

**Military Health System (MHS)  
Enterprise Architecture  
Compliance Assessment Framework (EACAF)  
for Defense Business Information  
Technology Certification (DBITC)  
Guidebook**



**Version 1.0**

**November 04, 2010**

## Document Change Record Control

Version Number	Date	Description
1.0	4 November 2010	Initial Release

# TABLE OF CONTENTS

<b>SUMMARY OVERVIEW .....</b>	<b>1</b>
<b>1. INTRODUCTION.....</b>	<b>2</b>
1.1 IDENTIFICATION .....	2
1.2 AUDIENCE .....	2
1.3 PURPOSE.....	2
1.4 ASSUMPTIONS.....	3
1.5 EXPECTED OUTCOMES .....	3
<b>2. ARCHITECTURE AND REGULATORY COMPLIANCE GUIDANCE.....</b>	<b>4</b>
2.1 DOD ARCHITECTURE GUIDANCE .....	4
2.2 BUSINESS ENTERPRISE ARCHITECTURE GUIDANCE.....	4
2.3 DOD NET-CENTRIC GUIDANCE.....	5
2.4 DOD CAPABILITY LIFECYCLE GUIDANCE.....	6
<b>3. MHS ENTERPRISE ARCHITECTURE COMPLIANCE OVERVIEW.....</b>	<b>8</b>
3.1 EA COMPLIANCE REVIEW PROCESS .....	8
3.2 ROLES AND RESPONSIBILITIES .....	9
3.3 EA COMPLIANCE ASSESSMENT APPROACH .....	9
3.4 EA COMPLIANCE FOCUS AREAS.....	10
<b>4. ARCHITECTURE ARTIFACTS.....</b>	<b>12</b>
4.1 ARCHITECTURE ARTIFACT GUIDANCE.....	12
4.2 REQUIRED ARCHITECTURE ARTIFACTS.....	13
4.3 REQUIRED ARCHITECTURE ARTIFACTS FOR TIER 4 INVESTMENTS AND CONCEPT DEVELOPMENT PROGRAMS.....	15
4.4 CONDITIONAL ARCHITECTURE ARTIFACTS .....	16
<b>5. MHS EACAF USER GUIDE .....</b>	<b>18</b>
5.1 EACAF COMPONENTS .....	18
5.2 QUESTIONNAIRE .....	18
5.3 SUMMARY REPORT .....	24
<b>6. ARCHITECTURE ASSESSMENT GUIDANCE .....</b>	<b>25</b>
6.1 CERTIFICATION PACKAGE CHECKLIST.....	25
6.2 BUSINESS PRIORITY .....	26
6.3 CONSISTENCY WITH MHS ENTERPRISE MODELING STANDARDS .....	27
6.4 COMPLIANCE WITH APPLICABLE LAWS, REGULATIONS AND POLICIES.....	31
6.5 COMPLIANCE WITH MHS TECHNOLOGY STANDARDS .....	32
6.6 COMPLIANCE WITH EXTERNAL ARCHITECTURE REQUIREMENTS .....	34
6.7 GENERAL DOCUMENTATION CONSISTENCY.....	36
<b>7. ACRONYMS.....</b>	<b>38</b>

## **SUMMARY OVERVIEW**

The Enterprise Architecture Compliance Assessment Framework (EACAF) has been developed to support the MHS Defense Business Information Technology Certification (DBITC) investment review process and the DBITC annual review process. The EACAF provides MHS OCIO Enterprise Architects the ability to conduct an architecture review of investment certification packages (ICPs) and compliance with enterprise architecture (EA) standards and processes.

The EACAF consists of a guidebook and an EACAF tool that includes a questionnaire and a summary report. The EACAF Guidebook is a reference document that provides guidance as to how to conduct an investment review of submitted architecture artifacts within an ICP.

The EACAF provides an architecture review process for all DHP-funded investments. Guidance is provided specifically to address investment review types and the difference stages in the acquisition lifecycle perspective. The EACAF recommends a set of required and conditional architecture artifacts to be provided by investment owners within certification packages.

The Enterprise Architecture Division (EAD) will implement the EACAF process described herein on the date of approval and release for publication.

# **1. INTRODUCTION**

## **1.1 IDENTIFICATION**

This guidebook is a reference document that is part of the Enterprise Architecture Compliance Assessment Framework (EACAF) Version 1.0, hereafter referred to as “EACAF” or “the framework.” The EACAF is prepared by the MHS EAD in support of the MHS OCIO.

## **1.2 AUDIENCE**

The EACAF is to be used by MHS EAD EA subject matter experts (SMEs) within the MHS investment review process to review an ICP for the MHS Information Management/ Information Technology portfolio, funded by Defense Health Program (DHP). The EACAF provides a structure for the MHS Defense Business Transformation (DBT) Community to review architecture artifacts within ICPs for development and sustainment programs. The EACAF allows MHS EAD EA SMEs to conduct certification reviews of architecture artifacts within the DBITC process and coordinate with external stakeholders, such as Department of Defense (DoD) component organizations and the Business Transformation Agency (BTA).

## **1.3 PURPOSE**

The purpose of the EACAF is to provide a repeatable architecture assessment and compliance process during the investment review cycle, utilizing a well-documented set of guidance and requirements. Where applicable, the framework leverages existing MHS investment compliance materials for the review process. The framework provides a defined set of criteria and questions for evaluating prospective MHS investments undergoing the DBITC process, and also provides guidance with regard to required and conditional architecture artifacts.

The requirements for developing the EACAF are the following:

1. Develop an evaluation tool that is robust, reliable and reusable. The tool must adequately describe assessment requirements and scope of the evaluation.
2. Develop a tool that clearly evaluates the scope of an IT investment against relevant EA requirements and evaluates/articulates how an investment supports MHS strategic priorities and mission outcomes.
3. Utilize and incorporate the latest feedback from the MHS community and program stakeholders in the assessment of the investment package.
4. Achieve a greater level of investment compliance by meeting DBITC requirements set forth by DoD and Office of Management and Budget (OMB).

The EACAF allows the MHS investment community to enhance the overall quality and methodology of the certification process as it is placed in the investment certification review process. The framework promotes active engagement and collaboration among Portfolio Management (PfM) colleagues, enterprise and solution architects, investment owners and other relevant stakeholders.

## 1.4 ASSUMPTIONS

The following EACAF assumptions provide context for usage of the framework and its role within the investment review process.

1. The framework is based on the current DoD and federal laws, regulations and policies. It is understood that compliance requirements are ever changing and an iterative process is necessary to integrate new compliance requirements into the framework.
2. The framework is aligned with the MHS DBITC User Manual v3.0 and provides guidance specific to EA compliance.
3. The use of the framework is for the evaluation of all DHP funded investments, regardless of whether investments are centrally-managed by an MHS Program Office, are part of TMA, or are initiated by a Military Service organization.
4. The framework is designed for use within the investment review process, regardless of whether the process is for annual review, certification or re-certification.
5. The framework assumes MHS EAD EA SMEs have a fundamental knowledge of DoD EA principles and DoD acquisition knowledge with regard to information technology investments and acquisition lifecycle.

## 1.5 EXPECTED OUTCOMES

The adoption of the EACAF provides the following core outcomes:

1. Provides a structured and standardized approach to conducting EA due diligence within the information technology certification process.
2. Ensures that architecture requirements for investments are well documented and are aligned with MHS mission objectives and enterprise standards.

## 2. ARCHITECTURE AND REGULATORY COMPLIANCE GUIDANCE

The following section provides EA compliance guidance references relevant for defense business certification. Each of these references has been provided to address adherence to investment certification, alignment with DoD business architecture requirements, traceability of architecture artifacts and compliance with the acquisition lifecycle.

### 2.1 DOD ARCHITECTURE GUIDANCE

#### **Department of Defense Architecture Framework Version 2.0 (DoDAF v2.0)**

DoDAF v2.0 is the prescribed framework for DoD and all component organizations. It serves as an overarching, comprehensive framework and conceptual model enabling the development of EA artifacts that can be leveraged for better information sharing across program boundaries.

Investment packages are expected to provide architecture information and meet DoDAF v2.0 specifications for the MHS DBITC review. It is understood that DoDAF v2.0 presents a significant shift in the approach to preparing architecture artifacts from previous framework versions, such as Version 1.5. EA tools such as IBM System Architect are just releasing tool usage to address new DoDAF v2.0 viewpoints.

DoDAF v2.0 documentation can be obtained within the DoD Chief Information Officer's site. A DoDAF 2.0.pdf is produced periodically and can be downloaded here:

[http://cio-nii.defense.gov/sites/dodaf20/products/DoDAF\\_v2-01\\_web.pdf](http://cio-nii.defense.gov/sites/dodaf20/products/DoDAF_v2-01_web.pdf)

#### **DoD CIO Memorandum, DoD IT Portfolio Registry (DITPR) and DoD Secret Internet Protocol Router (SIPRNET) IT Registry Guidance, August 10, 2009**

- The DoD DITPR and DoD SIPRNET IT Registry Guidance provides guidance to ensure each Component CIO registers all IT and National Security Systems in DITPR or SIPRNET registry and updates system information on an annual basis.

<http://www.doncio.navy.mil/Download.aspx?AttachID=1315>

### 2.2 BUSINESS ENTERPRISE ARCHITECTURE GUIDANCE

#### **BEA Architecture Product Guide**

The Business Enterprise Architecture (BEA) Architecture Product Guide is a document currently available from the BTA site and applies to the DoD business domain. MHS aligns to the DoD Human Resources domain which is one of the domains within the DoD Business Mission Area (BMA).

For the MHS DBITC review, the BEA Architecture Product Guide can be used as a reference, as BEA v7.0 provides a full set of artifact specifications including new viewpoints provided by DoDAF v2.0.

The BEA Architecture Product Guide can be obtained within the DoD BTA site listed here:

[http://www.bta.mil/products/BEA\\_7\\_0/BEA/html\\_files/apg.html](http://www.bta.mil/products/BEA_7_0/BEA/html_files/apg.html)

## **BEA Compliance Guidance**

BEA Compliance Guidance document provides guidance on how to assess Defense Business System (DBS) compliance to the BEA v7.0.

The BEA Compliance Guidance document can be found within the DoD BTA site as listed here:

[http://www.bta.mil/products/bea\\_7\\_0/BEA/products/bea\\_compliance\\_guidance.pdf](http://www.bta.mil/products/bea_7_0/BEA/products/bea_compliance_guidance.pdf)

## **Human Resources Management, HRM EA**

The DoD Human Resources Management (HRM) domain is a part of the DoD BMA, and the MHS is currently part of the HRM domain. The HRM domain provides a full set of EA views that has been prepared to follow the latest guidance by DoDAF v2.0.

The HRM domain EA page can be accessed from the link below:

[https://www.hrm.osd.mil/owa/hrm/pkg\\_hrm.page?id=HRM\\_EA&wgsid=#products](https://www.hrm.osd.mil/owa/hrm/pkg_hrm.page?id=HRM_EA&wgsid=#products)

## **2.3 DOD NET-CENTRIC GUIDANCE**

The following DoD directives, instructions and memorandums are provided as part of the MHS DBITC guidance since these documents ask for a set of architecture artifacts to be prepared by new DoD investment programs, to address DoD net-centric data strategy mandates and interoperability guidelines for information sharing.

**Department of Defense Directive DoDD 4630.05**, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004 (Certified Current as of April 23, 2007)

- Establishes Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and end-to-end operational effectiveness of that exchange.

[www.dtic.mil/whs/directives/corres/pdf/463005p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf)

**Department of Defense Directive DoDD 8320.02**, Data Sharing in a Net-Centric Department of Defense, December 2, 2004 (Certified Current as of April 23, 2007)

- Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG).

[www.dtic.mil/whs/directives/corres/pdf/832002p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf)

**Department of Defense Instruction DoDI 4630.8**, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004

- Implements a capability-focused, effects-based approach to advance interoperability and supportability throughout the DoD and provides a set of core EA artifacts that are necessary for interoperability.

<http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf>

**Chairman of the Joint Chiefs of Staff Instruction CJCSI 6212.01E**, Interoperability and Supportability (I&S) of Information Technology and National Security Systems, March 8, 2006 (Certified Current as of December 15, 2008)

- Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems.

[http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/6212\\_01.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf)

**DoD CIO Memorandum, DoD Information Enterprise Architecture, Version 1.2**, The Department of Defense Information Enterprise Architecture, May 7, 2010 (Certified Current as of May 10, 2010)

- The DoD Information Enterprise Architecture (DoD IEA) provides a common DoD Information Enterprise foundation to support accelerated Department of Defense (DoD) transformation to net-centric operations. It presents the vision of net-centric operations and establishes near-term priorities to address critical barriers that must be overcome in order to achieve the vision.

[http://cio-nii.defense.gov/sites/diea/products/DoD\\_IEA\\_v1\\_2\\_Signed\\_Memo\\_10\\_May\\_2010.pdf](http://cio-nii.defense.gov/sites/diea/products/DoD_IEA_v1_2_Signed_Memo_10_May_2010.pdf)

## 2.4 DOD CAPABILITY LIFECYCLE GUIDANCE

The following primary DoD guidance documents are listed since it is important to align MHS DBITC investments with the DoD acquisition lifecycle process. Investments can be compared based on size of investment, development milestone phase or sustainment and maintenance activities.

**Department of Defense Instruction DoDI 5000.02**, Operation of the Defense Acquisition System, December 8, 2008

- Establishes a flexible management framework for translating capability needs and technology opportunities into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems (AISs).

<http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf>

**Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G, “Joint Capabilities Integration and Development System,” March 1, 2009**

- Establishes the policies for the JCIDS and the procedures supporting the Chairman of the Joint Chiefs of Staff Joint Requirements Oversight Council (JROC) that identify and assess joint military capability needs as specified by milestone documentation.

[www.dtic.mil/cjcs\\_directives/cdata/unlimit/3170\\_01.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf)

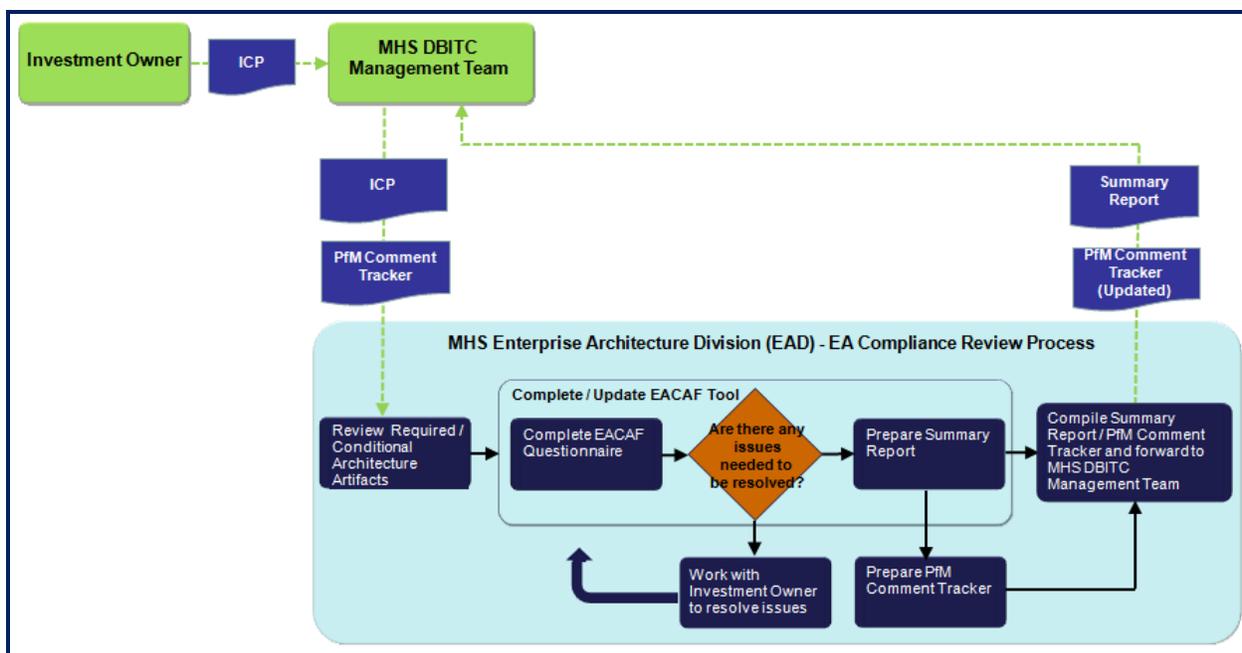
### 3. MHS ENTERPRISE ARCHITECTURE COMPLIANCE OVERVIEW

MHS EA compliance activities address the need for information technology portfolio investments to be reviewed against a set of established criteria and business objectives. The statutory requirement for a modernization architecture is provided within Title 10, Section 2222 that states that all Defense Business Systems must to be in compliance with the organization’s EA.

The EACAF tool provides specific guidance on how to assess, document and communicate the compliance of an investment against a defined set of enterprise criteria. The EACAF is an evolving framework that encourages component reuse, increased interoperability and greater transparency during an EA SME review.

#### 3.1 EA COMPLIANCE REVIEW PROCESS

As depicted in Figure 1 on the following page, the EA compliance review process is initiated once the MHS DBITC Management Team receives an ICP from the DHP funded investment owners (IT business systems Program Managers) and forwards the ICP to the MHS EAD. The MHS EA compliance review process includes a review of submitted architecture artifacts (required and conditional) included in the ICP. The EACAF tool (Questionnaire and Summary Report) creates a repeatable process allowing MHS EAD EA SMEs to review required and conditional architecture artifacts in a consistent manner. The EACAF Tool fosters a structured approach in completing the Questionnaire and preparing evaluation comments identified in the Summary Report. The MHS EAD provides the investment owner with an opportunity to address and resolve issues uncovered during the EA due diligence process. This turnaround process allows most issues to be resolved, prior to the MHS EAD forwarding its comments to the MHS DBITC Management Team.



**Figure 1 – EA SME Review within MHS DBITC Investment Review Process**

### 3.2 ROLES AND RESPONSIBILITIES

The following section provides a core set of roles and responsibilities that are specific to EA compliance review within the MHS DBITC investment review process.

Role	Responsibility
<b>MHS DBITC Management Team</b>	<ul style="list-style-type: none"> <li>• The MHS DBITC Management Team was established with the understanding that people need assistance to navigate through the certification process, to answer questions, to consolidate all comments from SME reviews, to assist with moving the investment package through the process and to generally help individuals focus their activities on preparing a proper investment package for the Pre-Certification Authority (PCA), HRM Investment Review Board (IRB) and Defense Business Systems Management Committee.</li> <li>• Provides assistance in many forms and ensures all inquiries are addressed with clarity, transparency, superior customer service in mind, and ensures accessibility to all.</li> </ul>
<b>DHP Funded Investment Owner (IT business system Program Manager)</b>	<ul style="list-style-type: none"> <li>• Develops the architecture artifacts</li> <li>• Ensures program information is accurately reflected in the submitted architecture artifacts within the ICP</li> <li>• Ensures program information is current within DoD level business system repositories as required by the DoD Networks and Information Integration (DoDNII) policy issuance, DITPR and SIPRNET IT Registry Guidance Memorandum</li> <li>• Ensures architecture artifacts clearly distinguish “as-is” and “to-be” state of the architecture, which the investment will fund.</li> <li>• Identifies if the investment will result in a change of the architecture</li> <li>• Provides verification of completed system review, certification, and approval before obligating funds over \$1M for modernization</li> <li>• Reuses architecture artifacts previously provided through requirements definition process or in acquisition documents and update to reflect the current modernization</li> </ul>
<b>MHS EAD</b>	<ul style="list-style-type: none"> <li>• The MHS EAD provides an EA SME review as part of MHS DBITC investment certification review process by reviewing submitted architecture artifacts within the ICP.</li> </ul>

**Table 1 – Roles and Responsibilities**

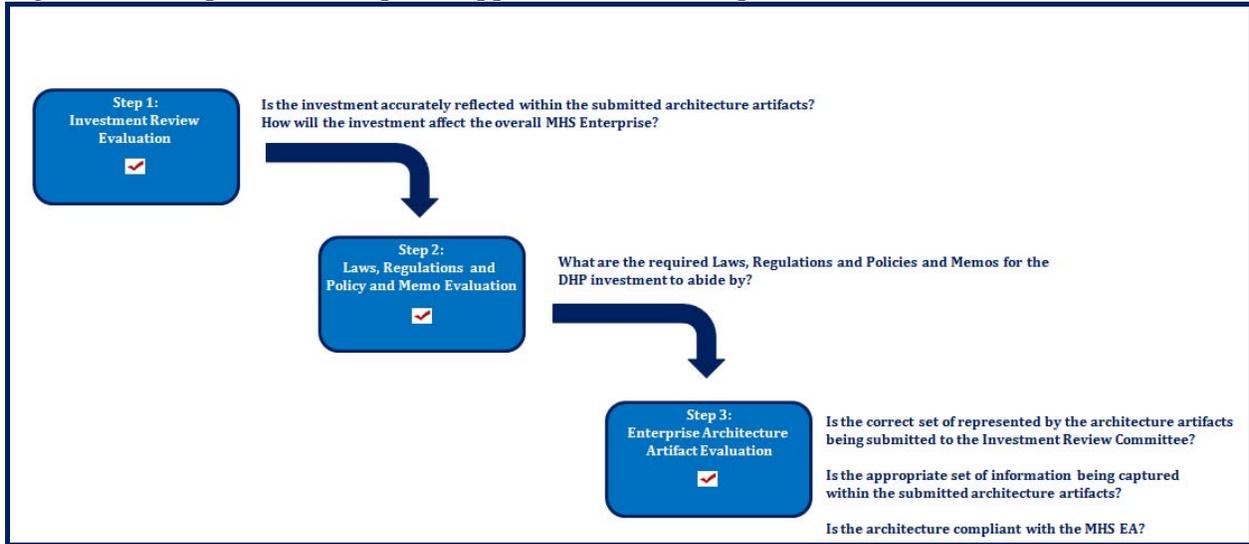
### 3.3 EA COMPLIANCE ASSESSMENT APPROACH

This section provides an understanding of a stepwise process to address key areas of compliance for an investment. EAD architects can assess artifacts based on three evaluation areas:

1. Investment Review Evaluation – assess if the investment is accurately reflected within the given architecture artifacts and how the architecture artifacts affect the overall MHS enterprise.

2. Laws, Regulations and Policy Evaluation – assess how investment abides by applicable laws, regulations and policies.
3. Architecture Artifact Evaluation – assess if appropriate information is captured within architecture artifacts.

Figure 2 below provides a stepwise approach for EA compliance assessment:



**Figure 2 – EA Compliance Assessment Approach**

### 3.4 EA COMPLIANCE FOCUS AREAS

Compliance to EA allows MHS to address its strategic priorities, and coordinate information technology investments with business systems stakeholders. Compliance activities are broad in coverage as it addresses business strategy (meeting mission goals and objectives), business operations (functions, processes, systems), business information (data, metadata), and technology (software, hardware, networks, communications, etc.). To address these concepts and criteria, the EACAF compliance review is outlined into six focus areas.

Focus Area	Description
<b>1. MHS Business Priority</b>	The investment’s business architecture should clearly illustrate how it supports the mission and is line with strategic and enterprise planning activities.
<b>2. Consistency with MHS Enterprise Modeling Standards</b>	The investment should be consistent with MHS Enterprise Modeling Standards for data, activity models and system functions.
<b>3. Compliance with applicable Laws, Regulations and Policies (LRPs)</b>	The investment should illustrate compliance with applicable laws, regulations and policies.
<b>4. Compliance with MHS Technology Standards</b>	Appropriate technology standards need to be identified by the investment package in order to accurately define the system’s technical components.

Focus Area	Description
<b>5. Compliance with External Requirements</b>	MHS investments must meet additional requirements set forth by the BTA (e.g., Standard Financial Information Structure (SFIS) for financial systems) or when MHS systems interface with partner systems (e.g., DoD/VA).
<b>6. General Documentation Consistency</b>	In general, the products included in the ICP should be consistent with each other in terms of describing the investment and system details.

**Table 2 – Compliance Focus Area Description**

## 4. ARCHITECTURE ARTIFACTS

This section provides an understanding of the required and conditional architecture artifacts necessary for DBITC EA compliance. The architecture artifact guidance may be revised as new requirements are received from DoD BTA and HRM IRB. “As-Is” and “To-Be” architecture artifacts are required for architecture views changed by the system modernization.

### 4.1 ARCHITECTURE ARTIFACT GUIDANCE

The following guidance is provided for investment tiers, type of certification, and the phase within the acquisition lifecycle.

#### Investment Tiers

For MHS DBITC review, investments fall under the following Tier definitions.

- **Tier 1** – Includes all Major Automated Information System (MAIS) programs (ACAT 1A, 1AM)
- **Tier 2** – Includes all program investments \$10 million or above
- **Tier 3** – Includes all program investments > \$1 million and < \$10 million
- **Tier 4** – Includes all program investments < \$1 million

#### Architecture artifact guidance based on investment tiers:

Tiers	Artifact Guidance
<b>Tiers 1, 2 and 3</b>	Investment Owners provide a full set of required architecture artifacts and those conditional artifacts identified for specific instances of submission.
<b>Tier 4</b>	Investment Owners provide a full set of required architecture artifacts as defined in Section 4.3, “Required Architecture Artifacts for Tier 4 Investments and Concept Development Programs,” in addition to any other architecture artifacts which the investment owner provides to clarify the investment.

**Table 3 – Architecture Artifact Guidance Based on Investment Tiers**

#### Architecture artifact guidance based on type of certification:

Certification Type	Artifact Guidance
<b>Certification</b>	Investment owners provide a full set of required and conditional architecture artifacts.
<b>Annual Review</b>	As defined in the current MHS DBITC User Manual, the annual review process applies to all systems regardless of the investment Tier, including systems for which there is no further planned development or modernization pending.  Investment Owners provide a full set of required and conditional architecture artifacts to reflect any changes made to the architecture since the previous certification for systems under annual review.

**Table 4 – Architecture Artifact Guidance Based on Type of Certification**

**Architecture artifact guidance based on acquisition lifecycle:**

<b>Lifecycle</b>	<b>Artifact Guidance</b>
<b>Concept development programs</b>	Investment owners provide the full set of required architecture artifacts as defined in Section 4.3, “Required Architecture Artifacts for Tier 4 Investments and Concept Development Programs.”
<b>Development programs / System modernization for programs under sustainment</b>	Investment owners provide the same required and conditional artifacts for development programs and programs undergoing system modernization.

**Table 5: Architecture Artifact Guidance Based on Acquisition Lifecycle**

**4.2 REQUIRED ARCHITECTURE ARTIFACTS**

The following DoDAF-based architecture artifacts are developed by the program offices required for investment certification, annual review and system modernization. “As-Is” and “To-Be” views are required for those architecture artifacts changed by the proposed system modernization.

<b>DoDAF Artifact</b>	<b>Overall Description</b>	<b>Value for Certification Decision Making</b>
<b>AV-1: Overview and Summary Information</b>	Describes a project's vision, goals, objectives, plans, activities, events, conditions, measures, outcomes and produced objects.	Aggregate program briefing and DBS Certification Dashboard information within AV-1 summary to address DoD reporting requirements.
<b>AV-2: Integrated Dictionary</b>	An architectural data repository specific with definitions of terms used in the architectural data and presentations for the ICP.	All program glossaries with specific project definitions and artifact information are collected and placed within an AV-2 dictionary allowing architects to review information for the enterprise.
<b>OV-2 : Operational Resource Flow Description</b>	A description of the resource flows exchanged between operational activities within and between business and system stakeholders.	Provides an illustration and analysis of critical business issues and information communication requirements. This ensures enterprise systems provide the proper communications and content delivery mechanisms.
<b>OV-3 : Operational Resource Flow Matrix</b>	A description of the information exchanged and the relevant attributes of the exchanges.	The OV-3 provides supplemental documentation to the OV-2 to define the business-level message details. An OV-3 matrix table provides specifics on information exchanges requirements.

<b>DoDAF Artifact</b>	<b>Overall Description</b>	<b>Value for Certification Decision Making</b>
<b>OV-5a : Operational Activity Decomposition Tree</b>	The capabilities and activities that are termed as operational activities are organized in a hierarchal structure.	The OV-5a activity model defines scope, business functions and processes, with defined syntax and semantics, logical rigor and consistent interpretation. The OV-5a allows investment owners to trace their activities to the MHS EA enterprise.
<b>OV-6c: Event-Trace Description</b>	The OV-6c model identifies business process activity, and responses to events that are provided in sequence.	The OV-6c documents the “as-is” and “to-be” business processes to receive the obligation of funds when the total cost for a defense business system modernization will be in excess of \$1,000,000, as prescribed in Section 1072 of the FY2010 National Defense Authorization Act (NDAA).  Contact the Deputy Assistant Secretary of Defense for Information Management (DASD (IM)) for additional guidance on BPR assessment requirements.
<b>SV-1 : Systems Interface Description</b>	The identification of systems, system items, and their interconnections.	The SV-1 illustrates system interfaces for the MHS enterprise and integration between operational or system nodes.
<b>SV-4 : Systems Functionality Description</b>	The functions performed by systems and the system data flows among those system functions.	The SV-4 provides a functional decomposition of system functions, which shows the scope and interfaces of the proposed system alignment with the business and the MHS enterprise.
<b>SV-5a : Operational Activity to Systems Function Traceability Matrix</b>	A mapping of system functions or activities back to operational activities or activities.	Ensures the continuity of business analysis and requirements across the operational and systems views. System functions are mapped to the MHS enterprise operational activities.
<b>StdV-1 : Standards Profile</b>	The listing of technical and data standards that apply to the solution elements.	Applicable standards for a system should be included within the StdV-1 artifact for reference to ensure conformance to standards at the MHS enterprise level.
<b>StdV-2 : Standards Forecast</b>	The description of emerging standards and potential impact on current solution elements, within short-term, mid-term and long-term time frames.	Standards are expected to evolve, and the StdV-2 artifact identifies the applicable standards, additions and impacts on the architecture. The StdV-2 forecast should match the timeframes for the associated systems.

**Table 6 – Required Architecture Artifacts**

### 4.3 REQUIRED ARCHITECTURE ARTIFACTS FOR TIER 4 INVESTMENTS AND CONCEPT DEVELOPMENT PROGRAMS

The following architecture artifacts are required for an investment categorized as a Tier 4 or falls under a concept development program in the acquisition lifecycle phase.

The MHS EAD EA SME will evaluate the architecture artifacts based on the architecture content and information captured, rather than the ability to conform to syntactic specifications for DoDAF-based artifacts. The EACAF Tool has not been modified to address the direct needs of Tier 4 or concept development program investments. When the EACAF Questionnaire is used to evaluate a Tier 4 investment or a concept development program, the EAD SME should determine if each question applies to the investment, and then formulate comments based relevance and effect.

DoDAF Artifact	Overall Description	Value for Certification Decision Making
<b>AV-1: Overview and Summary Information</b>	Describes a project's vision, goals, objectives, plans, activities, events, conditions, measures, outcomes, and produced objects.	Aggregate program briefing and DBS Certification Dashboard information within AV-1 summary to address DoD reporting requirements.
<b>OV-2: Operational Resource Flow Description</b>	A description of the resource flows exchanged between operational activities within and between business and system stakeholders.	Provides an illustration and analysis of critical business issues and information communication requirements. This ensures that enterprise systems provide the proper communications and content delivery mechanisms.
<b>OV-5a: Operational Activity Decomposition Tree</b>	The capabilities and activities that are termed as operational activities are organized in a hierarchal structure.	The OV-5a activity model defines scope, business functions and processes, with defined syntax and semantics, logical rigor and consistent interpretation. The OV-5a allows investment owners to trace their activities to the MHS EA enterprise.
<b>SV-1: Systems Interface Description</b>	The identification of systems, system items, and their interconnections.	The SV-1 illustrates system interfaces for the MHS enterprise and integration between operational or system nodes.
<b>StdV-1: Standards Profile</b> (Note: Does not apply to concept development programs)	The listing of technical and data standards that apply to the solution elements.	Applicable standards for a system should be included within the StdV-1 artifact for reference to ensure conformance to standards at the MHS enterprise level.

**Table 7 – Required Architecture Artifacts for Tier 4 Investments and Concept Development Programs**

#### 4.4 CONDITIONAL ARCHITECTURE ARTIFACTS

The following architecture artifacts are conditional to the investment owner based on the conditions that exist for the program at the time of submission. It is an advisory set of artifacts and investment owners should use prudence in determining if these artifacts are needed to describe their current acquisition activity.

DoDAF Artifact	Condition for Usage
<b>OV-1: High Level Operational Concept Graphic</b>	<p>High-level graphical diagram of operational environment of the investment.</p> <p>Program owners should prepare an OV-1 if the operational environment of the investment is significantly different from the MHS enterprise, and if there is a need to illustrate tracing of business functions to the MHS enterprise.</p>
<b>SV-2: Systems Resource Flow Description</b>	<p>A description of communications and messaging resource flows exchanged between systems.</p> <p>Providing an SV-2 is necessary when the investment is documenting infrastructure details. SV-2 provides additional details to an SV-1 interface diagram. Programs should prepare an SV-2 when it is necessary to include the networking and communications infrastructure to the business application.</p>
<b>SV-6: Systems Resource Flow Matrix</b>	<p>Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.</p> <p>SV-6 is a necessary artifact for program owners at critical design review and when the development system is implemented and deployed. As the system is fully defined, it is necessary to illustrate the data exchanges that include critical messages and data loads required in the effective operation of the business.</p>

DoDAF Artifact	Condition for Usage
<p><b>Services Viewpoint</b></p>	<p>The Services Viewpoint is a new set of DoDAF v2.0 models that describes services and their interconnections providing or supporting necessary DoD functions.</p> <p>Services viewpoints should be provided for any investment supporting the development of a Service Oriented Architecture (SOA) environment. Primary artifacts that should be considered to provide a Services view are:</p> <p><b>SvcV-1: Services Context Description</b></p> <p>This provides the identification of services, service items, and their interconnections that correlates to the SV-1 required artifact.</p> <p><b>SvcV-2: Service Resource Flow Description</b></p> <p>This description provides resource flows exchanged between services that correlate to OV-2 and SV-3 artifacts.</p> <p><b>SvcV-4: Services Functionality Description</b></p> <p>This provides the functions performed by services and the service data flows among service functions. It correlates to the SV-4 system functions and OV-2 operational resource flows.</p>

**Table 8 – Conditional Architecture Artifacts**

## 5. MHS EACAF USER GUIDE

### 5.1 EACAF COMPONENTS

Component	Description
1. Questionnaire	The Questionnaire is used by the EA SME to constructively assess the investment artifacts.
2. Summary Report	The Summary Report is used to communicate EA compliance comments to the IRC. The Summary Report may be sent to the Investment Owner for discussion and is used to generate the Summary Report.

**Table 9 – EACAF Components**

### 5.2 QUESTIONNAIRE

The Questionnaire is used by an EA SME to evaluate compliance of an investment, based on the information provided in various required and conditional architecture artifacts provided in the ICP. It enables the EA SME to consistently and thoroughly review the architecture artifacts based on a set of pre-defined questions. This addresses each of the compliance requirements (criteria) of the six (6) focus areas and provides a place for detailed assessment comments. The EA SME will then summarize the assessment comments into the Summary Report and forward it to the MHS DBITC Management Team.

**EA Compliance Assessment Framework (EACAF) Questionnaire**

System Name: \_\_\_\_\_ IRC Date: \_\_\_\_\_

Package Inventory:	Required Architecture Artifacts	Conditional Architecture Artifacts
Legend <div style="display: flex; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">Received</div> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">Not Received</div> </div>	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">AV-1</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">OV-2</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">OV-5a</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">SV-1</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">SV-5a</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">StdV-2</div> </div> <div style="display: flex; flex-wrap: wrap; gap: 5px; margin-top: 5px;"> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">AV-2</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">OV-3</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">OV-6c</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">SV-4</div> <div style="border: 1px solid gray; padding: 2px; background-color: #d9ead3;">StdV-1</div> </div>	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">OV-1</div> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">SV-6</div> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">SvcV-2</div> </div> <div style="display: flex; flex-wrap: wrap; gap: 5px; margin-top: 5px;"> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">SV-2</div> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">SvcV-1</div> <div style="border: 1px solid gray; padding: 2px; background-color: #f4cccc;">SvcV-4</div> </div>

Focus Area	Criteria	ID	Assessment	Guidance Steps	Assessment Comments
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14	Does the investment adhere to applicable laws, regulations and policies?	1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents. 2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary. 3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15	Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment. 2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile. 3. Verify that privacy standards are also included within standards profile.	

**Figure 3: EACAF Questionnaire**

## System Name

The EA SME will identify the system name as listed on the DBS Certification Dashboard included in the ICP.

System Name Section

### EA Compliance Assessment Framework (EACAF) Questionnaire

**System Name:**   IRC Date: \_\_\_\_\_

**Package Inventory:**

Legend

Received

Not Received

**Required Architecture Artifacts**

AV-1	OV-2	OV-5a	SV-1	SV-5a	StdV-2
AV-2	OV-3	OV-6c	SV-4	StdV-1	

**Conditional Architecture Artifacts**

OV-1	SV-6	SvcV-2
SV-2	SvcV-1	SvcV-4

Focus Area	Criteria	ID	Assessment	Guidance Steps	Assessment Comments
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14	Does the investment adhere to applicable laws, regulations and policies?	1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents. 2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary. 3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15	Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment. 2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile. 3. Verify that privacy standards are also included within standards profile.	

**Figure 4: EACAF Questionnaire with System Name Designated**

## Package Inventory Section

The package inventory section provides the EA SME the ability to indicate which architecture artifacts have been included in the ICP for a given investment. The EA SME will use the fill color “green” to represent the submitted architecture artifacts and use the fill color “red” to represent the architecture artifacts that are required but not submitted. Those architecture artifacts whose investments meet conditional requirements will be identified similarly.

**Package Inventory Section**

**EA Compliance Assessment Framework (EACAF) Questionnaire**

System Name:  IRC Date:

**Package Inventory:**

<p><b>Legend</b></p> <div style="border: 1px solid gray; padding: 2px; display: inline-block; background-color: #90EE90; margin-bottom: 2px;">Received</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block; background-color: #FFB6C1; margin-bottom: 2px;">Not Received</div>	<p><b>Required Architecture Artifacts</b></p> <table style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">AV-1</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">OV-2</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">OV-5a</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">SV-1</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">SV-5a</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">StdV-2</td> </tr> <tr> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">AV-2</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">OV-3</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">OV-6c</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">SV-4</td> <td style="border: 1px solid gray; background-color: #90EE90; padding: 2px;">StdV-1</td> <td></td> </tr> </table>	AV-1	OV-2	OV-5a	SV-1	SV-5a	StdV-2	AV-2	OV-3	OV-6c	SV-4	StdV-1		<p><b>Conditional Architecture Artifacts</b></p> <table style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">OV-1</td> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">SV-6</td> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">SvcV-2</td> </tr> <tr> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">SV-2</td> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">SvcV-1</td> <td style="border: 1px solid gray; background-color: #D3D3D3; padding: 2px;">SvcV-4</td> </tr> </table>	OV-1	SV-6	SvcV-2	SV-2	SvcV-1	SvcV-4
AV-1	OV-2	OV-5a	SV-1	SV-5a	StdV-2															
AV-2	OV-3	OV-6c	SV-4	StdV-1																
OV-1	SV-6	SvcV-2																		
SV-2	SvcV-1	SvcV-4																		

Focus Area	Criteria	ID	Assessment	Guidance Steps	Assessment Comments
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14	Does the investment adhere to applicable laws, regulations and policies?	<ol style="list-style-type: none"> <li>1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents.</li> <li>2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> <li>3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> </ol>	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15	Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	<ol style="list-style-type: none"> <li>1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment.</li> <li>2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile.</li> <li>3. Verify that privacy standards are also included within standards profile.</li> </ol>	

**Figure 5 – EACAF Questionnaire with Package Inventory Designated**

## Assessment Section

The EA SME will do his/her due diligence in conducting an assessment of the investment for each criteria of the focus area based on the submitted architecture artifacts.

**Assessment Section**

**EA Compliance Assessment Framework (EACAF) Questionnaire**

System Name:  IRC Date:

**Package Inventory:**

Legend

Received

Not Received

**Required Architecture Artifacts**

AV-1

OV-2

OV-5a

SV-1

SV-5a

StdV-2

AV-2

OV-3

OV-6c

SV-4

StdV-1

**Conditional Architecture Artifacts**

OV-1

SV-6

SvcV-2

SV-2

SvcV-1

SvcV-4

Focus Area	Criteria	Assessment	Guidance Steps	Assessment Comments	
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14	Does the investment adhere to applicable laws, regulations and policies?	<ol style="list-style-type: none"> <li>1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents.</li> <li>2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> <li>3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> </ol>	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15	Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	<ol style="list-style-type: none"> <li>1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment.</li> <li>2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile.</li> <li>3. Verify that privacy standards are also included within standards profile.</li> </ol>	

**Figure 6 – EACAF Questionnaire with Assessment Section Designated**

## Guidance Steps Section

Guidance steps have been provided for the EA SME to ensure each assessment question is appropriately addressed when evaluating whether the investment is compliant with each criteria. This section provides insight as to what is being asked in each assessment question and what architecture artifacts are required and / or conditional.



**EA Compliance Assessment Framework (EACAF) Questionnaire**

System Name: \_\_\_\_\_ IRC Date: \_\_\_\_\_

Package Inventory: Required Architecture Artifacts Conditional Architecture Artifacts

Legend: Received Not Received

Required Architecture Artifacts: AV-1, OV-2, OV-5a, SV-1, SV-5a, StdV-2, AV-2, OV-3, OV-6c, SV-4, StdV-1

Conditional Architecture Artifacts: OV-1, OV-6, SvcV-2, SV-2, SvcV-1, SvcV-4

Focus Area	Criteria	Assessment	Guidance Steps	Assessment Comments
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14 Does the investment adhere to applicable laws, regulations and policies?	<ol style="list-style-type: none"> <li>1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents.</li> <li>2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> <li>3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> </ol>	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15 Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	<ol style="list-style-type: none"> <li>1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment.</li> <li>2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile.</li> <li>3. Verify that privacy standards are also included within standards profile.</li> </ol>	

Figure 7 – EACAF Questionnaire with Guidance Steps Designated

## Assessment Comments Section

The EA SME will review all pre-defined set of questions for all compliance requirements and provide comments.



**EA Compliance Assessment Framework (EACAF) Questionnaire**

System Name: \_\_\_\_\_ IRC Date: \_\_\_\_\_

Package Inventory:

Legend	Required Architecture Artifacts						Conditional Architecture Artifacts		
Received	AV-1	OV-2	OV-5a	SV-1	SV-5a	StdV-2	OV-1	SV-6	OCV-2
Not Received	AV-2	OV-3	OV-6c	SV-4	StdV-1		SV-2	SvcV-1	SvcV-4

Focus Area	Criteria		Assessment	Guidance Steps	Assessment Comments
3. Compliance with Applicable Laws, Regulations and Policies	General LRP Compliance	14	Does the investment adhere to applicable laws, regulations and policies?	1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents. 2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary. 3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.	
	Health Data Policies and Standards (e.g. HIPAA, HITSP)	15	Does the investment share information with other Federal agencies such as the VA and civilian hospitals?	1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment. 2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile. 3. Verify that privacy standards are also included within standards profile.	

Figure 8 – EACAF Questionnaire with Assessment Comments Designated

### 5.3 SUMMARY REPORT

The Summary Report provides the IRC an overview of the EA SME compliance assessment comments once the Questionnaire is complete. It is composed of two sections including: Investment Profile and Focus Area Assessment Summary.

IRC Date: \_\_\_\_\_

**EA Compliance Assessment Framework (EACAF) Summary Report**

---

**Investment Profile**

System Name	_____	State of Transition Plan	_____
Tier	_____	Fiscal Period	_____
Total Amount Requested	_____	Requires SFIS Compliance?	_____

System Description

\_\_\_\_\_

---

**Focus Area Assessment Summary**

1. MHS Business Priority

\_\_\_\_\_

2. Consistency with MHS Enterprise Modeling Standards

\_\_\_\_\_

3. Compliance with Applicable Laws, Regulations and Policies

\_\_\_\_\_

4. Compliance with MHS Technology Standards

\_\_\_\_\_

5. Compliance with External Architecture Requirements

\_\_\_\_\_

6. General Documentation Consistency

\_\_\_\_\_

**Figure 9 – EACAF Summary Report**

**Investment Profile Section:**

The EA SME will complete the Investment Profile section based on the investment information included in the DBITC Compliance.

**Focus Area Assessment Summary Section:**

The EA SME will provide a high-level summary of comments based on the EA SME evaluation comments of the EACAF Questionnaire.

## 6. ARCHITECTURE ASSESSMENT GUIDANCE

This section provides guidance to the subject matter expert conducting the architecture assessment for an ICP.

### 6.1 CERTIFICATION PACKAGE CHECKLIST

The ICP includes several documents which will be useful to the architect to conduct the EA SME review. The MHS EAD SME should review the ICP for completeness of all the architecture artifacts. Contact the MHS DBITC Management Team if any documentation has not been provided.

The ICP includes the following:

- A presentation brief that provides an understanding of the investment and program activities.
- A Defense Health Program Systems Inventory Reporting Tool (DHP-SIRT) Certification Dashboard.
- A copy of the DHP-SIRT Regulatory Compliance Report.
- The proper set of privacy, information assurance, Federal Information Security Management Act (FISMA) compliance and authority to operate (ATO) documents.

The EA SME should:

- Ensure the ICP investment owner has prepared program summary information that can be prepared as an All View (AV-1) for the investment.
- Ensure the required set of architecture artifacts is provided in an electronic manner.
- Ensure the conditional architecture artifacts are provided in an electronic manner as appropriate.
- Ensure architecture artifacts changed by a proposed system modernization clearly distinguishes “as-is” versus “to-be” state of the architecture.

The following sections provide assessment and guidance steps for architecture focus areas, and correspond to the guidance steps provided within the EACAF questionnaire.

## 6.2 BUSINESS PRIORITY

Criteria	ID	Assessment	EA SME Guidance Steps	Relevant Architecture Artifacts
<b>Business Value</b>	1	Have stakeholders, users and customers of this investment been identified?	<ol style="list-style-type: none"> <li>1. Verify all stakeholders are identified within the AV-1 summary.</li> <li>2. Verify stakeholder names are reflected in the OV-2 description.</li> <li>3. Verify stakeholder names are reflected in the AV-2 glossary.</li> <li>4. Review Regulatory Compliance Report from DHP-SIRT and verify 'System Stakeholder' field matches OV-2 description.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> <li>• AV-2</li> <li>• OV-2</li> </ul>
<b>Business Value</b>	2	Are there other investments or organizations within the Defense Health Program, which may be reporting a similar capability based on the investment description provided in the DBT package?	<ol style="list-style-type: none"> <li>1. Explore current investments within MHS program offices and Services to verify functionality is not duplicated.</li> <li>2. Verify OV-5a traceability to MHS overall activities.</li> <li>3. Review operational activities in OV-5 and analyze if other MHS programs are addressing the same set of operational activities.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-5a</li> </ul>
<b>Strategic and Enterprise Planning</b>	3	Is the investment included within the DoD's most current Enterprise Transition Plan?	<ol style="list-style-type: none"> <li>1. Review the BTA program dashboard on the BTA website to verify program accuracy for investments that are budgeted for over \$1M. Verify that the investment is included within the DoD Enterprise Transition Plan.</li> <li>2. Verify that this information is described within the AV-1 program summary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> </ul>
<b>Strategic and Enterprise Planning</b>	4	In the DoD's most current Enterprise Transition Plan, is the investment identified as a "legacy" system? If so, indicate the termination and/or migration date for this investment.	<ol style="list-style-type: none"> <li>1. Review the current DoD Enterprise Transition Plan to determine if the investment is identified as a "legacy" system.</li> <li>2. Review program summary briefing to identify the termination and /or migration date and target system for the investment if it is considered a "legacy" system.</li> <li>3. If the system's capabilities are migrating to another system, include the name of the target system and verify if this information is reflected within the AV-1 program summary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> </ul>

Criteria	ID	Assessment	EA SME Guidance Steps	Relevant Architecture Artifacts
<b>Strategic and Enterprise Planning</b>	5	Is the architecture provided for the investment appropriate for its milestone phase? Are the milestones included in the certification dashboard consistent with the DoD ETP?	<ol style="list-style-type: none"> <li>1. Work with investment owners to understand if architecture artifacts reflect the development milestone phase or sustainment lifecycle.</li> <li>2. Review the DBS Certification Dashboard to determine if the milestones are consistent with the DoD ETP.</li> <li>3. Verify that this information is reflected within the AV-1 program summary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> </ul>

**Table 10 – Business Priority Guidance**

### 6.3 CONSISTENCY WITH MHS ENTERPRISE MODELING STANDARDS

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Enterprise Data</b>	6	Are the actors and information exchanges appropriately identified?	<ol style="list-style-type: none"> <li>1. Verify the OV-2 identifies the complete set of performers for the scope of the investment.</li> <li>2. Verify the performers identified in the OV-2 are consistent with the 'System Stakeholder' field in the Regulatory Compliance Report from DHP-SIRT.</li> <li>3. Verify the name of the performers identified in the OV-2 and the name of the resource flows in the OV-3 are identified with a unique naming convention.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-2</li> <li>• OV-3</li> </ul>
<b>Enterprise Data</b>	7	Is the right information flow captured between operational nodes?	<ol style="list-style-type: none"> <li>1. Verify the Needlines identified in the OV-2 are traceable to the resource flows identified in the OV-3 information exchange matrix.</li> <li>2. Verify the right resource flow is captured between performers by reviewing the operational activities in OV-5a, and data stores and performers identified within the OV-2 description.</li> <li>3. Verify the description of the resource flows identified in the OV-2 is reflected in the AV-2 glossary.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-2</li> <li>• OV-3</li> <li>• OV-5a</li> <li>• AV-2</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Operational Architecture</b>	8	Have the correct operational nodes been identified and consistent with MHS standards?	<ol style="list-style-type: none"> <li>1. Verify the performers captured in the OV-2 are aligned with the performers captured in the MHS enterprise-level OV-2 description.</li> <li>2. Verify consistency between the performers captured in the OV-2 and the operational taxonomy in OV-5a.</li> <li>3. Verify the correct performers have been identified in the OV-2 by reviewing the Needlines identified in the OV-2 and determining if the Needlines are traceable to the performers of the information exchanges identified in the OV-3 information exchange matrix.</li> <li>4. Verify the descriptions of the performers identified in the OV-2 are reflected in the AV-2 glossary.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-2</li> <li>• OV-3</li> <li>• OV-5a</li> <li>• AV-2</li> </ul>
<b>Operational Architecture</b>	9	Does the investment package include both "as-is" and "to-be" architecture models?	<ol style="list-style-type: none"> <li>1. Verify architecture artifacts address both "as-is" and "to-be" architecture models.</li> <li>2. Verify OV-5a operational taxonomy reflects the additional activities that need to be added for the "to-be state."</li> <li>3. Verify SV-1 system interface description reflects the current state interfaces and identifies interfaces to be added in the future.</li> <li>4. Verify OV-3 information exchange matrix addresses both current and future state requirements and Needlines.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-5a</li> <li>• SV-1</li> <li>• OV-3</li> </ul>
<b>Operational Architecture</b>	10	Are the operational activities consistent between the SV and OV products?	<ol style="list-style-type: none"> <li>1. Verify SV-4 system functions and operational activities in the OV-5a are reflected in the SV-5a Operational Activity to System Function Traceability Matrix.</li> <li>2. In the case of a Service Oriented Architecture environment, verify service functions are indicated in a SvcV-4</li> <li>3. In the case of Service Oriented Architecture environment, a service function list, SvcV-4, should be traced to the MHS OV-5a operational taxonomy.</li> </ol>	<ul style="list-style-type: none"> <li>• SV-4</li> <li>• SV-5</li> <li>• OV-5a</li> <li>• SvcV-4</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Enterprise System Functions</b>	11	Is the investment consistent with MHS system functions?	<ol style="list-style-type: none"> <li>1. Verify the system functions identified in the SV-4 are aligned and mapped to MHS enterprise-level common system function list.</li> <li>2. Identify if there are any potential gaps with the MHS enterprise-level common system function list.</li> <li>3. In the case of a Service Oriented Architecture environment, verify service functions are indicated in a SvcV-4.</li> </ol>	<ul style="list-style-type: none"> <li>• SV-4</li> <li>• SvcV-4</li> </ul>
<b>Enterprise System Functions</b>	12	Are the system functions mapped to operational activities?	<ol style="list-style-type: none"> <li>1. Verify system functions identified in the SV-4 support and provide traceability to operational activities in the OV-5a taxonomy.</li> <li>2. In the case of a Service Oriented Architecture environment, verify service functions are indicated in a SvcV-4.</li> <li>3. In the case of a Service Oriented Architecture environment, verify service functions are mapped to operational activities in the MHS OV-5a operational taxonomy.</li> <li>4. Verify the appropriate systems functions are mapped to the appropriate operational activities in the SV-5a matrix.</li> <li>5. Identify any potential gaps where the system functionalities are planned but not developed, where partial system functionality has been provided or where there is no relationship between a particular operational activity and system function.</li> </ol>	<ul style="list-style-type: none"> <li>• SV-4</li> <li>• OV-5a</li> <li>• SV-5a</li> <li>• SvcV-4</li> <li>• SvcV-5</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Internal Interfaces</b>	13	If this investment interfaces with other MHS system(s), have all interfaces been identified?	<ol style="list-style-type: none"> <li>1. Verify the internal system interfaces needed to implement and automate the internal resource flows referenced by the operational nodes in the OV-2 and corresponding Needlines are captured in the SV-1.</li> <li>2. In the case of a Service Oriented Architecture, verify if system interfaces are reflected within a SvcV-1 diagram.</li> <li>3. Identify any potential gaps where system interfaces internal to other MHS system(s) have not been identified and are not included within AV-1 program summary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> <li>• OV-2</li> <li>• SV-1</li> <li>• SvcV-1</li> </ul>

**Table 11 – Consistency with MHS Enterprise Modeling Standards**

## 6.4 COMPLIANCE WITH APPLICABLE LAWS, REGULATIONS AND POLICIES

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>General LRP Compliance</b>	14	Does the investment adhere to applicable laws, regulations and policies?	<ol style="list-style-type: none"> <li>1. Verify the investment adheres to the applicable laws, regulations and policies within DoD and federal guidance documents.</li> <li>2. Verify the applicable laws, regulations and policies such as HIPAA privacy, Information Assurance, and Section 508, are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> <li>3. Verify the applicable laws, regulations and policies unique to the investment are documented in the AV-1 program summary and AV-2 integrated dictionary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> <li>• AV-2</li> </ul>
<b>Health Data Policies and Standards (e.g. HIPAA, HITSP)</b>	15	Do transaction standards applicable to Health Insurance Portability Accountability Act (HIPAA) apply for this investment?	<ol style="list-style-type: none"> <li>1. Work with MHS Privacy Office to identify if HIPAA standards are applicable for monitoring within this investment.</li> <li>2. Identify appropriate HIPAA data and technical standards within StdV-1 standards profile.</li> <li>3. Verify that privacy standards are also included within standards profile.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1</li> </ul>
<b>Health Data Policies and Standards (e.g. HIPAA, HITSP)</b>	16	Do standards identified by the Health Information Technology Standards Panel (HITSP) apply to this investment?	<ol style="list-style-type: none"> <li>1. Evaluate if HITSP standards need to be adhered to by the solution provided within the investment.</li> <li>2. Verify that HITSP standards for this investment is coordinated with other affected systems and MHS partner organizations such as VA and TRICARE network providers.</li> <li>3. Verify StdV-1 reflects latest “Target DoD/VA Health Standards Profile” for sharing between DoD and VA.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1</li> </ul>

**Table 12: Compliance with Laws, Regulations and Policies**

## 6.5 COMPLIANCE WITH MHS TECHNOLOGY STANDARDS

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Interoperability Standards</b>	17	If the investment interfaces with other systems, have appropriate technology standards been identified (including message formats)?	<ol style="list-style-type: none"> <li>1. A StdV-1 standards profile should be prepared that reflects a full set of technology standards.</li> <li>2. Verify the StdV-1 includes DISR Online standards.</li> <li>3. Verify all appropriate standards have been identified by cross-checking the ICP artifacts with DISR Online.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1 with DISR Technical Standards Profile</li> </ul>
<b>Security Standards</b>	18	Does this investment require CAC Enablement? If so, have the appropriate standards been identified?	<ol style="list-style-type: none"> <li>1. If CAC enablement is required, then Public Key Infrastructure (PKI) standards will be included within the StdV-1 Standards Profile.</li> <li>2. The StdV-1 standards should be aligned with DISR Technical Standards Profile.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1 with DISR Technical Standards Profile</li> </ul>
<b>Security Standards</b>	19	Have user authentication and authorization standards been identified?	<ol style="list-style-type: none"> <li>1. Authentication and authorization standards should be reflected within a StdV-1 Standards Profile.</li> <li>2. These standards should be placed within a DISR Technical Standards Profile.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1 with DISR Technical Standards Profile</li> </ul>
<b>Infrastructure Standards</b>	20	Are the infrastructure standards compliant with MHS target standards?	<ol style="list-style-type: none"> <li>1. Prepare a StdV-1 Standards Forecast Profile for the program.</li> <li>2. Verify if infrastructure standards mentioned within the StdV-1 reflects standards stated within the MHS Target Standards Profile.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1</li> </ul>
<b>Infrastructure Standards</b>	21	Is this investment dependent on a Service Oriented Architecture? If so, have the appropriate standards been identified?	<p>If the investment is a Service Oriented Architecture environment, then:</p> <ol style="list-style-type: none"> <li>1. A SvcV-1 Services Interface Description should be prepared to reflect the environment.</li> <li>2. The StdV-1 Standards Profile should include appropriate Service Oriented Architecture standards in use within the environment.</li> <li>3. The StdV-2 Standards Forecast should reflect the upcoming or target Service Oriented Architecture standards.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1</li> <li>• StdV-2</li> <li>• SvcV-1</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Infrastructure Standards</b>	22	Is the operational activity model traceable to SOA processes?	<p>If the program is a Service Oriented Architecture environment, then:</p> <ol style="list-style-type: none"> <li>1. A SvcV-1 Services Interface Description should be used to reflect the environment.</li> <li>2. A SvcV-4 Services Functionality Description should be prepared that documents all of the service functions.</li> <li>3. The MHS OV-5a operational taxonomy should be mapped to the program SvcV-4 service functions.</li> </ol>	<ul style="list-style-type: none"> <li>• SvcV-1</li> <li>• ScvV-4</li> <li>• OV-5a</li> </ul>
<b>Infrastructure Standards</b>	23	Was the Enterprise Information Environment Mission Area (EIEMA) planning process and methodology considered for this investment as related to net-centric services and the GiG?	<ol style="list-style-type: none"> <li>1. If the program uses infrastructure support that includes net-centric services and GIG backbone support, then this information should be reflected within the AV-1 program summary.</li> <li>2. The EIEMA planning process reflects support such as what DISA provides to DoD clients. Any such support should be documented within the AV-1 program summary.</li> <li>3. The StdV-1 Standards Profile should reflect GIG Key Interface Profiles and Net-Centric standards in use by EIEMA.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> <li>• StdV-1</li> </ul>

**Table 13: Compliance with MHS Technology Standards**

## 6.6 COMPLIANCE WITH EXTERNAL ARCHITECTURE REQUIREMENTS

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>External Interfaces</b>	24	Have external interfaces and system dependencies with business entities been identified?	<ol style="list-style-type: none"> <li>1. Verify the SV-1 depicts system nodes, the system resident at these nodes and system interfaces needed to implement and automate the resource flows referenced by the operational nodes in the OV-2 and corresponding Needlines.</li> <li>2. External dependencies with business entities should be reflected within the AV-1 program summary.</li> <li>3. Verify OV-2 resource flows reflect external entities and business stakeholders.</li> </ol>	<ul style="list-style-type: none"> <li>• OV-2</li> <li>• SV-1</li> <li>• AV-1</li> </ul>
<b>BTA Compliance</b>	25	Is the investment compliant with BEA guidance and reference models?	<ol style="list-style-type: none"> <li>1. Verify all IT business systems have been registered and maintained to reflect the most current information in DITPR.</li> <li>2. Verify the investment adheres to the BEA reference models and latest BEA set of enterprise architecture artifacts by reviewing the DHP-SIRT Regulatory Compliance Report.</li> <li>3. Refer to the DHP-SIRT to verify the investment is compliant with the BEA.</li> <li>4. Verify that this information is reflected within the AV-1 program summary.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>BTA Compliance</b>	26	If this investment requires SFIS compliance, have the appropriate artifacts been provided (SFIS Compliance Checklist and Logical Data Model)?	<ol style="list-style-type: none"> <li>1. Determine if the investment is required to be SFIS compliant by reviewing the system description identified in the DBS Certification Dashboard.</li> <li>2. Review the system description identified in the DBS Certification Dashboard to determine if the system has been classified as a Legacy Accounting, Legacy Business Feeder, Target Business Feeder, or Target Accounting System. If so, the investment is required to be SFIS compliant.</li> <li>3. Verify investments complete the SFIS Compliance Checklist to determine if SFIS system requirements are currently met for investments that require being SFIS compliant.</li> <li>4. Verify that this information is reflected within the AV-1 program summary.</li> <li>5. SFIS data elements may be reflected in a logical data mapping within a relational or object-oriented data model.</li> </ol>	<ul style="list-style-type: none"> <li>• AV-1</li> </ul>
<b>DoD/VA Target Health Standards Profile</b>	27	If this system shares data with the VA, is it aligned with the DoD/VA Target Health Standards Profile?	<ol style="list-style-type: none"> <li>1. The system should have a StdV-1 Standards Profile.</li> <li>2. Verify the latest DoD/VA Target Health Standards Profile is reflected within the StdV-1 Standards Profile.</li> </ol>	<ul style="list-style-type: none"> <li>• StdV-1</li> </ul>

**Table 14: Compliance with External Architecture Requirements**

## 6.7 GENERAL DOCUMENTATION CONSISTENCY

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Package Completeness</b>	28	Does the IRC package for this investment contain the necessary artifacts?	<ol style="list-style-type: none"> <li>1. Verify all required architecture artifacts have been included within the ICP.</li> <li>2. Determine if conditional architecture views for SOA Services, Business Process Reengineering, and Communications Infrastructure are included within the ICP.</li> <li>3. Identify any potential gaps where the ICP does not contain all required and conditional architecture artifacts and has an insufficient level of data completeness where all necessary attributes of each data element are not specified to accurately reflect the scope and purpose of the investment.</li> <li>4. Verify a justification has been provided describing the reasons for any identified gaps in the Architecture Compliance Plan, recommended actions to address each comment and the proposed timeline to address each comment.</li> </ol>	<ul style="list-style-type: none"> <li>• All</li> </ul>
<b>Modernization Components</b>	29	Does the architecture support the modernization description? (If this is a multi-year investment, does it support the current FY?)	<ol style="list-style-type: none"> <li>1. Verify the architecture views accurately reflect the modernization description described in the DBS Certification Dashboard and the DHP-SIRT Regulatory Compliance Report.</li> </ol>	<ul style="list-style-type: none"> <li>• All</li> </ul>

Criteria	ID	Assessment	Guidance Steps	Relevant Architecture Artifacts
<b>Modernization Components</b>	30	If the investment is undergoing annual review, has the architecture changed since the original certification approval?	<ol style="list-style-type: none"> <li>1. Review the system and modernization description identified in the DBS Dashboard to identify any potential changes needed to be reflected in the architecture.</li> <li>2. Determine if architecture views such as OV-2, OV-5a and SV-1 have changed since the previous certification approval.</li> <li>3. Determine if the changes made to the architecture artifacts since the previous certification approval are accurately described in the modernization description identified in the DBS Certification Dashboard.</li> <li>4. Verify all additional changes to the architecture views are reflected within the submitted architecture views.</li> <li>5. Verify modernization description and changes to the architecture views are reflected in the overall MHS EA and the BEA.</li> </ol>	<ul style="list-style-type: none"> <li>• All</li> </ul>
<b>Modernization Components</b>	31	Are the data elements, processes, actors and system description consistent across the architecture artifacts (including scope)?	<ol style="list-style-type: none"> <li>1. Verify the scope of the investment and intended use of the architecture is first and foremost accurately reflected in the AV-1, AV-2, OV-2 and OV-5 architecture artifacts.</li> <li>2. Verify all architecture artifacts reflect information consistency as to whether the data in one architecture view agrees with the data in another architecture artifact.</li> </ol>	<ul style="list-style-type: none"> <li>• All</li> </ul>
<b>Modernization Components</b>	32	Is the modernization as described in the investment package reflected in the MHS and BEA operational architectures?	<ol style="list-style-type: none"> <li>1. Verify the architecture artifacts accurately reflect the modernization description and are reflected within the MHS EA and BEA.</li> <li>2. Verify the AV-1 program summary states how program modernization is occurring.</li> </ol>	<ul style="list-style-type: none"> <li>• All</li> </ul>

**Table 15: General Documentation Consistency**

## 7. ACRONYMS

Acronym	Term
<b>ACAT</b>	Acquisition Category
<b>AIS</b>	Automated Information System
<b>ATO</b>	Authority to Operate
<b>AV</b>	All Viewpoint
<b>BEA</b>	Business Enterprise Architecture
<b>BMA</b>	Business Mission Area
<b>BPR</b>	Business Process Reengineering
<b>BTA</b>	Business Transformation Agency
<b>CA</b>	Certification Authority
<b>CJCSI</b>	Chairman of the Joint Chiefs of Staff Instruction
<b>DASD (IM)</b>	Deputy Assistant Secretary of Defense for Information Management
<b>DoDNII</b>	DoD Networks and Information Integration
<b>DBITC</b>	Defense Business Information Technology Certification
<b>DBS</b>	Defense Business System
<b>DBT</b>	Defense Business Transformation
<b>DHP</b>	Defense Health Program
<b>DHP-SIRT</b>	Defense Health Program Systems Inventory Reporting Tool
<b>DITPR</b>	DoD Information Technology Portfolio Repository
<b>DIV</b>	Data and Information Viewpoint
<b>DoD</b>	Department of Defense
<b>DoDAF</b>	DoD Architecture Framework
<b>DoDD</b>	Department of Defense Directive
<b>DoDI</b>	Department of Defense Instruction
<b>EA</b>	Enterprise Architecture
<b>EACAF</b>	Enterprise Architecture Compliance Assessment Framework
<b>EAD</b>	Enterprise Architecture Division
<b>FISMA</b>	Federal Information Security Management Act
<b>FY</b>	Fiscal Year
<b>GIG</b>	Global Information Grid
<b>HRM</b>	Human Resources Management
<b>ICP</b>	Investment Certification Package
<b>IM / IT</b>	Information Management / Information Technology
<b>IRB</b>	Investment Review Board
<b>IRC</b>	Investment Review Committee
<b>IT</b>	Information Technology
<b>JCIDS</b>	Joint Capabilities Integration Development System
<b>JROC</b>	Joint Requirements Oversight Council
<b>MAIS</b>	Major Automated Information System
<b>MHS</b>	Military Health System
<b>NDAA</b>	National Defense Authorization Act
<b>NII</b>	Networks and Information Integration
<b>NR-KPP</b>	Net-Ready Key Performance Parameter
<b>NSS</b>	National Security System
<b>OCIO</b>	Office of the Chief Information Officer
<b>OMB</b>	Office of Management and Budget
<b>OV</b>	Operational Viewpoint

Acronym	Term
<b>PCA</b>	Pre-Certification Authority
<b>PfM</b>	Portfolio Management
<b>PKI</b>	Public Key Infrastructure
<b>PM</b>	Program Manager
<b>SIPRNET</b>	Secret Internet Protocol Router Network
<b>SME</b>	Subject Matter Expert
<b>StdV</b>	Standards Viewpoint
<b>SV</b>	Systems Viewpoint
<b>SvcV</b>	Services Viewpoint
<b>TMA</b>	TRICARE Management Activity