) – Consideration of Open Source Software Memorandum

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	Have OSS solutions been thoroughly evaluated where the solution requires the acquisition of COTS products?  Have OSS development practices been considered for VA-developed software solutions?	SDD: Detailed Design
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## 2.6.20 Standardized National Software

### Criterion

Modifications to local software instances of Protected National Software must be approved by the Software Modification Waiver Committee (SMWC) for sites that have implemented the certified Gold Disk version of Vista.

### Rationale

Veterans Health Administration (VHA) clinical and management operations rely on accurate and consistent support from a suite of information systems; of these, Veterans Health Information Systems and Technology Architecture (Vista) represents the major system. Vista is used to implement regulations, processes, and controls that must be applied consistently across VHA. Unauthorized changes to Vista can disable or impair critical VHA functions and, in serious cases, result in patient safety incidents.

### Sources

- [VA Directive 6402](#) – Modifications to Standardized National Software

### Solution Development Compliance

PMAS Milestone	Compliance Question	Relevant Artifact for Demonstrating Compliance
0	Not applicable	
1	If this solution will result in local modifications to a certified Gold Disk instance of Protected National Software, has an approved waiver been received from the SMWC?	SDD: Detailed Design
2	Not applicable	
3	Not applicable	

### IT Operational Analysis/System Sustainment

- Not applicable

## Appendix A Acronyms and Abbreviations

Abbreviation	Definition
AERB	Architecture Engineering Review Board
API	Application Programming Interface
ASD	Architecture, Strategy, and Design
ATO	Authority to Operate
BIA	Business Impact Analysis
BRD	Business Requirements Document
BRM	Business Reference Model
C&A	Certification and Accreditation
CBOC	Community-Based Outpatient Clinic
CDATA	Character Data
CDM	Conceptual Data Model
CIO	Chief Information Officer
COTS	Commercial-off-the-Shelf
CPU	Central Processing Unit
CSS	Cascading Style Sheet
DaaS	Data as a Service
DAR	Data Architecture Repository
DAS	Data Access Service
DISR	DoD Information Technology Standards and Profile Registry
DR	Disaster Recovery
DTD	Document Type Definition
E2E	End-to-End
EA	Enterprise Architecture
EAC	Enterprise Architecture Council
EAWG	Enterprise Architecture Working Group
EDM	Executive Decision Memorandum
EIM	Enterprise Information Management
EITA	Electronic and Information Technology Accessibility
EMF	Enterprise Management Framework
ESB	Enterprise Service Bus
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
FAQ	Frequently Asked Question
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GIS	Geographic Information System
GRC	Governance Risk and Compliance

Abbreviation	Definition
HITSP	Healthcare Information Technology Standards Panel
HL7	Health Level 7
HSPD-12	Homeland Security Presidential Directive - 12
HTML	HyperText Markup Language
IA	Information Assurance
IaaS	Infrastructure as a Service
IAM	Identity Access Management
IEEE	Institute of Electrical and Electronics Engineers
IMS	Integrated Master Schedule
IP	Internet Protocol
IPT	Integrated Project Team
ISCP	Information Systems Continuity Planning
ISO	Information Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LAN	Local Area Network
LOA	Level of Assurance
LOINC	Logical Observation Identifiers, Names, and Codes
MDR	Metadata Registry
MLLP	Minimal Lower Layer Protocol
MPS	Megabits per second
MS0	Milestone 0 (PMAS)
MS1	Milestone 1 (PMAS)
NASDAQ	National Association of Securities Dealers Automated Quotation
NIAP	National Information Assurance Program
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSOC	Network and Security Operations Center
OA	Operational Analysis
OAP	Operational Acceptance Plan
OI&T	Office of Information and Technology
OIS	Office of Information Security
OMB	Office of Management and Budget
OOR	Office of Responsibility
OS	Operating System
OSS	Open Source Software
PaaS	Platform as a Service
PD	Product Development
PE	Person Entity
PHI	Protected Health Information

Abbreviation	Definition
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Project Manager
PMAS	Project Management Accountability System
PMP	Project Management Plan
QA	Quality Assurance
ROI	Return on Investment
RPO	Recovery Point Objective
RSD	Requirements Specification Document
RTO	Recovery Time Objective
SaaS	Software as a Service
SDD	System Design Document
SDE	Service Delivery and Engineering
SEDR	System Engineering and Design Review
SLA	Service Level Agreements
SME	Subject Matter Expert
SMWC	Software Modification Waiver Committee
SNOMED	Systematized Nomenclature of Medicine
SOA	Service Oriented Architecture
SOAP	Simple-Object Access Protocol
SP	Special Publication (NIST)
SSOi	Single Sign-On Internal
TCP	Transmission Control Protocol
TRM	Technical Reference Model
TS	Technology Strategies
UI	User Interface
USC	U.S. Code
VA	Department of Veterans Affairs
VADI	VA Data Inventory
VAMC	VA Medical Center
VASI	VA Systems Inventory
VHA	Veterans Health Administration
VIM	Veteran Information Model
VistA	Veterans Integrated System Technology Architecture
VLER	Virtual Lifetime Electronic Record
VM	Virtual Machine
VOA	Virtual Office of Acquisition
VPL	Validated Product List
WAN	Wide Area Network
WebOps	VA Web Operations
WG	Working Group

Abbreviation	Definition
WS	Web Services
WS-I	The Web Services-Interoperability Organization
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definition

## Appendix B Terms and Definitions

This appendix describes the critical terms used in support of the development of this document and critical to the comprehension of its content. The number in brackets [ ] is the numbered reference in Appendix C: References.

1. **Business Logic layer:** The Business Logic layer implements the core functionality of the system and encapsulates the relevant business logic. It manages business processing rules and logic and is concerned with the retrieval, processing, transformation, and management of data. It typically comprised components that are exposed as service interfaces. [1]
2. **Cloud computing:** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [2]
3. **Data Access Layer:** The Data Access Layer of an Application Architecture provides access to data (persistence storage) hosted within the boundaries of the system, and data exposed by other networked systems, perhaps accessed through services. The data layer exposes generic interfaces that the components in the business layer can consume. The Data Access Layer shields the complexity of data implementation from the Business Logic Layer. [1]
4. **Enterprise Service:** A common or shared IT service that supports core mission areas and business services. Enterprise services are defined by the agency service component model and include the applications and service components used to achieve the purpose of the agency (e.g., identity management, knowledge management, records management, mapping/GIS, business intelligence, and reporting). [3]
5. **Enterprise Technical Architecture:** The ETA is a consistent, vendor-agnostic, open-standards-based, federated architecture composed of component architectures representing the desired “end state” for VA Systems and underlying infrastructure.
6. **Governance:** [4] Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.
7. **Information sharing:** Information sharing is making information available to participants (people, processes, or systems). It includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another. [5]
8. **Middleware:** In a distributed computing system, middleware is defined as the software layer that lies between the OS and the applications on each site of the system. [6]
9. **Platform:** A computing platform includes a hardware architecture and a software framework (including application frameworks), where the combination allows software, particularly application software, to run. [7]
10. **Presentation Layer:** The Presentation Layer of an Application Architecture contains the user-oriented functionality responsible for managing user interaction with the system, and

generally consists of components that provide a common bridge into the core business logic encapsulated in the business layer. [1]

11. Service: A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistently with constraints and policies as specified by the service description. [8]
12. Service Oriented Architecture: A paradigm for organizing and using distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations. [9]
13. Thin Client: Client software running on regular end-user machine (Desktop/Laptop/Mobile device) that relies on the server to perform the data processing.

## Appendix C References

1. *Technical Standard, Service-Oriented Architecture Ontology*. Document number C104. The Open Group.2010.
2. Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing*. SP 800-145. U.S. Department of Commerce. September 2011. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
3. *IEEE Standard Glossary of Software Engineering Terminology*. IEEE Standards Board. 1990. [http://www.mit.jyu.fi/ope/kurssit/TIES462/Materiaalit/IEEE\\_SoftwareEngGlossary.pdf](http://www.mit.jyu.fi/ope/kurssit/TIES462/Materiaalit/IEEE_SoftwareEngGlossary.pdf).
4. *OASIS SOA Reference Model*. IEEE Standards Board. August 2002.
5. "Information Technology Infrastructure Library (ITIL) Glossary of Terms, Definitions, and Acronyms v3." v3.1.24." May 30, 2007. [http://www.bonneaud.net/download/ITIL\\_Glossary\\_V3\\_1\\_24.pdf](http://www.bonneaud.net/download/ITIL_Glossary_V3_1_24.pdf).
6. Krakowiak, Sacha, "What is Middleware?" OW2 Consortium. 2003. <http://middleware.objectweb.org>.
7. Wikipedia, "Computing Platform." [https://en.wikipedia.org/wiki/Computing\\_platform](https://en.wikipedia.org/wiki/Computing_platform).
8. The Open Group. *Service-Oriented Architecture Ontology Technical Standard*. December 8, 2010.
9. "OASIS Reference Model for Service Oriented Architecture 1.0 Committee Specification 1." OASIS. August 2, 2006. <https://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf>.

# Appendix D ETA Compliance Criteria Frequently Asked Questions

## D1 Purpose of FAQs

The purpose of this set of Frequently Asked Questions (FAQ) is to assist program IPTs in using ETA compliance criteria to ensure alignment of VA programs, projects, initiatives, or investments with the technical layer of the VA EA. This FAQ, along with the ETA compliance criteria document, serves as an entry point into the vast architecture documentation set developed by OI&T to describe how the IT environment must be designed, configured, and maintained to do the following:

- Ensure interoperability of solutions
- Transition VA's IT capabilities to the technology environment envisioned in the VA ETSP

Program IPTs can use the ETA Compliance Criteria document to both ensure that solutions they develop are in alignment with enterprise-wide technical guidance and help prepare for PMAS milestone reviews that their solutions must pass. At present, PMAS Milestone 0 and Milestone 1 reviews are conducted by the AERB as part of Architecture/Design Evaluation Reviews.

The AERB is the governance body formally designated by VA to make the final determination on whether an IPT is compliant with the ETA. Thus, the role of the AERB is to review the ETA compliance assertions submitted by each IPT and make a formal determination on whether each IPT is compliant with the ETA. At the completion of the milestone review meeting, AERB may deny approval, issue a conditional approval, or issue an approval.

All VA solutions and investments are subject to compliance with both the business and technical layers of the VA EA. The ETA represents only the technical layer of the VA EA; therefore, compliance and/or alignment with the criteria provided in these documents does not represent full VA EA compliance. These documents simplify compliance with the technical layer, which is required by all solutions and investments. Business architecture compliance is defined by the relevant VA Administration or Corporate Staff Office.

After reviewing the FAQs and associated documents along with the referenced URLs, the reader should understand:

- Overall VA EA compliance process and the key elements of VA EA compliance
- Rules, roles, and responsibilities involved in demonstrating and asserting compliance
- Artifacts, processes, and tools that may facilitate VA EA compliance assertion and certification

## D2 Frequently Asked Questions

FAQ #	Question	Answer
1	What is an ETA compliance assertion?	An ETA compliance assertion is the set of activities that an IPT must execute in preparation for an ETA compliance review performed by the AERB.
2	Why is an ETA compliance assertion needed?	<p>Memorandum # VAIQ 7258313, issued by the VA Assistant Secretary for Information and Technology on December 6, 2012, requires that all IPTs subject to PMAS milestone reviews be assessed for compliance with the ETA. It states, "Effective the date of this memo, the attached VA ETA Compliance Criteria shall be used to assess compliance and alignment of all VA development activities with the technical layer of the VA EA. Compliance will be assessed at PMAS Milestone 0 and Milestone 1 reviews."</p> <p>As part of the implementation of this memo, all IPTs subject to PMAS milestone reviews are also required to go through an ETA compliance review with the AERB before their PMAS Milestone 1 review. The purpose of an AERB compliance review of an IPT is to validate that the solution proposed by the IPT complies with VA's ETA. Determination by the AERB that the IPT's proposed solution is ETA-compliant is a prerequisite for full PMAS Milestone 1 approval. For Milestone 0, which occurs early in the program lifecycle, AERB does not perform an ETA compliance review; however, IPTs are required to conduct a self-assessment with applicable ETA compliance criteria, which are structured more in the form of guidance for Milestone 0 reviews.</p>
3	How does an IPT conduct an ETA compliance assertion (logistics and process)?	An ETA compliance assertion is an internal IPT process that should be resourced and executed based on the professional judgment of the IPT PM. The process itself is highly dependent on the type of solution being developed and the associated IPT artifacts. At a minimum, the IPT should rely on the requirements and design documents, such as SDD, to demonstrate that the proposed solution is being developed in a manner compliant with each ETA compliance criterion. The AERB provides an ETA Compliance Checklist for the IPT to document its compliance assertion for each ETA compliance criterion. The IPT then submits the completed ETA Compliance Checklist, SDD, and any other applicable IPT artifacts to the AERB in advance of the AERB ETA compliance review.
4	Who conducts an ETA compliance assertion?	An ETA compliance assertion is the sole responsibility of the IPT. The AERB is responsible for conducting the ETA compliance review. The AERB may rely on subject matter experts (SME) from each OI&T Pillar.

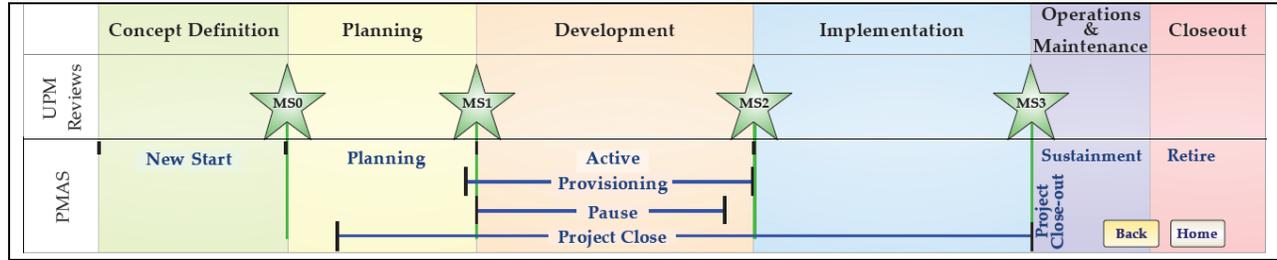
FAQ #	Question	Answer
5	What are the rules for conducting an ETA compliance assertion?	The IPT should rely on the AERB process documented in the most recent release of ProPath and the detailed instructions in the ETA Compliance Checklist provided by the AERB to the IPT.
6	When is an IPT required to complete an ETA compliance assertion?	If an IPT is subject to a PMAS Milestone 1 review, that IPT must also perform an ETA compliance assertion in anticipation of its PMAS Milestone 1 review. If the AERB has approved the IPT SDD for multiple increments, the IPT is already considered ETA compliant for all corresponding PMAS Milestone 1 reviews; no further reviews are necessary.
7	What artifacts are used to complete an ETA compliance assertion?	In addition to the ETA Compliance Criteria Checklist itself, the IPT should rely on the Infrastructure Architecture documents referenced by the ETA Compliance Criteria Checklist, and the IPT SDD and other internally produced IPT artifacts as necessary.
8	How should the IPT prepare and report ETA compliance assertion findings?	Upon completing the ETA Compliance Checklist, the IPT should forward its ETA compliance assertion package to the AERB for review. This assertion package should consist of the completed ETA Compliance Checklist, the IPT SDD, and any other IPT artifacts necessary to substantiate the responses in the completed ETA Compliance Checklist.
9	How should an IPT interpret ETA Compliance Criteria Checklist questions?	The ETA Compliance Criteria Checklist was designed to be self-explanatory. However, if the IPT is unsure about a given criterion, the IPT should rely on the Infrastructure Architecture documentation referenced by each ETA compliance criterion. If the IPT requires further clarification, the IPT should work with its ASD IPT representative to identify the correct OI&T Pillar SME to answer the question.
10	Are there different types of ETA compliance assertions?	It is recognized that not all compliance questions are applicable to every solution being developed. To assist the IPTs, the compliance questions in the ETA Compliance Criteria Checklist have been grouped into commonly developed solution types, which are listed in Table 1-1: Solution Types in this document. These solution types should not be considered mutually exclusive. When completing the ETA Compliance Checklist, the IPT must ensure that all IPT compliance assertions are completed and that any non-applicable criteria are marked as <b>N/A</b> with corresponding comments.

FAQ #	Question	Answer
<b>11</b>	When and how often should an IPT conduct an ETA compliance assertion?	An ETA compliance assertion should generally be performed in advance of the IPT's PMAS Milestone 1 review. Exceptions may exist where the ETA compliance assertion is not required for a given PMAS Milestone 1 review. An example of an exception is where the AERB approves an IPT SDD for multiple IPT increments, because there are no material changes in the SDD across those IPT increments, each of which requires a separate Milestone 1 review.
<b>12</b>	What is the outcome of an ETA compliance assertion?	The final step in the ETA compliance assertion process is an AERB meeting with the IPT to review the IPT's SDD and compliance assertion and any other relevant documentation that the IPT chooses to provide to the AERB. During the course of this meeting, members of the AERB may seek clarifications on the SDD as it relates to ETA compliance. At the completion of this meeting, the AERB may deny approval, issue a conditional approval, or issue an approval. When the AERB issues either a conditional approval or approval, the AERB will document the results in a signed decision certificate that will be provided to the IPT.
<b>13</b>	Upon completing an ETA compliance assertion, what should an IPT do if it is non-compliant with one or more ETA compliance criteria?	When an IPT is not compliant with one or more ETA compliance criteria, the IPT can request that the AERB perform a Waiver Review for the ETA compliance criteria. However, waiver of ETA compliance criteria should be considered the exception rather than the rule. The more likely outcome of an AERB review in this situation is the issuance of a conditional approval, where the IPT will comply with the ETA compliance criteria by a future date or milestone, or the complete denial of approval. All waivers must be signed and approved by the Deputy Chief Information Officer (CIO) of ASD based on a recommendation from the AERB.
<b>14</b>	Where can the IPT find additional information related to ETA compliance assertions?	For more information regarding the completion of an ETA compliance assertion, IPTs should refer to the VA EA website and the latest release of ProPath. As an additional alternative, the IPT may also consult with the ASD representative on the IPT.

FAQ #	Question	Answer
15	What is the difference between guidance and compliance?	<p>ETA guidance describes the policies with which an IPT must comply. ETA compliance can only be determined by the AERB, which relies on ETA guidance, VA policies and directives, and AERB SME's professional judgment.</p> <p>ETA Compliance Criteria describes the rules required to assess compliance for all VA development activities at PMAS Milestone 0 and Milestone 1 reviews with the technical layer of the VA EA. Although IPTs are not required to demonstrate compliance at Milestone 0 currently, the criteria included for Milestone 0 should be used as guidance in planning the design of the solutions. The AERB will determine the ETA Compliance at Milestone 1 using the associated criteria.</p>
16	How are ETA compliance criteria maintained and updated?	ETA compliance criteria are maintained and updated by ASD EA as part of VA EA through the Enterprise Architecture Working Group (EAWG). The EAWG consists of stakeholders from across VA, including representatives from each OI&T Pillar.
17	How does an IPT request an ASD representative for the IPT?	To request an ASD representative for an IPT, an IPT representative should complete and submit an ASD Service Request form through the VA EA Intranet site by selecting the <b>Request ASD/EA Support</b> link in the left navigation column under the label <b>FEEDBACK</b> . An email addressed to ASD EA opens. The IPT representative should then attach the service request to this email and select <b>Send</b> .
18	What is the role of the ASD representative on an IPT?	<p>The ASD representative on an IPT provides guidance in the area of VA EA content. An IPT can be either a consumer or producer of VA EA content. When the IPT is a consumer of VA EA content, the ASD representative may support the IPT in identifying relevant VA EA content to inform the IPT BRD and RSD.</p> <p>When an IPT may be defining new enterprise-wide requirements, the ASD representative may also guide the IPT and its functional sponsor through the process of proposing new VA EA content to the EAWG.</p>
19	What is the role of the AERB in the ETA compliance assertion process?	The AERB is the governance body formally designated by VA to make the final determination on whether an IPT is compliant with the ETA. Thus, the role of the AERB is to review the ETA compliance assertions submitted by each IPT and make a formal determination on whether each IPT is compliant with the ETA. At the completion of this meeting, the AERB may deny approval, issue a conditional approval, or issue an approval. When the AERB issues either a conditional approval or approval, the AERB will document the results in a signed decision certificate that will be provided to the IPT.

FAQ #	Question	Answer
20	What is the relationship of the TRM to the ETA?	The TRM is the official list of products and services that are allowed to operate on VA networks. The ETA contains the technical standards with which all IPTs must comply. Included within the ETA technical standards is the requirement that any products or services introduced by an IPT onto VA networks be approved for inclusion in the TRM.
21	What is the difference between a System Engineering and Design Review (SEDR) and an ETA Compliance Criteria?	The ETA Compliance Criteria is a consolidated list of evaluation criteria pulled from VA's Infrastructure Architecture. A SEDR is conducted by OI&T SDE to verify that the proposed infrastructure portion of a modernization effort is designed, deployed, and managed in a manner that complies with VA's Infrastructure Architecture. The ETA Compliance Criteria is a high-level review that is broader in scope than a SEDR and applies to all IPTs. A SEDR is focused solely on infrastructure and consists of a detailed analysis of the proposed solution architecture.
22	What are the current ETA compliance requirements for PMAS Milestone 0 reviews?	No formal compliance requirements for PMAS Milestone 0 exist at this time. However, the IPT should verify that its proposed solution aligns with the VA EA Business Reference Model (BRM) and is not duplicative of existing or other proposed investments in VA's IT portfolio.
23	How does an IPT obtain the ASD signature for the IPT SDD?	The signed decision certificate issued by the AERB, which documents that the SDD and other associated design documents are ETA compliant, serves as the ASD signature on an IPT's SDD.
24	How can the IPT contact the AERB directly?	Programs and IPTs can contact the AERB by emailing <a href="mailto:vacovaarchitecture@va.gov">vacovaarchitecture@va.gov</a> .
25	How can a copy of the current ETA Compliance Checklist be obtained?	Programs and IPTs may request a copy of the current ETA Compliance Checklist to the AERB by emailing <a href="mailto:vacovaarchitecture@va.gov">vacovaarchitecture@va.gov</a> .
26	Where can copies of current ESS-related documentation be obtained?	Programs and IPTs may find additional ESS-related documentation on the VA EA web site on the Enterprise Shared Services/Service Oriented Architecture page.

## Appendix E PMAS Milestone Artifacts



PMAS States	Artifact
<b>New Start</b>	Project Charter Business Requirements Document (BRD)
<b>Planning</b>	Requirements Specification Document (RSD) Project Management Plan (PMP) Project Schedule Risk Log or Risk Register System Design Document (SDD) Quad Chart Spend Plan (Process Only) Product Evaluation and Decision Analysis (Buy Only) Acquisition Strategy Contract Information Outcome Statement Customer Acceptance Criteria Plan PMAS Readiness Checklist Operational Acceptance Plan (OAP) Confirmation of Release Requirements/Artifacts (ProPath) Submitted Acquisition Package (Virtual Office of Acquisition [VOA]) Executive Decision Memorandum (EDM)
<b>Provisioning</b>	Contract Award (VOA) Updates to Milestone 1 documents
<b>Active</b>	Success Criteria Customer Acceptance Form Integrated Project Team (IPT) Charter Updates to Milestone 1 documents