



# **DoD Business Enterprise Architecture: Compliance Guidance**

**--BEA 8.0--**

March 11, 2011

## Version History

---

Version Number	Document Date	Key Modifications
6.0	March 11, 2011	Changes for BEA 8.0
5.0	March 12, 2010	Changes for BEA 7.0
4.0	May 14, 2009	Changes for BEA 6.0
3.0	May 23, 2008	Changes for BEA 5.0
2.0	January 2007	Effective BEA Version, ACART™, Assertion Steps, Compliance Plans
1.0	April 10, 2006	Initial Guidance

# Table of Contents

---

Version History .....	i
Table of Contents .....	ii
1. Introduction .....	1
2. Purpose and Scope .....	1
3. Business Enterprise Architecture (BEA) .....	2
3.1 BEA 8.0 Overview .....	2
3.2 BEA 8.0 Content Structure .....	3
3.2.1 E2E Processes .....	3
3.2.2 Key Elements .....	3
4. Compliance Process .....	3
4.1 Authority .....	3
4.2 Defense Information Technology Portfolio Repository (DITPR) .....	4
4.2.1 Identifying BEA Gaps .....	5
4.3 BEA Structure for Compliance .....	5
4.3.1 Basic Steps – BEA Assessment .....	7
4.4 Compliance Findings .....	7
5. Incremental Approach to BEA Compliance .....	8
5.1.1 BCL Overview .....	8
5.1.2 Pre-MS A/MS A .....	8
5.1.3 Pre-MS B/MS B .....	8
5.1.4 Pre-Initial Operational Capability (IOC) .....	9
5.1.5 Subsequent Increments .....	9
6. Process Support .....	9
6.1 Compliance Documentation and Retention .....	9
6.1.1 Architecture Compliance Plan (ACP) .....	10
6.2 Roles and Responsibilities for Compliance .....	10
6.3 Additional Information .....	11
6.3.1 BEA Assessment and Compliance Process Support .....	11
6.3.2 Technical Standards for Expeditionary Environments .....	11
Appendix A: References .....	13
Appendix B: DoDAF Mapping .....	14
Appendix C: Definitions .....	15
Appendix D: Acronyms .....	18

# 1. Introduction

---

The Business Enterprise Architecture (BEA) is the enterprise architecture for the Department of Defense (DoD) Business Mission Area (BMA) and reflects the DoD’s business transformation priorities, the business capabilities required to support those priorities, and the combinations of enterprise systems and initiatives that enable those capabilities. Per section 2222(c)(1) of title 10, United States Code (U.S.C.) (Reference (a)), the overarching purpose of the BEA is to “guide, constrain, and permit implementation of interoperable defense business system solutions” across the DoD.

The BEA is a required element of the DoD Investment Review Board (IRB) Process (henceforth, “IRB Process”), the Business Capability Lifecycle (BCL), and the Enterprise Transition Plan (ETP). In addition to Component architectures and transition plans, the BEA enables the IRBs to assess investments relative to their functional needs and evaluate the impact on end-to-end business processes. These products and processes provide both the end-state and the roadmap to deliver more robust business capabilities.

Section 2222 of Reference (a) requires any defense business system (DBS) modernization that will have a total cost in excess of \$1M to achieve BEA compliance.

## 2. Purpose and Scope

---

The DoD Business Enterprise Architecture: Compliance Guidance for BEA 8.0 (henceforth, “Guidance”) provides direction on assessing and asserting compliance to the BEA. It is intended for the following Office of the Secretary of Defense (OSD) or DoD Component personnel responsible for, accountable for, contributing to, and/or supporting the development of DBSs, specifically for the BEA compliance assessment process:

Functional Sponsors	Chief Information Officers (CIOs)
Chief Management Officers (CMOs)	Program Managers (PMs)
Program Executive Offices (PEOs)	Acquisition Executives
DoD IRB membership and leadership	Test Community

After reviewing this Guidance, the reader should understand: (1) the overall BEA compliance process and the key elements of BEA compliance; (2) the rules, roles, and responsibilities involved in demonstrating and certifying DBS compliance; and (3) the artifacts, processes, and tools that may facilitate BEA compliance assertion and certification.

This Guidance enables participants to ensure that the DBS complies with governing BEA statute and policies, listed below:

- The DBS Investment Review and Certification processes and requirements established by sections 186 and 2222 of Reference (a)
- The policies and procedures established in Directive-Type Memorandum (DTM) 08-020, “Investment Review Board (IRB) Roles and Responsibilities” (Reference (b))

- The policies and procedures established in the “Interim Acquisition Guidance for Defense Business Systems (DBS)” (Reference (c))

This Guidance is to be used in conjunction with “DoD IT Defense Business Systems Investment Review Process: Guidance,” January 2009 (henceforth, “IRB Guidance”) (Reference (d)), which describes IRB processes and procedures.

**This Guidance document does not establish DoD architecture development requirements and policies.**

## 3. Business Enterprise Architecture (BEA)

---

There are two types of BEA releases: *official releases and informational releases*. Official releases, such as BEA 8.0, are published annually in March and are to be used by DoD Components when asserting BEA compliance. Informational releases are generally published in July and December, and reflect interim content updates. These updates allow stakeholders to accelerate the implementation of requirements outside of the official release schedule while obtaining insight into other ongoing BEA updates. Informational releases, at this time, are not to be used for BEA Compliance.

### 3.1 BEA 8.0 Overview

BEA 8.0 is a consolidation of the informational releases of BEA 7.1 and BEA 7.2 in addition to BEA content and visualization updates. Such an approach allows stakeholders to accelerate coordination and implementation of End-To-End (E2E) requirements that focus on improving the Department’s ability to manage business operations.

The main focus areas for BEA 8.0 support the intended uses of the architecture:

- Investment Management – Support alignment of services, systems, and solutions to the prioritized strategic capabilities of the Department, and
- Interoperability – Support the development of enterprise systems through identification of standard data used within the Department’s business processes

The Department’s Strategic Management Plan (SMP) (Reference (e)) is the key driver of the BEA. The transformation effort guiding BEA development continues to focus on both providing tangible outcomes for a limited set of enterprise level priorities within the SMP and E2E framework, and developing an architecture that is integrated, understandable, and implementable. As E2E processes continue to be refined and decomposed in the BEA with each release, individual DBSs will be able to align their own processes with the Department’s overall desired end state, reaching across functional silos and achieving greater business process optimization.

For more detailed information regarding changes to the BEA, refer to the BEA 8.0 Summary Document (Reference (f)).

## 3.2 BEA 8.0 Content Structure

### 3.2.1 E2E Processes

The Department's fifteen E2E business processes play a critical role in how the Department builds its business capabilities and what drives BEA content:

DoD's 15 End to End (E2E) Business Processes	
Acquire to Retire	Order to Cash
Budget to Report	Plan to Stock
Concept to Product	Procure to Pay
Cost Management	Proposal to Reward
Deployment to Retrograde/Redeployment	Prospect to Order
Environmental Liabilities	Service Request to Resolution
Service to Satisfaction	Hire to Retire
Market to Prospect	

**Table 1: E2E Processes**

BEA requirements have been mapped to various levels of the BEA<sup>1</sup>. By extracting applicable requirements through the E2E Business Processes at Level I, any DoD organization can refine and decompose these requirements to their own specific business process and system configurations through the use of business process reengineering (BPR).

### 3.2.2 Key Elements

BEA 8.0 is developed within the DoD Architecture Framework (DoDAF) 2.0<sup>2</sup> and comprises a set of integrated products. Overall, the BEA represents the data and implementation requirements necessary to achieve the Department's Enterprise priorities. The BEA has selected content that has been identified as **key elements for BEA compliance**: Operational Activities (OAs), Processes, Information Exchanges (IEs), Data Attributes and associated Metadata (*i.e.*, length, type, and permitted values), Defense Financial Management Improvement Guidance (DFMIG) Statements (which include Federal Financial Management Improvement Act (FFMIA) requirements), Business Rules, and Laws, Regulations, and Policies (LRP).

## 4. Compliance Process

---

### 4.1 Authority

The requirement and authority for BEA compliance is derived from section 2222 of Reference (a); the requirement applies to any DBS modernization that will have a total cost in excess of \$1M, is

---

<sup>1</sup> Level I E2Es identify each of the major process areas that comprise the E2E and represent the scope of lifecycle activity that may take place within a particular E2E. These processes are generic in nature and are not specific to a business scenario or configuration.

<sup>2</sup> Refer to Appendix B for DoDAF 1.0 to 2.0 alignment for BEA usage purposes.

recognized under section 2222(a)(2)(A) of Reference (a), and is governed through the certification, approval and annual review process (*i.e.*, the IRB Process) as described in Reference (d):

Section 2222(a)(2) of title 10 U.S.C. Classification	Definition
A	Has been determined by the appropriate chief management officer to be in compliance with the enterprise architecture and business process engineering requirements outlined in 2222(a)(1) of Reference (a)
B	Is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security
C	Is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect

**Table 2: Statutory Compliance Requirements**

Accordingly, the ETP will include any DBS modernization with an obligation in excess of \$1M during the preceding fiscal year that was not certified under subsection (a) of section 2222 of Reference (a) and the reasons for the waiver.

From an IRB governance standpoint, BEA utilization and compliance aids the IRBs in determining if DoD Component DBSs support DoD Enterprise priorities and requirements.

## 4.2 Defense Information Technology Portfolio Repository (DITPR)

As mandated by the DoD Chief Information Officer (CIO) in a March 17, 2005 Memo, “Department of Defense (DoD) Information Technology Portfolio Registry (DITPR)” (Reference (g)), DoD Components must register and maintain current information about all IT systems in DITPR. DITPR does not serve the purpose or function for assessing BEA compliance and it is not approved for that usage. BEA-related information, however, must be consistent between DITPR and any method used to assess BEA compliance for the purposes of portfolio management and visibility throughout the IRB governance process. Information that must be updated in DITPR includes: OAs (“As-Is” and “To-Be”), Business Capabilities, Business Processes, and System Functions for DBSs in the IRB Process.

The “As-Is” or “To-Be” architecture should be established in DITPR prior to assessing BEA compliance as OAs, Business Capabilities, Business Processes, and System Functions. Next, the BEA compliance assessment will be conducted. This step may identify additional information about the DBS that is inconsistent with the functional information entered in DITPR. If this occurs, it is critical that DITPR is updated to reflect these circumstances.

The IRB process relies on accurate DITPR data. At the IRB Chair’s discretion, IRB submissions with incomplete or inaccurate data entries in DITPR may be placed on hold until the Component has provided updated data in DITPR. For more detailed processes and procedures for entering BEA data into DITPR, refer to the DITPR User’s Guide (Reference (h)).

## 4.2.1 Identifying BEA Gaps

It may be determined that there are no OAs, Business Capabilities, Business Processes, or System Functions that can be selected in DITPR that accurately describe the functions of the DBS. Since the BEA is constantly evolving, it is possible that not all business functionality has been incorporated into the BEA. A function has been developed in DITPR to capture BEA gaps. At any time a gap is discovered, the responsible Component should record these gaps in DITPR. As they are reported to the BEA Staff through DITPR, the BEA gaps are analyzed and prioritized by the IRB for inclusion into the next official release of the BEA.

## 4.3 BEA Structure for Compliance

Table 3 outlines key terms in the BEA compliance process. Additional terms and definitions can be found in Appendix C.

Term	Definition
Scoping	Scoping is the process of selecting architecture objects from the Activities, Processes, and Information Exchanges (IEs) based on the functionality of the DBS. Scoping determines and narrows the subsequent objects to which one will be able to assert BEA Compliance.
Assertion	Assertion is the process of verifying and declaring that the DBS is compliant with the BEA key element selected during Scoping.

**Table 3: Compliance Process Terms**

BEA 8.0 aligns with DoDAF 2.0 naming conventions<sup>3</sup> and comprises a set of integrated products including the All Viewpoint (AV), Capability Viewpoint (CV), Operational Viewpoint (OV), System Viewpoint (SV), Services Viewpoint (SvcV), Standards Viewpoint (StdV), and Data & Information Viewpoint (DIV). Together, these Viewpoints display capabilities, activities, processes, data, Information Exchanges, Business Rules, System Functions, services, system data exchanges, technical standards, terms, and linkages to LRP.

Table 4 identifies BEA DoDAF 2.0 Artifacts or Content used for BEA compliance, depicts the key elements for compliance, and how each element is used (*i.e.*, whether for scoping or assertion).

BEA DoDAF 2.0 Artifact	BEA DoDAF 2.0 Artifact/ Content Name	Key Elements	Element Use
OV-5b	Operational Activity Model	Operational Activities	Scoping
OV-6c	Event-Trace Description	BPM Process	Scoping
OV-3	Operational Resource Flow Matrix	Information Exchanges	Scoping
LRP	Guidance	LRP	Assertion

<sup>3</sup> Refer to Appendix B for DoDAF 1.0 to 2.0 alignment for BEA usage purposes.

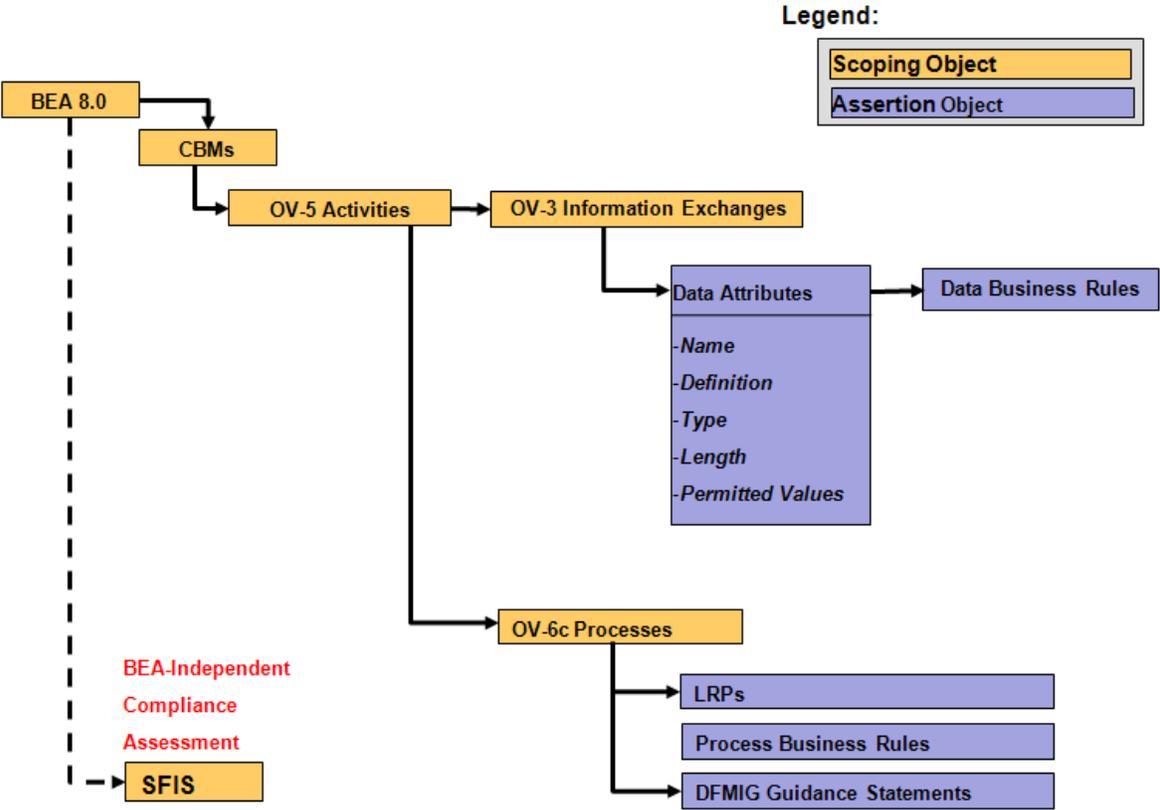
Guidance Statements	Guidance	Defense Financial Guidance Statement (DFMIG)	Assertion
OV-6a	Operational Rules Model	Business Rules	Assertion
DIV-2	Logical Data Model	Data Attributes	Assertion

**Table 4: BEA DoDAF Artifacts/Content Used for Compliance**

BEA Compliance will be asserted using one of the following methods or tools:

- The Manual Process for BEA compliance using BEA HTML (Reference (i))
- The Architecture Compliance and Requirements Traceability (ACART™) tool (Reference (j))

Figure 1 provides an illustration of the BEA structure related to compliance based on scoping and assertion as defined in Table 3.



**Figure 1: BEA Structure Related to Compliance**

### 4.3.1 Basic Steps – BEA Assessment

BEA assessments should be conducted by an interdisciplinary team familiar with the DBS to be assessed, the BEA, and DoDAF 2.0 architecture. The team should include functional specialists to focus on LRP, DFMIG, and Business Rules; and data modelers to focus on IEs, Data Attributes and Metadata. It is recommended that all members of the interdisciplinary team participate in the scoping of the BEA key elements and that specialists form work groups to focus on the assertion criteria.

1. The team assessing a DBS determines which BEA version should be used to conduct the BEA assessment (see Chapter 5, “Incremental Approach to BEA Compliance” regarding versioning).
2. The team then identifies BEA content applicable to the DBS through scoping. The elements used for scoping are: OV-5 Operational Activities, OV-3 Information Exchanges, and OV-6c Business Processes.
3. After relevant criteria have been scoped, the assertions on the Data Attributes and Metadata, data-related Business Rules, LRP, process-related Business Rules, and DFMIG Statements can be completed.

For DBSs that must conform to the Standard Financial Information Structure (SFIS), the SFIS Checklist must be completed. SFIS is the common business language that supports information and data requirements for budgeting, financial accounting, cost/performance management, and external reporting across the DoD Enterprise. At the time of the publication of this Guidance, SFIS requirements have not been fully integrated into the BEA. Please refer to the SFIS Resources web site (Reference (k)) for more detailed information.

## 4.4 Compliance Findings

The assertion process can result in the following findings:

1. Non-Compliant – One or more assertions are non-compliant.
  - If the DBS is classification (B) or (C), BEA compliance is not required under section 2222 of Reference (a).
2. Compliant – Able to demonstrate or assert compliance to the BEA Data Attributes, Business Rules, DFMIG Statements and LRP.
  - As a general rule, if the DBS has not yet deployed any capability into an operational environment, the responsible Component shall assert as Planned Compliant. Under 2222 of Reference (a), however, it is considered compliant to the BEA.
  - Alternately, if there is no content in the BEA related to the functions that the DBS performs, giving the Component no basis for assessing BEA compliance for their DBS, the responsible Component shall assert as Compliant to the BEA. Refer to Section 4.2.1 for addressing gaps in the BEA.

Components in the IRB Process should clearly address, in their memorandum to the IRB, their status of BEA compliancy.

## 5. Incremental Approach to BEA Compliance

---

DBSs should be developed and deployed utilizing an incremental approach, which quickly puts capability into the hands of the user while balancing DoD Enterprise needs, priorities, and resources. In addition, it allows room for continued maturity as desired outcomes evolve. This approach is implemented through BCL and described in Reference (c). Section 5 explains at what point in time one should assert and comply with the BEA during the incremental build and delivery of a DBS. DBSs subject to the BEA compliance process should maintain an architecture that aligns with the BEA to ensure that they are BEA compliant.

### 5.1.1 BCL Overview

BCL is tailored for the rapid delivery of enterprise business capability and leverages tools, technology, and process efficiencies including the BEA, ETP, and IRB processes. BCL aligns DoD DBS requirements, investment, and acquisition processes under the IRB governance framework, founded on the principle of tiered accountability. This governance framework delegates authority and accountability for program outcomes and compliance to the appropriate levels.

BCL is comprised of three distinct Phases: Business Capability Definition (BCD), Investment Management (IM), and Execution (the acquisition portion of BCL).

**A detailed description of BCL, its phases, and milestones is available in Reference (c).**

### 5.1.2 Pre-MS A/MS A

BCD and IM Phase activities in BCL all occur prior to a Milestone (MS) A decision.

When certification is requested at pre-MS A or at MS A, the Component should assert Planned Compliance to the latest official release of the BEA. This is based on current understanding of detailed information needs, the ability of the planned technical solution to become BEA compliant, and the contents of the BEA at that time. There should be no plan to select a technical solution that cannot be BEA Compliant, unless the planned solution falls under classification (B) or (C) of Reference (a) as detailed in Section 4.4 of this Guidance. In addition, it is critical to develop a “to-be” business process mapped to the BEA and reflected in the OV-6c prior to a MS A decision.

The results of the “to be” business process is a critical input to the Analysis of Alternatives (AoA) to facilitate the discovery of a best possible solution. The AoA is completed during the IM Phase of BCL.

*DoDAF artifacts required: OV-5b, OV-6c that reflects BPR. Once the BPR has been completed, the LRP impact must be determined and then any updates to existing policy must be facilitated, if needed.*

### 5.1.3 Pre-MS B/MS B

Any selected solution resulting from the AoA process should have the technical feasibility to be BEA compliant.

When Certification is requested at MS B, more is known regarding the DBS's functional and architectural requirements. For a DBS's initial increment at MS B, PMs should select the latest official BEA release as the guide for the DBS's capability delivery, thereby effectively locking in the first increment of the DBS to that version of the BEA and adding target dates for achieving BEA compliance. For 180 days after the official release of a version of the BEA, the Component may still select the *last* official version of the BEA to follow. After 180 days, the latest official release *must* be selected. Compliance to a different version of the BEA outside of this 180 day rule must be with the approval of the IRB Chair.

Any deployed capability defined prior to this stage must also be compliant to this same version of the BEA.

*DoDAF Artifacts required for BEA Compliance: LRP, OV-5b, OV-6c, OV-6a, OV-3, DIV-2*

## 5.1.4 Pre-Initial Operational Capability (IOC)

IOC occurs during the Limited Deployment phase of BCL where a capability is fielded into an operational environment. Prior to IOC, the increment must be tested against BEA compliance criteria (*i.e.*, tested to assert compliance to the version declared at MS B). Typically, this would occur during initial operational test and evaluation (IOT&E). Any capability delivered must be tested for compliance to the BEA.

Upon completion of testing, the DoD Component will state that either:

- The DBS is Compliant to the BEA, and will report these results to the IRB, or
- The DBS is Non-Compliant to the BEA, in whole or in part, and shall develop and retain an Architecture Compliance Plan (ACP) that may be requested by the IRB, CMO, or the Deputy Chief Management Officer (DCMO).

During any subsequent IRB reviews for Certification, Annual Review, or Close-out review for the increment, the results of BEA compliance tests must be reported.

## 5.1.5 Subsequent Increments

Subsequent increments of the DBS will assert to the most recent official release of the BEA when submitting a certification request to the IRB and follow the process for these increments as outlined above. Additionally, as part of a subsequent increment's development process, previously fielded increments will be upgraded to comply with the most recent official release of the BEA. The funds necessary to accomplish these upgrades must be incorporated into modernization requests of each follow-on increment.

# 6. Process Support

---

## 6.1 Compliance Documentation and Retention

In order to support compliance validation and audits, the Component must retain the results of compliance assessments to support the compliance results. The documentation should be detailed enough to describe the assertion for each key element including:

- **LRP:** Identify the applicable LRP requirements that are relevant to the system, and determine if they are Compliant, Planned Compliant, or Not Compliant.
- **Process and Data-Related Business Rules:** Identify the applicable business rules from the processes and the Data Attributes supported by the system and whether they are Compliant, Planned Compliant, or Not Compliant.
- **Data Attributes and Metadata:** Data Attributes and Metadata: Identify the applicable Data Attributes and Metadata (i.e., Length, Type, and Permitted Values), and whether they are Compliant, Planned Compliant, or Not Compliant.
- **DFMIG Statements:** Identify whether they are Compliant, Planned Compliant, or Not Compliant.

All supporting compliance documentation should be retained for two years.

### 6.1.1 Architecture Compliance Plan (ACP)

If a DBS (and/or increment) has been found to be non-Compliant to the BEA, the PM must develop an ACP to identify how the PM will take steps to be Compliant within a specified timeframe. The Component is not required to submit an ACP for review unless directed specifically by the IRB and/or DoD DCMO/CMO or unless the DBS is being audited. In addition to the compliance documentation listed in Section 6.1, an ACP should include:

- A detailed assessment of the extent to which the DBS is not compliant to the BEA, including a list of the specific Data Attributes and Metadata, Business Rules, DFMIG Statements, and LRP asserted to
- The key milestones and proposed deadline to achieve compliance
- The actions needed to achieve compliance, and
- Identification of the risks and critical dependencies (if applicable) associated with achieving compliance.

There is no specific format for an ACP. However, the plan should demonstrate how individual non-compliant key compliance elements will be made compliant.

## 6.2 Roles and Responsibilities for Compliance

The roles and responsibilities specific to the BEA compliance process are detailed in Table 5. Expanded roles and responsibilities as they pertain to the IRB Process are described in References (b) and (d).

Role	Responsibility
PM	Serves as DBS subject matter expert
	Ensures the modernization complies with the BEA with the appropriate documentation
	Along with the DBS's Functional Sponsor, ensures compliance with implementation guidance for Section 1072 of the Fiscal Year 2010 National Defense Authorization Act (NDAA) BPR requirements (Reference (l)) and corresponding statute (section 2222 of Reference (a))
	Ensures that all required data is valid and provides an accurate picture of the state of the information provided

	Identifies system requirements against the BEA for compliance
PCA	Documents BEA and BPR compliance in memorandum to the DCMO through the appropriate IRB in the non-Military Department Components ( <i>e.g.</i> , Defense Agencies)
CMO/DCMO	Determines that the DBS modernizations are compliant to the BEA and meet section 2222 of Reference (a) BPR requirements
	Documents the determination in a letter to the DBSMC through the Certification Authority (CA)
IRB	Recommends certification requests to the IRB and/or CA
IRB Chair	Reviews DBS certification materials
	Recommends certification of the DBS development/modernization and forwards to the CA for certification
	Recommends waivers, if appropriate, as outlined in Reference (a)
CA	Determines criteria and required supporting documentation by which the respective DBS modernization requests will assert BEA and BPR compliance
	Issues waivers, if appropriate, as outlined in Reference (a)
	Certifies DBS development/ modernization requests and forwards to the DBSMC for approval
DBSMC	Approves CA certifications, CMO determinations, and waivers
Test Community	Tests DBS for BEA compliance
BEA Staff	Develop and review compliance criteria
	May conduct BEA audits, as directed

**Table 5: Architecture Compliance Roles and Responsibilities**

## 6.3 Additional Information

### 6.3.1 BEA Assessment and Compliance Process Support

The Architecture & Information Management (A&IM) and the ACART™ teams are available to assist DoD Components with the BEA compliance assessment process, depending on the specific requirement or need. In addition, there is a compliance tutorial that is updated with every BEA publication, along with one-on-one training support that the BEA team can provide. To request assistance send an e-mail to [AskBEA@bta.mil](mailto:AskBEA@bta.mil). Technical help for BEA 8.0 can be found on the BEA website by visiting: [http://www.bta.mil/products/BEA\\_8\\_0/index.htm](http://www.bta.mil/products/BEA_8_0/index.htm) (Reference (m)), then selecting BEA and Technical Help on the menu bar at the top of the page.

### 6.3.2 Technical Standards for Expeditionary Environments

Currently, the BEA compliance process does not require compliance to the DoD Information Technology Standards and Profile Registry (DISR)-mandated StdV-1 Standards Profile. As general guidance only, the DISR technical standards profiling questionnaire related to DBS used in an expeditionary environment is included in the BEA. The profiling questionnaire identifies the mandated standards based on the certifying system requirements for DBS to be deployed in expeditionary environments.

The profiling questions are located on the BEA 8.0 web site (Reference (o)). On the site, select “BEA”, “DODAF Models” on the menu bar, “StdV-1 Standards Profile”, and “Supporting Expeditionary Operating Environment: StdV-1 Profiling Questionnaire Considerations for Deploying Systems in Constrained Environments.”

## Appendix A: References

---

- a) Title 10, United States Code [http://uscode.house.gov/download/title\\_10.shtml](http://uscode.house.gov/download/title_10.shtml)
- b) Directive-Type Memorandum 08-020, “Investment Review Board (IRB) Roles and Responsibilities”, January 26, 2009 <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-020.pdf>
- c) “Interim Acquisition Guidance for Defense Business Systems (DBS)”, November 15, 2010 <https://acc.dau.mil/adl/en-US/408952/file/54480/BCL%20Interim%20Acquisition%20Guidance%20Final.pdf>
- d) “DoD IT Defense Business Systems Investment Review Process: Guidance”, January 2009 <http://www.bta.mil/products/IRB-Guidance-2009.pdf>
- e) “Fiscal Year 2011 Strategic Management Plan; Department of Defense”, December 30, 2010 [http://www.defense.gov/pubs/FY\\_2011\\_SMP\\_12302010.pdf](http://www.defense.gov/pubs/FY_2011_SMP_12302010.pdf)
- f) BEA 8.0 Summary Document, <http://www.us.army.mil/suite/doc/27405957>
- g) Department of Defense Chief Information Officer Memorandum, “Department of Defense (DoD) Information Technology Portfolio Registry (DITPR),” March 17, 2005
- h) “DOD Information Technology Portfolio Repository (DITPR) User’s Guide,” October 30, 2009
- i) BEA 8.0 Automated Compliance Instructions (ACART) <http://www.us.army.mil/suite/doc/27405819>
- j) BEA 8.0 Manual Compliance Process Instructions <http://www.us.army.mil/suite/doc/27406386>
- k) Standard Financial Information Structure (SFIS) Resources: The Common Business Language of DoD: [http://www.bta.mil/SFIS/sfis\\_resources.html](http://www.bta.mil/SFIS/sfis_resources.html)
- l) “Interim Guidance for the Implementation of Section 1072 of the Fiscal Year 2010 National Defense Authorization Act – Business Process Reengineering,” April 1, 2010
- m) BEA 8.0 Website: [http://www.bta.mil/products/BEA\\_8\\_0/index.htm](http://www.bta.mil/products/BEA_8_0/index.htm)
- n) “DoD Architecture Framework, Version 2.0,” Volume I, Volume II, and Volume III, May 28, 2009  
<http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%201.pdf>,  
<http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%202.pdf>,  
<http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%203.pdf>,

## Appendix B: DoDAF Mapping

Starting with BEA 7.0, BEA artifact names were updated to align with DoDAF 2.0 naming conventions, as detailed in Table 6. BEA 8.0 continues with DoDAF 2.0 naming conventions. “DoD Architecture Framework, Version 2.0,” Volume I, Volume II, and Volume III is available at Reference (n).

For purposes of BEA 7.0 and 8.0 Compliance, this update had minimal impact when asserting to the BEA; the objects within each DoDAF 2.0 artifact (e.g. OAs, IEs, Data Attributes and Metadata, Business Rules, DFMIG, and LRP) that system owners are required to scope and assert to remain unchanged.

Before BEA 7.0		BEA 7.0 and After	
DoDAF 1.5 Product Number	DoDAF 1.5 Product Name	DoDAF 2.0 Product Number	DoDAF 2.0 Product Name
OV-5	Operational Node Tree and Activity Model Diagrams	OV-5b	Operational Activity Model
OV-6c	Business Process Diagram	OV-6c	Event-Trace Description
OV-3	Operational Information Exchange Matrix	OV-3	Operational Resource Flow Matrix
LRP	Laws, Regulations, and Policies	Guidance	Laws, Regulations and Policies
	Guidance Statements		Guidance
OV-6a	Operational Rules Model	OV-6a	Operational Rules Model
OV-7	Logical Data Model	DIV-2	Data And Information Viewpoint - Logical Data Model

**Table 6: Architecture Compliance Roles and Responsibilities**

## Appendix C: Definitions

Term	Definition
Architecture Compliance Plan	Provides (1) a detailed assessment of the DBS's current degree of compliance, (2) the key milestones and proposed deadline to achieve full compliance, (3) the required actions to achieve full compliance, and (4) any risks and dependencies that are associated with achieving full BEA compliance.
ACART™	An automated tool used to filter BEA facets in an organized manner to facilitate system compliance
Business Capability Lifecycle	A holistic approach that emphasizes rigorous analysis of requirements to enable rapid delivery of business capabilities to the warfighter in a compressed timeframe. BCL aligns the existing DoD business capability policies by consolidating requirements, acquisition, and BEA compliance into a single oversight structure.
Business Enterprise Architecture	The blueprint to guide and constrain investments by DoD Components as they relate to or impact business operations.
Business Rules	The set of operational rules which define what the DoD business mission must do and cannot do.
Certification Authority	The Certification Authorities are Approval Authorities as defined in section 2222 of Reference (a).
Component	Military Department or agency of the Department of Defense that includes: the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, DoD field activities, and all other organizational entities within the Department of Defense.
Data Attributes	Attributes are characteristics that either identify or describe Entities. Attributes are associated with only one Entity.
Defense Business System	An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management (section 2222 (j)(2) of Reference (a)).

Defense Business System Management Committee	Governance body established by section 186 of Reference (a) to oversee the DBS investment review process required by section 2222 of Reference (a).
Defense Business System Modernization	(A) The acquisition or development of a new defense business system; or (B) any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services). (section 2222 (j)(3) of Reference (a)).
Defense Financial Management Improvement Guidance	A composition of existing federal financial management systems requirements mandated by the FFMA of 1996 and selected internal DoD requirements which help DoD managers comply with a myriad of financial requirements when planning, designing, enhancing, modifying, and implementing financial management systems.
DoD Architecture Framework	The Department of Defense Architecture Framework (DoDAF) is a reference model to organize the Enterprise Architecture (EA) and systems architecture into complementary and consistent views.
DoD Information Technology Portfolio Repository	The Department's authoritative inventory of IT systems.
Entity	The representation of a set of real or abstract things (people, objects, places, events, ideas, etc.) that are recognized as the same type because they share the same characteristics and participate in the same relationships.
Increment	A useful and supportable operational capability that can be effectively developed, produced, acquired, deployed and sustained.
Information Exchange	Listed in the OV-3 and shows the information exchanged between two Operational Nodes.
Initial Operational Capability	The initial point in time when a fully trained and supported user organization of a specified size is equipped with a capability achieving the performance thresholds documented in the Business Case and Acquisition Program Baseline (APB).
Interoperability	The ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner (44 U.S.C. § 3601(6)).
Investment Review Board	The Boards established by an Under Secretary or Assistant Secretary of Defense under authority delegated pursuant to section 2222(f) of Reference (a) to conduct the investment review process required by section 2222(g) of Reference (a).

Laws, Regulations, and Policies	Imposed on people, processes, and systems by various governing bodies. Include constraints mandated by various offices within the Office of the Secretary of Defense (OSD) that apply to the entire Enterprise and may be in the form of regulatory documents (e.g., Office of Management and Budget (OMB) Circulars, Federal Acquisition Regulations (FAR), DoD Financial Management Regulation (FMR), DoD Instructions or Directives, Department of Treasury Financial Manuals, Public Laws, or policies issued in Memorandums or other issuances). Expressed in the BEA via three DoDAF products: (1) As controls on the OV-5 (2) As business rules in the OV-6a and (3) As mappings to the OV-6c and allowing specific LRP to be linked to: OV-6c Processes, OV-6a Business Rules and the Defense Financial Management Improvement Guidance (DFMIG) (includes FFMIA Rules).
Milestone	The point at which a recommendation is made and approval sought regarding starting or continuing an acquisition program, (i.e., proceeding to the next phase).
Operational Activity	A business function that creates or transforms information.
Process Step	A specific task within a business process that produces a certain outcome.

## Appendix D: Acronyms

Acronym	Definition
ACART	Architecture Compliance and Requirements Traceability
ACP	Architecture Compliance Plan
AoA	Analysis of Alternatives
AV	All Viewpoint
BCD	Business Capability Definition
BCL	Business Capability Lifecycle
BEA	Business Enterprise Architecture
BMA	Business Mission Area
BPR	Business Process Reengineering
CA	Certification Authority
CBM	Core Business Mission
CIO	Chief Information Officer
CMO	Chief Management Officer
CV	Capability Viewpoint
DCMO	Deputy Chief Management Officer
DBS	Defense Business System
DBSMC	Defense Business System Management Committee
DFMIG	Defense Financial Management Improvement Guidance
DISR	DoD Information Technology Standards and Profile Registry
DITPR	DoD Information Technology Portfolio Repository
DIV	Data and Information Viewpoint
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDI	Department of Defense Instruction
DTM	Directive-Type Memorandum
E2E	End-to-End business process
EA	Enterprise Architecture
ETP	Enterprise Transition Plan
FFMIA	Federal Financial Management Improvement Act
FMR	Financial Management Regulation
HTML	Hyper Text Markup Language
ICOM	Input Control Output Mechanism
IE	Information Exchange
IM	Investment Management
IOC	Initial Operational Capability
IOT&E	Initial Operational Test and Evaluation
IRB	Investment Review Board

IT	Information Technology
LRP	Laws, Regulations, and Policies
MS	Milestone
OA	Operational Activity
OSD	Office of the Secretary of Defense
OV	Operational Viewpoint
PCA	Pre-Certification Authority
PEO	Program Executive Offices
PM	Program Manager
PSA	Principal Staff Assistant
SMP	Strategic Management Plan
SFIS	Standard Financial Information Structure
StdV	Standards Viewpoint
SV	System Viewpoint
SvcV	Services Viewpoint
USC	United States Code