Department of Veterans Affairs

OneVA – Enterprise Architecture (EA)
Enterprise Technical Architecture(ETA)

ETA Compliance Criteria
Version 1.0

Date: 08/28/2012

This page intentionally left blank for the purpose of printing front and back copies

Contents

1. Introduction

1.1. Purpose

This document 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 OneVA Enterprise Architecture (OneVA 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 IT solutions / investments.

This guide serves as an entry point into the vast architecture documentation that has been developed by OIT to describe how our IT environment must be designed and configured to both:

- Ensure interoperability of solutions, and
- Transition our IT capabilities to the technology environment envisioned in our VA IT Roadmap.

Application developers can use this document to both ensure that solutions they develop are in alignment with enterprise-wide technical guidance and to help prepare for milestone review processes which their solutions must pass. 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 / investments are subject to compliance against both the business and technical layers of the OneVA EA. The ETA represents only the technical layer of the OneVA EA; therefore, compliance and/or alignment with the criteria in this document does not represent full OneVA EA compliance. This document simplifies 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.

1.2. Background

The OneVA 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. It 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 both veterans and VA employees.

Table 1 - OneVA EA Global Principles

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 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.*

The OneVA EA details the full operations of the Department of Veterans' Affairs. As such it has 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.

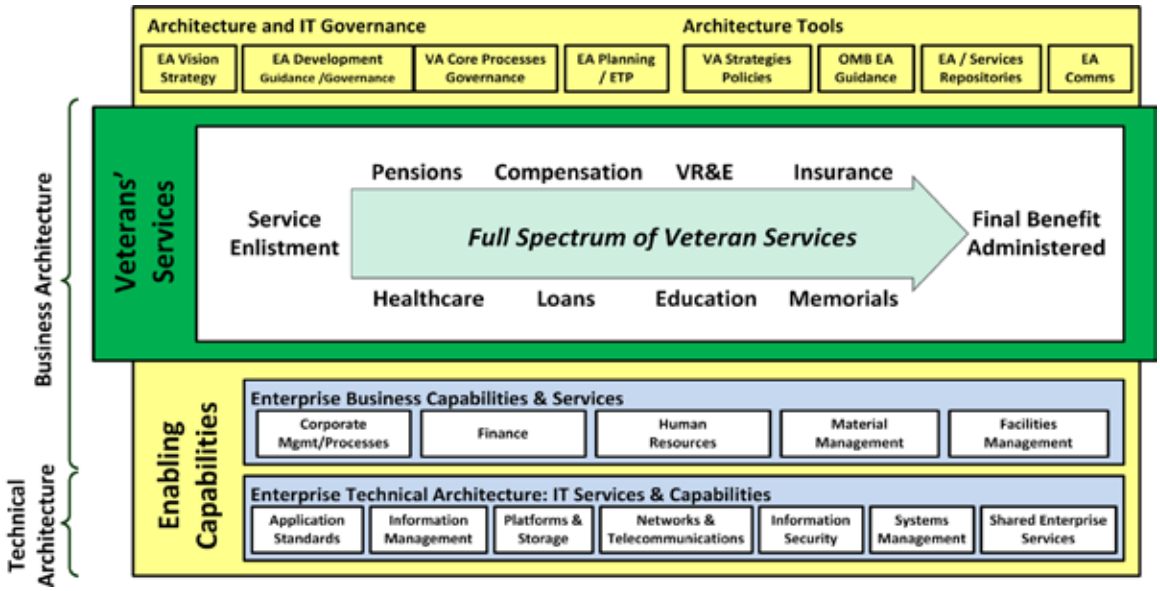


Figure 1 - OneVA Enterprise Architecture

Enterprise Architecture for the technical layer of the OneVA EA, dubbed the VA (ETA), is largely rules and standards based. These rules and standards cover a wide range of topics including use of the VA's infrastructure (including networks, platforms and data storage), information security standards and standards for application design. These rules are influenced both by the needs of today and by our understanding of where and how we need to evolve our technology future as described in our VA IT Roadmap. Over the past year VA's Office of Information and Technology (OIT) 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 OneVA EA intranet site (http://vaww.ea.oit.va.gov/) along with other OneVA EA products, include:

1. VA Enterprise Target Application Architecture v1.0, June 2012, Office of Product Development (PD) (Pending)
2. VA SOA Technical Framework v0.3.1, April 2012, Office of Product Development (PD) (Pending)

3. VA SOA Layer Implementation Guide v0.1, January 2012, Office of Product Development (PD) (Pending)
4. OIT Release Architecture V1.21, November 30, 2011, Service Delivery and Engineering(SDE)
5. The Department of Veterans Affairs Enterprise Architecture Vision and Strategy Document (OneVA EA), Office of Architecture, Strategy & Design (ASD)
6. VA Policy 6500, Handbook 6500, and other 6500 appendices
7. VA Technical Reference Model (TRM), Office of Architecture, Strategy & Design (ASD)
8. VA IT Roadmap, July 2012, Office of Architecture, Strategy & Design (ASD) (Pending)
9. VA Cloud First Policy, DIRECTIVE 6517
10. VA Virtualize First Policy - VA 2105, September 27, 2011
11. VA Information Security Reference Guide v1.0
12. OMB Shared First Policy, December 8, 2011
13. VLER XML Schema Directive, January 24, 2011

These documents collectively contain well over 2000 pages of rules, standards and configuration information that apply to all IT resources within the 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 arose the need for this compliance criteria document.

1.3. Scope

This document has been crafted as a direct response to the need for stakeholders to be able to simply and easily navigate the full array of ETA rules and standards detailed in the documents listed above and be able to ask (and answer) the questions necessary to gauge alignment of solutions with this collective guidance. The VA Enterprise Architecture team reviewed the full array of ETA documentation and developed an initial set of questions, that if answered "YES", would ensure compliance / alignment with the vast majority (90%+) of all ETA rules and standards. The EA team worked closely with the owners of each of the related ETA document owners 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, the program or investment will have to request a waiver from the Architecture and Engineering Review Board (AERB) in order to move forward. Waivers granted should always be conditional on a program or investment having a plan (and budget) in place to achieve the necessary "YES" answer at a defined and agreed upon future date.

The OneVA 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 OneVA 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 there is context 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 might vary based on where in the lifecycle a program or investment lies. To account for this each question provides additional context as to how it can and should be applied at each PMAS milestone (M0-M3), including how one might 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 / alignment means at these additional stages.

1.3.1. **Relationship to PMAS and Other Related Processes**

This document is not intended to layer an additional requirement on developers over and beyond PMAS required documentation, but rather to help focus developers on what part of PMAS documentation is critical at what points in the process. Thus, it should serve not only as a sort of compliance checklist, but also as a navigation tool to both all ETA documentation and PMAS documentation. It is recognized that in this initial state we have additional work to be done to ensure the intended smooth integration; however, both the EA and PMAS teams are committed to working through these details as we move forward. All recognize that it is difficult to gauge the best way to integrate these criteria into the process until they are actually being used. Therefore we will assess and update the Compliance Criteria and PMAS based on feedback gained during initial implementation of these criteria in PMAS reviews.

1.4. Document Conventions

- In order to keep the compliance criteria generic for all applicable lifecycles (i.e. Acquisition vs. System Development), this document uses the term “Solution” in the compliance questions to refer the effort (investment/ project/ application/ program) that is being measured for compliance.

- This document follows the conventions conforming to RFC2119. 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", "SHALL NOT". Exceptions require a waiver and a transition plan.

  Recommended use: These guidelines are identified by the key words "SHOULD", “RECOMMENDED”, "SHOULD NOT", “NOT RECOMMENDED”. These guidelines describe a preferred alternative as judged by VA. Deviation should only be on a limited use and justified by the circumstances.

1.5. Audience

This document is primarily written for the following audience to ensure alignment with enterprise architecture rules and standards.

- VA Project Managers, 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 / alignment

14.

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

Ø Does the solution support Veteran centric mission need or capability?		
Rationale	VA Solutions must enable consistent and seamless delivery of high-quality services to Veterans and their families. 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 objectives, goals, principles, and major initiatives in the VA Strategic Plan Refresh 2011 -2015. The solution must identify the primary mission capability being served with linkage to the strategic direction contained in the VA Strategic Plan Refresh 2011 -2015. This Compliance Criteria document is specific to Technology (not Business) compliance with the OneVA EA. As IT professionals, however, we should never lose sight of our ultimate mission.	
Source	OneVA EA Vision and Strategy, Section 2.1: Principles, p. 3. VA Strategic Plan Refresh FY 2011-15, Chapter-2 Guiding Principles, p. 21	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0-3	Does the business need support VA Major Initiatives (MI) or integrated objectives defined in VA Strategic Plan Refresh 2011 - 2015?	Project Charter – Need & Benefit (section 3)

2.1.2. Business Architecture

Ø Is the solution compliant with the 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 OneVA EA compliance. In addition to Technical (ETA) compliance, all VA IT solutions are also subject to Business EA compliance.	
Source	OneVA EA Vision and Strategy, Section 2.2: Strategic Goals, p. 6.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0-3	Is the solution compliant with appropriate business architecture?	Specifics of Business Architecture

		compliance is beyond the scope of this document.

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

Ø Is the Application 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?
Ø Do the Layers 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 should be functionally organized into layers. Such layering must be reflected in the dependency structure of the application code. For example, the presentation layer[1] should depend on the business logic layer[2], but business logic code must not depend on presentation code. Furthermore, application layers SHOULD be determined independently of the runtime infrastructure. The layered structure also provides a logical way to divide the application development tasks.
Source	VA Enterprise Target Application Architecture v1.0, Section 4: Application Architecture Layers, p. 49.

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has the required analysis been performed to identify the application type, i.e. a web application (generic browser based), a rich-internet application (advanced web application with desktop like interactivity), a portal application (personalized and aggregated view of diverse information sources) or a mobile application? Has a VA recommended application framework for the identified application type been selected for the application development?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Is the application design functionally organized into Presentation, Business Logic and Data Access layers? Is the Presentation layer free from Business or Data Access logic? Is the Business Logic layer free from Presentation and Data Access	System Design Document(SDD) – Software Detailed Design (section 6.2)

[1] Appendix – B Glossary #10

[2] Appendix – B Glossary #1

	logic? Does the Business Logic layer interface with the Data Access layer[3] for processing the data logic and data manipulation? Does the application design ensure the communication between the layers happens via loosely coupled interface components?	
Milestone 3	Not Applicable	

2.2.2. **Data Independence**

ø **Is the application logic 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.
Source	VA Enterprise Target Application Architecture v1.0, Section 5.1.4.5: Separation of Business Logic and Data Logic, p. 99.

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Does the application logic access and manage data via a data access layer or a data access service instead of directly accessing the database?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Is the application logic free from the database implementation details (e.g. data base URLs, internal file formats, schema information)?	System Design Document(SDD) – Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.2.3. **Common Look and Feel**

ø **Does the application user interface follow the enterprise common UI templates and style guidelines?**	
Rationale	The solution should provide user interfaces that have a consistent "look and feel," following enterprise templates and style guidelines.
Source	VA Enterprise Target Application Architecture v1.0, Section 4.1.2.1.2: End-User Interface, p. 51.

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the enterprise templates and style guidelines for the user interfaces applicable to the application type (Web/Rich-Internet Application	System Design Document(SDD) – Interface Design Rules (section 8.1); Project Management Plan –

[3] Appendix – B Glossary #3

	(RIA)/Portal/Mobile)?	Testing (section 11)
Milestone 2	Have the applicable enterprise conventions and standards been applied in the design of the user interface(s)?	System Design Document(SDD) – Overview of the Technical Requirements (section 2.5.4)
Milestone 3	Not Applicable	

2.2.4. **Data Persistence**

ø **Is the data used by the solution stored on enterprise servers 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 security, privacy, etc. concerns). It also promotes consistency in how data custodianship is executed and isolates changes to common services when polices are modified.
Source	VA Enterprise Target Application Architecture v1.0, Section 2.1: OIT Architecture Principles, p. 21.

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to ensure the permanent storage of application data will not happen on the end user devices?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Is the transient application data stored temporarily on end user devices via mechanisms like cookies purged periodically or once the user session expires? Is the relational/ non-relational data used by the solution stored on enterprise servers?	System Design Document(SDD) – Data Design (section 5)
Milestone 3	Not Applicable	

2.2.5. **Test Driven Development**

ø **Have unit tests been 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, as well as 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.
Source	VA Enterprise Target Application Architecture: SOA Layer Implementation Guide v0.1, Section 3.1: Architecture Considerations, page 32

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Does the solution leverage the VA recommended unit testing framework? Has required analysis been performed to identify the mock data/implementation of interface components required for unit	System Design Document(SDD) – Conceptual Application Design (section 3.1)

	tests?	
Milestone 2	Have unit tests been defined for all solution functions and publicly exposed methods? Have the designed unit tests been automated to be executed during the build and deployment process?	System Design Document(SDD) – Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.2.6. **Exception Handling**

Ø **Are there procedures in place for communicating and resolving and unhandled exceptions?**	
Rationale	A shared service may encounter usage that was unexpected in its original development. It is not possible to anticipate all potential causes of failure. A generic approach should be used to alert the user to unexpected error conditions, even when the cause cannot be identified or anticipated.
Source	VA Enterprise Target Application Architecture: SOA Layer Implementation Guide, Section 3.1: Architecture Considerations, page 32

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Is there a strategy for processing unhandled exceptions? Is there a strategy for communicating unhandled exceptions to system users? Have unit tests been designed to test unhandled exceptions?	Project Management Plan – Testing (section 11)
Milestone 2	Are there procedures in place for resolving the unhandled exceptions?	System Design Document(SDD) – Software Detailed Design (section 6.2);
Milestone 3	Not Applicable	

2.2.7. **Scalability**

Ø **Is the application designed to scale out (rather than scale up) and designed to operate on a series of loosely coupled commodity platforms?** Ø **Can the application 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) rather than scale up (i.e., run on larger and larger SMP systems).
Source	OIT Release Architecture v1.21, System Availability/Performance: Scalability, page 8

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Is the application designed to scale out (rather than scale up) and designed to operate on a series of loosely coupled commodity platforms?	System Design Document(SDD) – Conceptual Application Design (section 3.1) System Design Document(SDD) – Hardware Detailed Design (section 6.1)

Milestone 2	Can the application scale-out without requiring code changes?	System Design Document(SDD) – Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.2.8. **Stateless Business Logic**

ø **Is the application business logic "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 (via presentation layer) and system interaction (via integration layer using enterprise messaging).
Source	VA Target Enterprise Target Application Architecture SOA Layer Implementation Guide v0.1, Section 2.2: Management Principles, p. 33.

Alignment Context		**Applicability:** PD & OOR PMAS Projects
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to ensure user session information is not stored within the business logic?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Is the application business logic "stateless" (i.e. user session information is not stored within the business logic)?	System Design Document(SDD) – Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.2.9. **Accessibility Requirements**

ø **Does the solution 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 must meet accessibility requirements.
Source	VA Enterprise Target Application Architecture v1.0, Section 4.1.2.1.2: End-User Interface, p. 51.

Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has requirement analysis been performed to identify the applicable Electronic and Information Technology Accessibility (EITA) Standards required for the solution to be in compliance? Is 508 compliance testing included in the test plan?	System Design Document(SDD) – Overview of Significant Functional Requirements (section 2.5.1); Project Management Plan – Testing (section 11)
Milestone 2	Does the solution comply with Electronic and Information Technology Accessibility (EITA) Standards?	System Design Document (SDD) – Overview of the Technical Requirements (section 2.5.4)
Milestone 3	Not Applicable	

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

ø Have all appropriate data standards published by VA EA been adhered to?		
Rationale	The use of common data standards (like NIEM, HL7, LOINC, SNOMED, VIM and HITSP) will foster consistently defined and formatted data elements and sets of data values, and provide enterprise access to more meaningful data.	
Source	OneVA EA Vision and Strategy, Section 2.1: Principle #5 - Seamless Capabilities	
Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has the required analysis and conceptual design been performed to identify the applicable Data Standards?	System Design Document(SDD) – Conceptual Data Design (section 3.2)
Milestone 2	Have the data elements and values been defined and formatted in accordance with the VA EA Data Standards?	System Design Document(SDD) – Data Design (section 5)
Milestone 3	Not Applicable	

2.3.2. Authoritative Information Sources

ø Have authoritative information sources (including user identity data) been 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.	
Source	VA Enterprise Target Application Architecture v1.0, Section 2.2 Data Management Principles, p. 32.	
Alignment Context		**Applicability:** PD, OOR PMAS Projects
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify authoritative information sources? Has the usage of authoritative data and data sources been reviewed and approved by the responsible data stewards?	System Design Document(SDD) – Conceptual Data Design (section 3.1)
Milestone 2	Have authoritative information sources been leveraged for data retrieval and manipulation wherever authoritative sources have been identified by the enterprise?	System Design Document(SDD) – Data Design (section 5)

Milestone 3	Not Applicable	

2.3.3. Enterprise Data Model

ø Has information captured by the proposed solution been syntactically and semantically harmonized with the VA Enterprise Conceptual Data Model (CDM)?	
Rationale	Promote usage of a VA Enterprise Data Model that will identify each "enterprise" entity that contains at least one attribute (data element) that might be of use outside of the system in which it is created or stored. Any data that enters or leaves a system is considered to be data used outside of 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 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.
Source	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.

Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has the required analysis been performed to identify alignment with the VA EA Enterprise Conceptual Data Model (CDM)? 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?	System Design Document(SDD) – Conceptual Data Design (section 3.1)
Milestone 2	Has alignment with the VA EA Enterprise Conceptual Data Model (CDM) been reviewed and approved by the responsible data stewards? Has information captured by the proposed solution been syntactically and semantically harmonized with the VA Conceptual Data Model (CDM)? Has the VA Conceptual Data Model (CDM) been updated with the new enterprise entities introduced by the solution?	System Design Document(SDD) – Data Design (section 5) VA EA Enterprise Conceptual Data Model (CDM)
Milestone 3	Not Applicable	

2.3.4. Local Copies of Authoritative Information Sources

ø Can the solution 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, then permission of the responsible data steward must be obtained for such use. Also, any update to such a copy or 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.
Source	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.

Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS	**Compliance Question**	**Relevant Artifact for**

Universal Milestone		Demonstrating Compliance
Milestone 0	Not Applicable	
Milestone 1	Has the conceptual data design identified the need for using local copies of authoritative data instances? Has approval/authorization been granted to store local copies of authoritative data instances?	System Design Document(SDD) – Conceptual Data Design (section 3.1)
Milestone 2	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?	System Design Document(SDD) – Data Design (section 5)
Milestone 3	Not Applicable	

2.3.5. **Meta Data Registry**

ø **Does the data gathered and generated by this system have its definitions registered in the VA Meta Data registry?**		
Rationale	Metadata registries store the data schemas/domain vocabularies and manage the semantics of data independent of the subject matter area. The metadata registry 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 Meta Data registry to promote harmonization, standardization, use, re-use, and interchange.	
Source	VA Enterprise Target Application Architecture v1.0, Section 4.5.3.2: ESB Functions, p. 72.	
Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the required authoritative data schemas/domain vocabularies in the VA Meta Data registry?	System Design Document(SDD) – Conceptual Data Design (section 3.1)
Milestone 2	Has the authoritative information generated by this system been registered in the VA Meta Data registry?	System Design Document(SDD) – Data Design (section 5)
Milestone 3	Not Applicable	

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**

ø Does the solution 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[4] has the potential to play a major part in improving VA service delivery.	
Source	VA DIRECTIVE 6517, Cloud First Policy	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Has the solution's business model been evaluated to leverage existing cloud computing services or to create new cloud computing services?	Project Charter – Project Dependencies System Design Document (SDD) – Application Locations
Milestone 1	Has the required analysis been performed 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)? 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?	System Design Document (SDD) – System Architecture (section 4)
Milestone 2	Does the VA Network and Security Operations Center (NSOC) evaluate and test the security control requirements and provide recommendations for continuous monitoring, implementation, and maintenance of cloud services?	Operational Acceptance Plan-C&A SMART Status (section 4); System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 3	Does the VA cloud service meet FedRAMP and NIST requirements prior to adoption of the service to ensure compliance and adherence with VA regulatory authority and NIST standards?	Operational Acceptance Plan-C&A SMART Status – Section 4

[4] Appendix – B Glossary #2

2.4.2. **Standard OS Images**

ø **Are end user devices and servers used by the solution configured using the standard system images published in the current VA Release Architecture?**		
Rationale	Reduce complexity by standardizing platforms[5] that include hardware, operating system, middleware, databases and supporting system software. Ensure the solution conforms to the VA Standard Operating Systems.	
Source	OIT Release Architecture v1.21, Platforms, p. 6.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Are end user devices and servers used by the solution configured using the standard system images published in the current VA Release Architecture?	Requirements Specification Document - Applicable Standards (section 3) System Design Document(SDD) – Software Architecture (section 4.2) Operational Acceptance Plan - Physical Support Requirements (section 4), Architecture / Dependencies (section 11)
Milestone 2	Not Applicable	
Milestone 3	Not Applicable	

2.4.3. **Standard Databases**

ø **Are the Relational Databases and Object Oriented Databases published in the current VA Release Architecture sufficient to meet solution needs?**		
Rationale	Reduce complexity by standardizing platforms that include hardware, operating system, middleware, databases and supporting system software. Ensure the solution conforms to the VA Standard Databases.	
Source	OIT Release Architecture v1.21, VistA Platforms, p. 10; Database Products, p. 14.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Will the solution employ database products included in the VA Release Architecture to meet its data requirements?	System Design Document (SDD) – Database Information (Section 3.2.2)
Milestone 2	Not Applicable	
Milestone 3	Not Applicable	

[5] Appendix – B Glossary #9

2.4.4. **Virtualization**

ø **Is the solution designed to be developed and operated in the standard OIT defined virtual environments?**		
Rationale	The solution shall be independent from 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 re-using existing hardware resources. Virtualization provides the ability to run more workloads and provide higher utilization and capitalization on a single server, and facilitates virtual machine mobility without downtime.	
Source	OIT Release Architecture v1.21, Platforms, p. 6. VA Enterprise Target Application Architecture v1.0, Section 1.6: Relevance to Transition to Cloud Computing, p. 17.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Is the solution designed to support virtualization so it can be independent from the underlying hardware?	System Design Document(SDD) – Conceptual Infrastructure Design (section 3.3)
Milestone 2	Is the current solution hosting infrastructure based on the standard OIT defined virtual environments?	System Design Document(SDD) – Detailed Design (section 6)
Milestone 3	Is the system hosted by the standard OIT Virtual Environment?	Operational Acceptance Plan

2.4.5. **Infrastructure Capacity**

ø **Are production capacity requirements 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.	
Source	OIT Release Architecture v1.21. Background p.5	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Have infrastructure capacity requirements been assessed and an infrastructure impact analysis been performed?	Requirements Specification Document - Performance Specifications (section 2.9) System Design Document(SDD) – System Criticality and High Availability (section 3.3.1), Functional Workload and Functional Performance Requirements (section 2.5.2)
Milestone 2	Has appropriate load testing and impact analysis been performed to leverage the VA infrastructure to host the solution?	Operational Acceptance Plan - Physical Support Requirements (section 4), Service Level Requirements (section 8), Architecture / Dependencies

		(section 11)
Milestone 3	Not Applicable	

2.4.6. **Storage**

∅ **Are storage capacity requirements 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.	
Source	OIT Release Architecture v1.21, Storage Capacity, p. 9.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has a detailed storage capacity analysis been conducted and have infrastructure storage capacity requirements been evaluated?	System Design Document(SDD) – Data Design (section 5), Hardware Detailed Design (section 6.1)
Milestone 2	Is the solution storage infrastructure based on the standard OIT storage provisioning model?	Operational Acceptance Plan - Physical Support Requirements (section 4), Service Level Requirements (section 8), Architecture / Dependencies (section 11)
Milestone 3	Not Applicable	

2.4.7. **Network Configurations**

∅ **Is the solution designed to operate within the current VA LAN and WAN network configurations?**		
Rationale	The network should be able to support connectivity (latency and bandwidth) requirements of the solution in establishing internal and external communications with VA Data Centers, VA Medical Centers, Community-Based Outpatient Clinics (CBOC) and VA Facilities. Also, remote management of the solution must be incorporated into the overall system design.	
Source	OIT Release Architecture v1.21, Network, p. 10.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Is the solution designed to operate within the current VA LAN and WAN network configurations?	System Design Document(SDD) – Communications Detailed Design (section 6.3), External Interface Design (section 7)
Milestone 2	Have the current VA LAN and WAN configurations been evaluated against the solution's planned network traffic profile?	Operational Acceptance Plan Physical Support Requirements (section 4), Service Level Requirements (section 8)
Milestone 3	Not Applicable	

2.4.8. **System Monitoring**

ø **Does the deployment environment meet the performance and downtime monitoring requirements of the solution?**		
Rationale	Ensure the solution is monitored vigilantly. 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.	
Source	OIT Release Architecture v1.21, Instrumentation/Monitoring Products, p. 14	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Have the reliability and availability requirements been assessed and evaluated with respect to infrastructure capabilities for continuous monitoring?	Requirements Specification Document - Reliability Specifications (section 2.11) System Design Document(SDD) – System Criticality and High Availability Requirements (2.5.6), System Criticality and High Availability (section 3.3.1.)
Milestone 2	Does the deployment environment meet the performance and downtime monitoring requirements of the solution?	Operational Acceptance Plan - Physical Support Requirements (section 4), Service Level Requirements (section 8)
Milestone 3	Not Applicable	

2.4.9. **Disaster Recovery**

ø **Has a disaster recovery plan been developed and provisioned?** ø **Are critical infrastructure components (including Data) located at multiple (physical) locations?**		
Rationale	Disaster Recovery (DR) is 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 Disaster Recovery 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 in the same area.	
Source	OIT Release Architecture v1.21, System Availability, p. 8.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Have the disaster recovery requirements been assessed and evaluated with respect to infrastructure capabilities? Have Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) been defined and approved?	Requirements Specification Document - Disaster Recovery Specifications (section 2.4) System Design Document(SDD) – System Criticality and High Availability Requirements (2.5.6),

		System Criticality and High Availability (section 3.3.1)
Milestone 2	Does the disaster recovery plan maximize use of OI&T infrastructure capabilities?	Operational Acceptance Plan Physical Support Requirements (section 4), Service Level Requirements (section 8)
Milestone 3	Not Applicable	

2.4.10. **Backup & Restore**

ø **Will the backup and restore solution meet data recovery requirements (Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO))?**		
Rationale	Infrastructure users help to determine the amount or the period of data that is needed to backup and the amount of data needed to restore. Recovery requirements help to determine the backup and restore capabilities.	
Source	OIT Release Architecture v1.21, Storage Technologies, p. 9.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Have the archival, backup and restore requirements been assessed and evaluated with respect to infrastructure capabilities? Does the application need to be paused or altered during the run process in order to guarantee a consistent and usable backup? Have Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) been defined and approved? Does data need to be extracted from the system and moved to long term archival at any point in the data lifecycle?	Requirements Specification Document - Disaster Recovery Specifications (section 2.4.) System Design Document(SDD) – System Criticality and High Availability Requirements (2.5.6), System Criticality and High Availability (section 3.3.1.)
Milestone 2	Does the backup and restore plan maximize use of OI&T infrastructure capabilities? Does the security of data backups comply with VA requirements?	Operational Acceptance Plan Physical Support Requirements (section 4), Service Level Requirements (section 8)
Milestone 3	Not Applicable	

2.4.11. **Thin Client**

ø **Is the solution either browser or "thin client" based?**	
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 like the need for device integration where an applet like 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[6] technology is cited in the source. See the TRM for browser standards.
Source	OIT Release Architecture v1.21, Client, p. 11. VA Enterprise Target Application Architecture v1.0, Section 2.1: OIT Architecture Principles, p 21.

Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	If the solution is thin client based: Does it use the standard thin client technologies? Can the solution run on the VA standard browsers? If the solution is a mobile device based: Has required analysis been performed to design the solution using device agnostic mobile frameworks like HTML5, CSS3? Can it run on VA Standard Mobile Images?	Operational Acceptance Plan - Architecture / Dependencies (section 11)
Milestone 2	Is the user interface designed with device and browser independent technologies like HTML (XHTML, HTML5), CSS and JavaScript?	
Milestone 3	Not Applicable	

[6] Appendix – B Glossary #13

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

ø Have all applicable Information Security rules been adhered to?		
Rationale	Ensure the solution adheres to and is in compliance with established Federal laws and regulations as per the policy provided in The Department of Veterans Affairs (VA) Policy 6500, Handbook 6500, and other 6500 appendices.	
Source	Information Security Program - VA Directive and Handbook 6500, Section 3: Utilization of This Handbook and Appendices, p. 7.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Has the solution identified all potential information security and privacy vulnerabilities that will need to be addressed? Will this solution be included in another application's C&A and privacy documentation?	Requirements Specification Document (RSD) - Security Specifications (Section 2.13); System Design Document(SDD) – Overview of the Security or Privacy Requirements (section 2.5.5); System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 1	Has the required security and privacy documentation been developed and approved?	Risk Log Requirements Specification Document (RSD) - Security Specifications (Section 2.13); System Design Document(SDD) – Overview of the Security or Privacy Requirements (section 2.5.5); System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 2	Has the solution passed Certification and Accreditation?	Operational Acceptance Plan-C&A SMART Status (Section 3)
Milestone 3	Not Applicable	

2.5.2. **External Hosting**

ø **If hosting externally, have all guidelines for using commercial partners been followed?**		
Rationale	Ensure the solution follows the external hosting guidelines and VA security policy for using such hosted solutions	
Source	OIT Release Architecture v1.21, p. 4. VA Information Security Reference Guide v1.0 – External Information Services (Section SA-9), p. 103.	
Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	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?	Requirements Specification Document (RSD) - Security Specifications (Section 2.13); System Design Document(SDD) – Overview of the Security or Privacy Requirements (section 2.5.5);
Milestone 1	Have all guidelines for using commercial partners been communicated to the hosting provider?	Operational Acceptance Plan-C&A SMART Status (Section 3); Operational Acceptance Plan - Anomaly / Risk Summary (section 12)
Milestone 2	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 web site 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?	Operational Acceptance Plan-C&A SMART Status (Section 3); Operational Acceptance Plan - Anomaly / Risk Summary (section 12)
Milestone 3	Not Applicable	

2.5.3. **Secure Access Paths**

ø **Are established secure access paths followed for application and database access?**		
Rationale	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 which bypass VA security infrastructure.	
Source	VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Architecture Application Principles, p. 35. VA Information Security Reference Guide v1.0 – Access Control Policy & Procedures (Section AC-1), p. 15. VA Handbook 6500 - External Business Partner Connections, p.66.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Are access controls being planned that ensure that only authorized individuals gain access to information system resources, are	System Design Document (SDD) – System Integrity Controls

	assigned an appropriate level of privilege, and are individually accountable for their actions? For moderate and high-impact systems, are there plans to ensure that the flow of information between endpoints (i.e., via Interconnection Agreements, Site to Site Connections, or Business Partner Gateways (BPGs)) is appropriate?	(section 9)
Milestone 2	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? Do moderate and high-impact systems validate and ensure that the flow of information between endpoints is appropriate, documented, and has been approved by the designated officials? Are data communication pathways from VA facilities to non-VA business partners that cannot pass through the One-VA Internet gateways fully documented and have the ISO approvals? Are these connections managed and coordinated with and by the VA NSOC?	System Design Document (SDD) – System Integrity Controls (section 9) Operational Acceptance Plan - Architecture / Dependencies (Section 11) System Design Document (DSS) – Interface Detailed Design (section 7.2)
Milestone 3	Not Applicable	

2.5.4. **Secure Information Sharing**

ø **Does the solution document specific reasons for all limited, external access to data, including the need to know along with security, privacy or other legal restrictions?**	
Rationale	The solution should follow Secure information sharing guidelines; Information shall be "shared by rule and withheld by exception" with all authorized users with a need to know.
Source	VA Enterprise Target Application Architecture v1.0, Section 2.1: OIT Architecture Principles, p. 28.

Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Will the solution employ automated audit logs for external data access?	Requirements Specification Document (RSD) - Security Specifications (Section 2.13) System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 2	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?	System Design Document(SDD) – Overview of the Security or Privacy Requirements (section 2.5.5); System Design Document (SDD) – System Integrity Controls (section 9) Operational Acceptance Plan - Anomaly / Risk Summary (section

	Will audit logs be sufficient in 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?	12)
Milestone 3	Are operational procedures in place to ensure audit logs are reviewed periodically for action?	Operational Acceptance Plan - Anomaly / Risk Summary (section 12)

2.5.5. **PII & PHI**

Ø Have appropriate controls been implemented to prevent the unwarranted disclosure of sensitive, or Personally Identifiable Information (PII) or Protected Health Information (PHI)?	
Rationale	The solution should ensure all access to Personally Identifiable Information (PII) and Personal Health Information (PHI) is logged and subjected to audits. Ensure appropriate controls are implemented and enforced to prevent storing sensitive, or Personally Identifiable Information (PII) or Protected Health Information (PHI) in exception messages, log files or persistent cookies.
Source	VA Enterprise Target Application Architecture v1.0, Section 2.1: OIT Architecture Principles, p. 29.

Alignment Context		**Applicability: Applicable to PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the Personally Identifiable Information (PII) or Protected Health Information (PHI) the solution needs to handle? If the solution handles PII or PHI, Can the solution log the details of the access of Personally Identifiable Information (PII) and Personal Health Information (PHI)?	System Design Document (SDD) – Overview of the Security or Privacy Requirements (Section 2.5.5)
Milestone 2	If the solution handles PII or PHI, Does the solution 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, or Personally Identifiable Information (PII) or Protected Health Information (PHI) in exception messages, log files or persistent cookies?	System Design Document (SDD) – Overview of the Security or Privacy Requirements (Section 2.5.5)
Milestone 3	If the solution handles PII or PHI, Are operational procedures in place to ensure audit logs of access to PII and PHI data reviewed periodically for action?	Operational Acceptance Plan - Anomaly / Risk Summary (section 12)

2.5.6. **HSPD-12**

ø **Has the solution been smart-card 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 employees' and contractors' 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.	
Source	OMB M11-11: HSPD-12 Directive	
Alignment Context		**Applicability: PD, OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the solution's readiness to handle logical logon based on Personal Identity Verification (PIV) cards?	System Design Document (SDD) – Overview of the Security or Privacy Requirements (Section 2.5.5); System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 2	Has the solution been smart-card enabled to handle logical logon of the internal VA users using Public Key Infrastructure (PKI)?	System Design Document (SDD) – System Integrity Controls (section 9)
Milestone 3	Not Applicable	

2.6. Enterprise Services

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. System Integration

ø Are all system interfaces (both external and internal) used by the solution integrated as services based on open standards (SOAP/REST/JMS/MQ/SFTP) and standard message formats (NIEM/HL7/EDIFACT)?		
Rationale	Ensure Solution access from other systems is permitted only via the VA provided infrastructure (i.e. through service requests mediated by the Enterprise Service Bus (ESB) and based on Service Oriented Architecture (SOA)[7] principles and standards.	
Source	VA Enterprise Target Application Architecture v1.0, Section 5.6.4.3: Format Harmonization, p. 109.	
Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the application interfaces required for system integration?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Are the system interfaces (both external and internal) designed based on open standards (SOAP/REST/JMS/MQ/SFTP) and standard message formats (NIEM/HL7/EDIFACT) rather than on proprietary protocols and/or custom built message formats?	System Design Document(SDD) – External Interface Design (section 7) and Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.6.2. Service Registry

ø Does the application leverage existing services published in the VA services registry?	
Rationale	Ensure usage of Enterprise Shared Services 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 re-use by the enterprise and application. Development efforts should re-use registered services.
Source	OMB Shared First Policy VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Application Architecture Principles, p. 34.

[7] Appendix – B Glossary #12

Alignment Context		Applicability: PD & OOR PMAS Projects
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to leverage applicable Shared Enterprise Services in the VA Service Registry?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Have the services introduced/upgraded by the solution been published in the VA service registry?	VA Service Registry
Milestone 3	Not Applicable	

2.6.3. **Shared Enterprise Services**

Ø Does the solution utilize Core Common Business Services and Core Common Infrastructure Services rather than developing local services?	
Rationale	Ensure usage of Enterprise Shared Services 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. Leveraging cross-cutting services save effort and leads to consistent and reliable execution of common capabilities (i.e., security, auditing, logging, exception management). These shared application components can be the focus of implementing policy changes rather burdening all application projects which require them.
Source	OMB Shared First Policy VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Application Architecture Principles, p. 34.

Alignment Context		Applicability: All PMAS Projects
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to eliminate development of local services duplicative of existing services defined in the VA services registry?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Does the solution utilize Core Common Business Services and Core Common Infrastructure Services rather than developing local services?	System Design Document(SDD) – External Interface Design (section 7) and Software Detailed Design (section 6.2) VA Services Registry
Milestone 3	Not Applicable	

2.6.4. **Identity and Access Management (IAM) Service**

Ø Does the solution utilize the Enterprise Identity and Access Management (IAM) Service?		
Rationale	The Federal Identity, Credential, and Access Management (FICAM) Roadmap details additional rationale 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.	
Source	OMB Shared First Policy VA Enterprise Target Application Architecture v1.0, Section 2.3: Enterprise Application Architecture Principles, p. 35.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Do the business requirements include identity and access management aspects (i.e. managing person identity, compliance, customer self-service, authenticating users, and enforcing entitlement/access decisions) which enable adequate integration of the solution with the IAM capabilities?	Business Requirements Document (BRD); Draft Requirements Specification Document(RSD) section 2.4 – Security Specifications
Milestone 1	Has the required analysis been performed to leverage Enterprise Identity and Access Management (IAM) capabilities for the solution's authentication, authorization, and auditing needs?	System Design Document(SDD) – Conceptual Application Design (section 3.1)
Milestone 2	Does the solution utilize the Enterprise Identity and Access Management Service (IAM)? If the required IAM capabilities are not leveraged, Has IAM team been communicated the reasons for not leveraging IAM offered capabilities?	System Design Document(SDD) – External Interface Design (section 7) and Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.6.5. **VLER Information Services**

ø Does the solution utilize available VLER information services?		
Rationale	The purpose of VLER is to enable VA and its partners to provide the full continuum of services and benefits to veterans through veteran centric processes made possible by effective, efficient and secure standards-based information sharing. The solution MUST enable the development and usage of VLER information services wherever applicable.	
Source	VLER XML Schema Directive	
Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the available VLER Information Services required for the solution? Has required analysis been performed to identify and facilitate development of new VLER information Services?	System Design Document(SDD) – Application Context (section 3.1.1)
Milestone 2	Does the solution use VLER information services rather than	System Design Document(SDD) –

	accessing the related data stores directly?	External Interface Design (section 7) and Software Detailed Design (section 6.2)
Milestone 3	Have the new VLER Information Services developed as part of this solution been published in the VA Service Registry?	VA Services Registry

2.6.6. **Service Enabled Information Sharing**

ø **Is enterprise information used by this solution available through services?**		
Rationale	The goal is to disallow development of monolithic systems. The solution needs to share the business functionality for enterprise usage via service[8] enabled design. Re-using enterprise level services and making application services available to the enterprise saves money and resources. It also promotes continuity in processing.	
Source	VA Enterprise Target Application Architecture v1.0, Section 2.3. Enterprise Application Architecture Principles, p. 34.	
Alignment Context		**Applicability: PD & OOR PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to identify the available Shared Enterprise Services required for the solution in the VA Service Registry?	System Design Document(SDD) – Application Context (section 3.1.1); System Design Document(SDD) – Data Design (section 5) VA Service Registry
Milestone 2	Is enterprise information used and produced by this solution available through services? Are all services that are part of this system registered in the VA services registry and discoverable through the VA services portal?	System Design Document(SDD) – External Interface Design (section 7) and Software Detailed Design (section 6.2)
Milestone 3	Not Applicable	

2.6.7. **Technical Reference Model**

ø **Are all Products and Standards used by the solution listed and identified as permissible for usage in the VA Technical Reference Model (TRM)?**		
Rationale	Ensure the solution adheres to VA approved standards and products. Leverage of IT investments, implementation of an integrated technology framework (Clinger-Cohen Act)	
Context	Applicable to PD, OOR PMAS Projects	
Source	VA TRM	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Has required analysis been performed to determine that the solution will be supported by the permissible products and	Operational Acceptance Plan - Electronic Inventory List and Asset

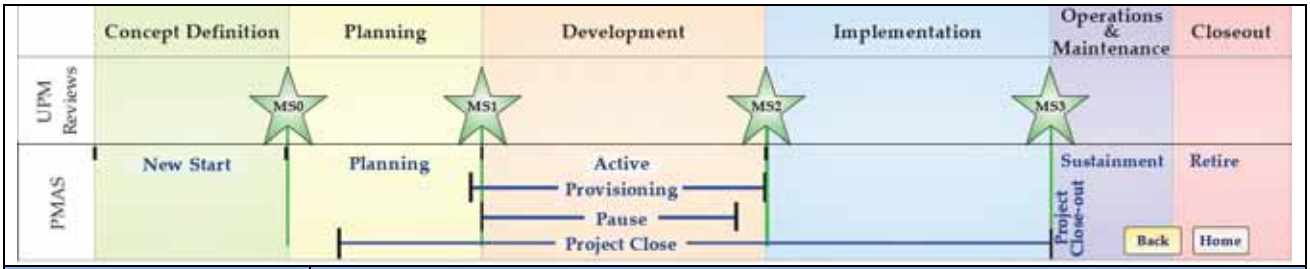
[8] Appendix – B Glossary #11

	standards in TRM?	Management (section 7) VA TRM
Milestone 2	If the project needs new products that are not in the TRM, 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? Has a life-cycle cost estimate been performed for the candidate technologies? Have common cost-savings practices been taken into consideration for avoidance of additions to the TRM?	Product Evaluation and Decision Analysis
Milestone 3	Has a determination been made to retire older products from the TRM that were replaced by the new products?	VA TRM

2.6.8. **COTS Products**

ø **Are all COTS products used in the solution 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 commercial off-the-shelf (COTS) products used in the solution are supported by the vendor across the VA enterprise over its full life cycle until it is removed from VA service.	
Source	VA Enterprise Target Application Architecture v1.0, Section 2.1: OIT Architecture Principles, p. 25.	
Alignment Context		**Applicability: All PMAS Projects**
PMAS Universal Milestone	**Compliance Question**	**Relevant Artifact for Demonstrating Compliance**
Milestone 0	Not Applicable	
Milestone 1	Is the vendor company stable and likely to remain so to support the COTS product as long as VA needs it?	Product Evaluation and Decision Analysis
Milestone 2	Are all IT products on the National Information Assurance Program (NIAP) Validated Product List (VPL) or have been accepted for NIAP evaluation? 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)? Does custom code interact with COTS products only through vendor supplied Application Program Interfaces (APIs) or interfaces that the vendor guarantees will be supported through future versions? 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?	Product Evaluation and Decision Analysis System Design Document (SDD) – Software Detailed Design (Section 6.2)
Milestone 3	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 would have a copy of the source code as a basis for future maintenance efforts?	

Appendix A – PMAS Milestone Artifacts



PMAS States	Artifact
New Start	Project Charter Business Requirements Document (BRD)
Planning	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)
Provisioning	Contract Award (VOA) Updates to MS1 documents
Active	Success Criteria Customer Acceptance Form IPT Charter Updates to MS1 documents

Appendix B – Glossary

This subsection describes the critical terms used in support of the development of this document and critical to the comprehension of its content.

1. **Business Logic layer** [10]: 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's typically composed of components which are exposed as service interfaces.

2. **Cloud computing** [2]: 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.

3. **Data Access Layer** [10]: 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.

4. **Enterprise Service** [12]: 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).

5. **Enterprise Technical Architecture**: The Enterprise Technical Architecture (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** [5]: 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** [9]: Information sharing is making information available to participants (people, processes or systems). It includes the cultural, managerial and technical behaviours by which one participant leverages information held or created by another.

8. **Middleware** [7]: In a distributed computing system, middleware is defined as the software layer that lies between the operating system and the applications on each site of the system.

9. **Platform** [6]: A computing platform includes a hardware architecture and a software framework (including application frameworks), where the combination allows software, particularly application software, to run.

10. **Presentation Layer** [10]: 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

11. **Service** [4]: 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.

12. **Service Oriented Architecture** [4]: A paradigm for organizing and utilizing 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.

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 - Acronyms and Abbreviations

Table 2 – List of Acronyms and Abbreviations used in this document

Acronym	Definition
ASD	Architecture, Strategy and Design
API	Application Programming Interface
C&A	Certification and Accreditation
COTS	Commercially available Off-The-Shelf
DNS	Domain Name System
EDW	Enterprise Data Warehouse
ESB	Enterprise Service Bus
ETA	Enterprise Technical Architecture
HA	High Availability
HITSP	Healthcare Information Technology Standards Panel
HL7	Health Level 7 International
HTTP	Hypertext Transfer Protocol
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol
LOINC	Logical Observation Identifiers Names and Codes
MQ	Message Queue
NIEM	National Information Exchange Model
ODS	Operational Data Store
OIT	Office of Information and Technology
OLTP	Online transaction processing
OMB	Office of Management and Budget
OOR	Office of Responsibility
PD	Product Development
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Project Manager
PMAS	Project Management Accountability System
PMP	Project Management Plan
ROM	Rough Order of Magnitude
RSD	Requirements Specification Document
SD&E	Service Delivery and Engineering
SDD	System Design Document
SDLC	System Development Life Cycle
SNOMED	Systematized Nomenclature of Medicine
SOA	Service Oriented Architecture
VA	Department of Veterans Affairs
VIM	Veteran Information Model

References

[1] Technical Standard, Service-Oriented Architecture Ontology, Document Number: C104, The Open Group 2010
[2] The NIST Definition of Cloud Computing - SP 800-145
[3] IEEE Standard Glossary of Software Engineering Terminology, IEEE Standards Board
[4] OASIS SOA Reference Model
[5] Information Technology Infrastructure Library (ITIL) v3 Glossary v3.1.24
[6] Wikipedia - Computing Platform
[7] ObjectWeb.org - What is Middleware?
[8] Federal Standard 1037C
[9] DoD Info Sharing Strategy
[10] Microsoft Application Architecture 2nd Edition - Patterns & Practices
[11] SOA Glossary, Definitions for Service-Oriented Computing Terms, Thomas Erl
[12] FSAM/OMB FEA Practice Guidance
[13] W3C: Web Services Glossary