Business Enterprise Architecture (BEA) Compliance Guidance

-- BEA 5.0 --

May 23, 2008

Version History

Version Number	Document Date	Key Modifications
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

1. Purpose

The purpose of this document is to provide guidance on how to assess and document program compliance with the Enterprise Architecture for Defense Business Systems, currently referred to as the Business Enterprise Architecture (BEA), and how to provide a corrective action plan if a program is not fully compliant. The guidance in this document complements the Department of Defense (DoD) defense business system investment review and certification processes established by section 2222 of title 10, United States Code.

One goal of the BEA is to ensure systems are interoperable at the Enterprise level.

This guidance shall be used by Program Managers (PMs), Component Pre-Certification Authorities (PCAs), and IRBs in the execution of their roles and responsibilities for BEA compliance.

2. Scope

The BEA Compliance Guidance provides the procedures for a program / system asserting compliance to the enterprise architecture for defense business systems, currently the BEA. After reading this Guidance, the reader should have an understanding for the following relevant areas:

- The requirement(s) for compliance;
- Definitions of the roles and responsibilities of those involved in demonstrating and certifying compliance for a defense business system;
- Identification of the artifacts, process, and tools that may facilitate the assertion and certification of compliance, and
- Requirements and structure of an Architecture Compliance Plan (ACP), which must be prepared for any program or system that is not fully compliant.

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

3. Background Information

3.1. Business Enterprise Architecture (BEA)

Section 2222(c) of title 10, United States Code, directs the Secretary of Defense, acting as the Chair of the Defense Business System Management Committee (DBSMC), to develop:

1. *An enterprise architecture to cover all defense business systems, and the functions and activities supported by defense business systems, which shall be sufficiently defined to effectively guide, constrain, and permit implementation of interoperable defense business system solutions and are consistent with policies and procedures established by the Director of the Office of Management and Budget, and;*
2. *A transition plan for implementing the enterprise architecture for defense business systems.*

The BEA is the enterprise architecture for the DoD Business Mission Area (BMA). The BEA contains a set of integrated operational, system, and technical standards that are built using the DoD Architecture Framework (DoDAF). The DoDAF defines a standard way to organize and document an enterprise or system architecture using complementary and consistent views. Within these products are Activities, Processes, Information Exchanges, Data Standards, Business Rules, and Laws, Regulations, and Policies

(LRPs) which focus on the Department's Business Enterprise Priorities (BEPs). These BEPs align to strategic transformational capabilities identified by the Principal Staff Assistants (PSAs).

The specific goals for the BEA are to:

- Describe and establish standard business processes for the DoD BMA as they relate to the six Business Enterprise Priorities (BEPs);
- Establish foundational Data Standards, Business Rules, and LRPs;
- Support DoD investment management criteria in support of systems certification.

The BEA also ensures that policies, procedures, data standards and system interoperability requirements are applied uniformly throughout the Department.

3.2. BEA Compliance

In accordance with section 2222(c) of title 10, United States Code, funds may not be obligated for defense business system modernizations in excess of $1M over a defense business system modernization until they are certified by the Approval Authority/ (Certification Authority (CA)) and approved by the DBSMC.

Component program architectures define linkages to Component-level architectures. Component architectures define their operational, system, and technical standard requirements and are federated and aligned with the BEA.

PCAs are expected to assess their systems against the BEA, their Component architectures, and "other" Component architectures that serve to fill BEA gaps during investment reviews. Program architectures are typically less robust in the early stages of a system's lifecycle and become more extensive as the program matures.

BEA compliance is one element of the IRB certification process and is used by the IRB to assess whether the business investment(s) being reviewed for certification supports DoD Enterprise priorities and requirements.

4. Architecture Compliance

4.1. Compliance Requirement

All defense business system modernizations must comply with the BEA. New versions of the BEA are released annually. Programs shall make every effort to comply with the most recent version of the BEA. While it is difficult to execute a program with changing requirements, PMs shall identify the version of the BEA they will comply with when they forward their program documentation to the IRB for certification. New releases of the BEA should not impact the program for that modernization effort.

Programs must assert compliance to the latest version of the BEA for IRB certifications that occur more than 180 days after its release.

For BEA 5.0, the following improvements were made in support of the BEA compliance process in order to enhance the quality of the results from the compliance process: an Integrated Node Tree was implemented; and detailed data requirements were captured in support of Enterprise Data Initiatives. These improvements not only make the BEA more illustrative of the BMA as a whole, but also establish the data standards necessary to ensure interoperability.

The Integrated Node Tree has been extended with additional un-integrated activities that will be used to categorize systems that previously had no home or were not decomposed enough to distinguish specific differences. The detailed data requirements enable the IRBs to implement and enforce compliance requirements in support of interoperability and data standardization.

As a result of the detailed content added to BEA 5.0, the compliance requirements have been extended down into the data level. This enables limited implementation of data standardization across the Department to ensure interoperability.

For BEA 5.0, the BEPs have defined a finite set of Information Exchanges, Data Synonyms, and/or Attributes that define the specific data requirements. Currently, the requirement is only to assert to the definition of the Data Synonym and Attribute for Compliance. The list of approved Information Exchanges for BEA Compliance is found at the following link: http://www.defenselink.mil/dbt/tools_certification.html. Business Rules have also been identified for Data Synonyms and Attributes. The Business Rules provide clarity on how the data is derived and structured.

4.2. DoD Architecture Framework (DODAF) Products Used for BEA Compliance

In 2004, the Department adopted the DoDAF as the standard framework for all architectures, including the BEA. Systems requesting certification should use the information contained in the specified BEA DoDAF products listed in Table 1 below to conduct their BEA compliance assessments. However, it is the architecture-related information (BEA Objects) contained in these products, and not the products themselves, which are most important for assessing a system's compliance to the BEA.

Table 1. BEA DoDAF Products/Content Used for Compliance Assessments

BEA DoDAF Product	BEA DoDAF Product/Content Name	BEA Object
OV-3/OV-7	Operational Information Exchange Report	Information Exchange/Data Synonym/Attribute
OV-5	Operational Activity Model Diagram and Node Tree Diagram	Operational Activity
OV-6a	Operational Rules Model Diagram	Business Rules
OV-6c	Operational Event-Trace Diagram	Process Steps
LRP	Laws, Regulations, and Policies	LRP

4.3. Compliance Process

The compliance assessment process demonstrates adherence to the BEA Data Synonyms and Attributes, Business Rules and LRPs that are supported by the defense business system being assessed. Ideally, this assessment approach would demonstrate alignment of the business system's relevant DoDAF products (i.e., OV-5, OV-6c, OV-6a, OV-3, and OV-7) to the equivalent BEA products. The compliance assessment process requires analysis and decision-making, and the results may vary from system to system. Figure 1 summarizes the key elements for BEA Compliance.

The BEA compliance assessment and review can result in **four** different findings:

1. Compliant – Able to demonstrate or assert adherence to the BEA Data Synonyms and Attributes, Business Rules, and LRP's.

2. Compliant (non-conflicting) – System contains no capabilities expressed in the BEA or system capabilities are insufficiently defined to access BEA compliance.
3. Planned Compliant – One or more assertions are non-compliant, but a plan is in place to become compliant with the BEA.
4. Non-Compliant – One or more assertions are non-compliant and there is no plan to become compliant with the BEA.

BEA compliance steps shall be documented using one of the following methods:

- The Architecture Compliance and Requirements Traceability (ACART) process for BEA Compliance (Figures 1 and 2)
- The Manual Process for BEA Compliance using BEA HTML (Figure 3)
- A Component or Agency approved software tool containing the BEA

ACART provides one method for assessing BEA compliance and developing corrective action (compliance plans) where required. Any program subject to the IRB certification process may find ACART's capabilities useful in satisfying the requirements of this document. ACART may be accessed at https://acart.bta.mil. Instructions for registration of a candidate program and request for user access are located at this site.

Figure 1. ACART Process for BEA Compliance

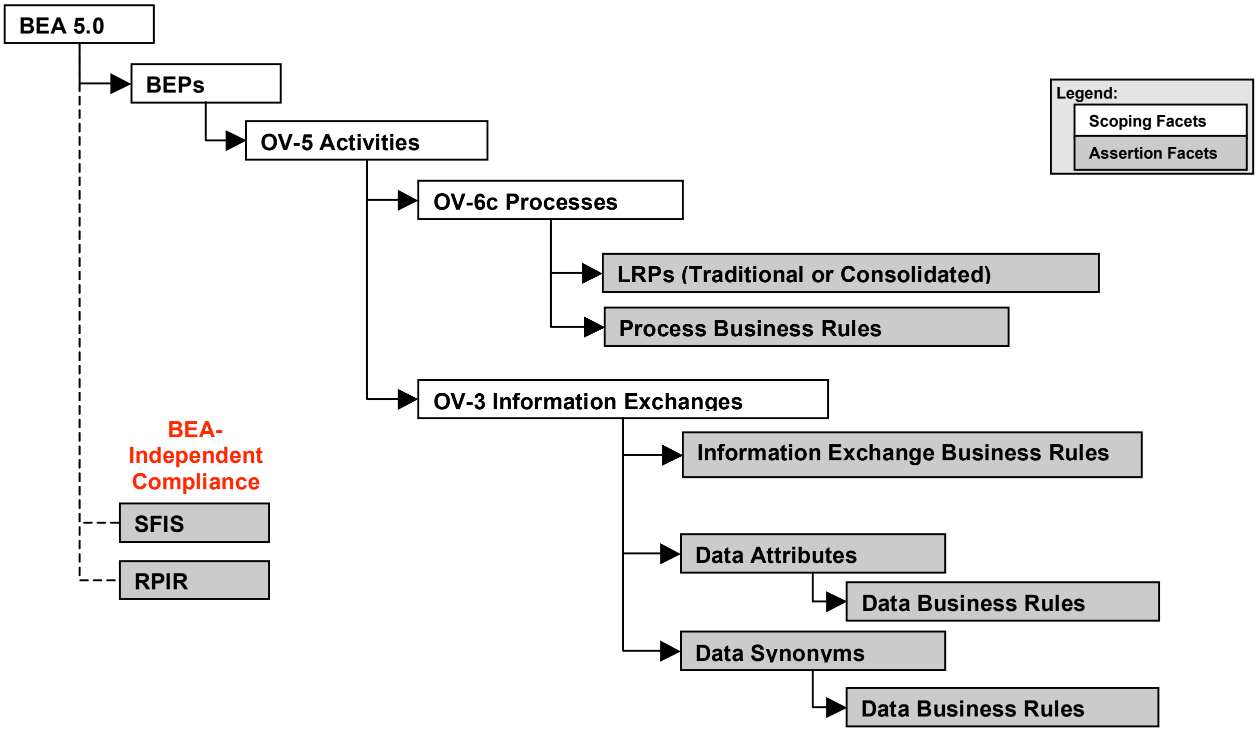

Figure 2. ACART Process for BEA Compliance:

1. **Scope** relevant BEPs for the candidate system. (It is recommended that all BEPs be selected initially if there is any uncertainty about which Operational Activities are relevant)
2. **Scope** relevant leaf-level **Operational Activities** for the candidate system. (Leaf-level activities are identified as "True")
3. **Scope** relevant **Business Processes** linked to the in-scope Operational Activities.
4. **Assert** that the candidate system configuration complies with the process related **Business Rules.**
   a. **Compliance Guidance:** When asserting Compliance to the Process-related Business Rules, the user is asserting that within the context of the Process, the system adheres to the Business Rule definition of the BEA.
5. **Scope and Assert** that the candidate system configuration complies with the process related **Laws, Regulations and Policies** . Assessor may use either the Traditional method (assert at the LRP level) or Consolidated method (assert at the process level).
   a. **Compliance Guidance:** When asserting Compliance to the Process-related LRPs, the user is asserting that within the context of the Process, the system adheres to the LRP description designated by the BEA.
6. **Scope** relevant **Information Exchanges** linked to the in-scope Operational Activities selected above.
7. **Assert** that the candidate system configuration complies with the definition of **Data Synonyms and Attributes** within the information Exchange. (When viewing the Data Synonyms and Attributes select "Show Predecessor" option to display the related Information Exchange)
   a. **Compliance Guidance: Attributes:** When asserting Compliance to the Attributes, the user is asserting that within the context of the Information Exchange, the system produces, consumes, or exchanges the data consistent with the BEA definition of the Attribute.
   b. **Compliance Guidance: Data Synonyms:** When asserting Compliance to the Data Synonyms, the user is asserting that within the context of the Information Exchange, the system produces, consumes, or exchanges the data consistent with the BEA definition of the Data Synonym. The Data Synonym is linked to one or more Attributes.
8. **Assert** that the candidate system configuration complies with the **Information Exchange** related **Business Rules** . (When viewing the Information Exchange Business Rules, select "Show Predecessor" to display the related Business Rules within the context of the Information Exchange)
   a. **Compliance Guidance:** When asserting Compliance to the Information Exchange Related Business Rules, the user is asserting that within the context of the Information Exchange, the system adheres to the Business Rule definition specified by the BEA.
9. **Assert** that the candidate system configuration complies with the **Data Synonym** and **Attribute Business Rules** . (When viewing the Data Synonym and Attribute Business Rule, select "Show Predecessor" to display the related Business Rules within the context of the Data Synonyms and Attributes.)
   a. **Compliance Guidance:** When asserting Compliance to the Data Synonym and Attribute-related Business Rules, the user is asserting that within the context of the Information Exchange and the Data Synonym and Attribute , the system adheres to the Business Rule definition specified by the BEA.
10. Assess Compliance with **SFIS** and **RPIR** Checklists
    a. Relevant areas of the checklist shall be determined by identifying the Category(ies) of the candidate system.
    b. Based on the selected Category(ies) assert whether the candidate system adheres to the requirements of the checklist .
11. **Scope and Assert** the system complies with the relevant Data Standards of the **SFIS Checklist**
    Scope and Assert the system complies with the relevant Data Standards of the **RPIR Checklist**

For those systems that choose not to use ACART for Compliance, manual instructions have been provided, using the BEA HTML for Compliance. Figure 3**,** describes the necessary steps for BEA Compliance:

Figure 3. Manual Process for BEA Compliance using BEA HTML

The following is the manual process for asserting BEA Compliance using the BEA HTML. The assessment may also be manually accomplished using architectural products:

1. ***Select*** *OV-5 Activity Model*
2. ***Select*** *"OV-5 Node Tree" – (Node Tree description will be displayed)*
3. ***Select*** *"BEA Operational Activity Node Tree"*
4. ***Select*** *an Operational Activity that is (1) leaf-level activity (an activity at the lowest point of the hierarchical structure). At this point, Processes and ICOM Arrows are displayed.*
5. *Identify the relevant ICOMs/Information Exchange that your system supports*
6. *To assert to Data Synonyms, Attributes, Data-Synonym - Related Business Rules, and Attribute-Related Business Rules within the context of the Information Exchange, refer to the list of approved Information Exchanges for Compliance:*
   http://www.defenselink.mil/dbt/tools certification.html
   a. *Based on the relevant ICOMs/Information Exchanges identified:*
      i. ***Assert*** *whether your system complies with the Information Exchange - related Business Rules*
      ii. ***Assert*** *whether your system complies with the Data Synonym and Attribute definition within the context of the Information Exchange*
      iii. ***Assert*** *whether your system complies with the Data Synonym-related Business Rules associated to the Information Exchange*
      iv. ***Assert*** *whether your system complies with the Attribute - related Business Rules associated to the Information Exchange*
7. *To assert to Business Rules associated to "Processes"*
   a. *Select a Process*
      i. *Expand "OV-6a Business Rules" and assert whether your system complies with the business rule*
8. *To assert to LRP associated to Processes:*
   a. *Select a Process*
   b. *Select LRP Home on the navigational bar(located on the left side of the web page)*
   c. *Select LRP Reports*
   d. *Select OV-6c*
   e. *Select BPM Process (OV-6c)-LRP Traceability, alphabetic*
   f. *Select letter that the process step name begins with*
      i. *Search process step name, expand the process step and assert whether your system complies with this LRP*
9. *Assess Compliance with Checklists located at the following website:*
   http://www.defenselink.mil/dbt/tools_certification.html
   a. *Relevant areas of the checklist shall be determined by identifying the Category(ies) of the candidate system or feeder system being evaluated.*
   b. *Based on the selected Category(ies) assert whether the candidate system enforces the requirements of the checklist.*
   c. ***Scope and Assert*** *that the system configuration complies with the relevant sections of the* ***SFIS Checklist***
   d. ***Scope and Assert*** *that the system configuration complies with the relevant sections of the* ***RPIR Checklist****.*

4.4. Roles and Responsibilities in Compliance Process

There are a number of people with a role in the BEA assessment and review process. However, the PCA's role in the compliance assessment and review process is extremely important. Under the principle of tiered accountability, PCAs are responsible for assessing compliance with the BEA, the Component architectures, and for pre-certifying that those system investments forwarded to the IRB for certification are compliant to the BEA or request a waiver through an ACP. Table 2 outlines some of the key roles and responsibilities.

Table 2: BEA Compliance Roles and Responsibilities

Role	Responsibility
PM	• Ultimate subject matter experts (SME) for their respective systems • Maintains all information related to the business system requiring approval and certification of DoD funds and/or annual review as specified in section 2222 of title 10, United States Code • Identifies system requirements against the BEA for Compliance
PCA	• Review BEA Compliance results for system certification • Assert, via memorandum, that the system is in compliance with the conditions of obligation of funds as specified in section 2222 of title 10, United States Code
IRB	• Review IRB certification packages. • Recommend approval of certification requests to the DBSMC.

5. Architecture Compliance Plans

As a condition of certification for systems that are not fully compliant to the BEA, the IRB or PCA may require the PM to submit an Architecture Compliance Plan (ACP). For PMs, the ACP will provide a roadmap and a commitment to achieve full BEA compliance. For PCAs, the ACP will provide documentation and assurance that the PMs understand and will comply with the plan's requirements. For IRBs and Transition Planners, the ACP will identify system gaps and help track the business system transformation progress. The PCA shall ensure that key system milestones in the IRB-approved ACP are reflected in the ETP. For all defense business system stakeholders, the ACP provides visibility into critical dependencies that could impact successful system implementation and deployment.

At minimum, ACPs will include:

- A detailed assessment of the system's current degree of compliance;
- The key milestones and proposed deadline to achieve compliance; and,
- The actions needed to achieve compliance and identification of the risks and critical dependencies (if applicable) that are associated with achieving compliance.

ACPs should be supported by documentation that describes the system's current degree of compliance in the following areas:

1) **LRPs** — Identify the applicable laws, regulations and policy requirements applicable to the relevant process steps supported by the system, and the degree to which the system conforms to them;
2) **Process and Data-Related Business Rules** — Identify the applicable business rules from the processes and the Data Synonyms and Attributes supported by the system and the degree to which the system enforces them; and,
3) **Data Synonyms and Attributes** — Identify the applicable Data Synonyms and Attributes relevant to the Information Exchanges supported by the system and the degree to which the system can support them.

ACPs shall be reviewed, approved, and retained by the PCA. If an ACP is required as the result of an approval condition levied by an IRB, copies of PCA-approved plans shall be forwarded to the lead IRB (or Priority Content Area SME) by the designated date. If an ACP is a condition of a PCA approval, the plan shall be retained by the PCA and documented in the PCA memorandum. ACPs should be validated annually and updated to reflect completed actions and milestone revisions. To facilitate transformation efforts, PCAs must ensure that architecture compliance milestones are updated in the ETP and/or their Component Transition Plans as appropriate.

A completed Compliance Assessment and Compliance Plan, as outlined in ACART, are sufficient to meet the requirements of this section. Relevant compliance plan reports in ACART may be used to meet the approval condition.

6. Document Retention

PCAs are encouraged to forward BEA compliance assessment documentation to the IRB support staff in preparation for review at an IRB. Sufficient documentation, which may include BEA and program architectural products, must exist to support the PCA compliance assessment and must be retained by the PCA for validation and audit purposes.

7. Compliance Assessment Support

The BTA Enterprise Integration (EI) support team and the ACART team are available to assist Components with the BEA compliance assessment process. The Enterprise Planning and Integration (EP&I) IRB support team can be contacted through the BTA website (http://www.defenselink.mil/bta/contact.html) for the system certification process. Additional system certification and BEA compliance information can be found at http://www.defenselink.mil/dbt/tools_certification.html.

References

(a) Section 2222 of title 10, United States Code

(b) "DoD Architecture Framework, Version 1.5," Volume I, Volume II, and Volume III, February 9, 2004

(c) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and NSS," May 5, 2004

(d) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and NSS," June 30, 2004

(e) CJCSI Manual 3170.01F, "Operation of the Joint Capabilities Integration and Development System," May 1, 2007

(f) "BMA Federation Strategy and Roadmap," September 28, 2006

Definitions

Term	Definition
Architecture Compliance Plan	An Architecture Compliance Plan is required for systems that are not fully compliant and provides (1) a detailed assessment of the system's current degree of compliance, (2) the required actions to achieve full compliance, (3) the key milestones and proposed deadline to achieve full compliance, and (4) any risks and dependencies that are associated with achieving full BEA compliance.
ACART	The Architecture Compliance and Requirements Traceability (ACART) tool is an automated tool used to filter Business Enterprise Architecture facets in an organized manner to facilitate system compliance. ACART can also be used to create Compliance Plans.
Approval Authority	The designated Principal Staff Assistant with responsibility for review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems. Primary authority for certification of the system.
Attributes	Attributes are characteristics that either identify or describe Entities. Attributes are associated to one and only one Entity.
Business Enterprise Architecture	The EA for Defense Business Systems is the blueprint to guide and constrain investments by DoD Components as they relate to or impact business operations. Enterprise Architecture is as defined in section 3601(4) of title 44, United States Code.
Business Rules	Derivation (Associated to Process Steps): A Business Rule that uses algorithms to compute derivable facts from other terms, facts, derivations, or action assertions. Structural Assertion (Associated to Attributes): A Business Rule that reflects static aspects of the mission or business terms and facts. Action Assertion (Associated to Process Step): Action Assertion: reflect dynamic aspects of the business, and specifies constraints on a process.
Certification Authority	For purposes of this Guidance, Certification Authority means the same as Approval Authority.
Component	DoD Components are defined to be 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, the DoD field activities, and all other organizational and operational entities within the DoD.
Data Synonyms	Data Synonyms are optional terms used to capture alternate names in use in various BEA stakeholder communities. Every Data Synonym must be represented as one or more Attributes related to a specific Information Exchange.
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.
Defense Business System Management Committee	The Committee established by section 186 of title 10, United States Code, to oversee the defense business system investment process required by section 2222 of title 10, United States Code.
Enterprise Architecture	Enterprise Architecture is as defined in section 3601(4) of title 44, United States Code.
Enterprise Transition Plan	An enterprise level document that lays out a roadmap for achieving DoD's business transformation by implementing changes to technology, process, and governance. It contains time-phased milestones, performance metrics, and a statement of resource needs for new and existing systems that are part of the BEA. The ETP also includes a termination schedule for those legacy systems that will be replaced by systems in the target BEA environment.

Term	Definition
	Consistent with tiered accountability, systems that are outside the current scope and organizational span of the BEA are managed within Component transition plans and reflected in the ETP.
Entity	An Entity represents a set of things (people, objects, places, events, ideas, combination of things, etc.) having common characteristics and /or relationships to other Entities.
Federated Architecture	An approach for enterprise architecture development that is composed of a set of coherent but distinct entity architectures; the architectures of separate members of the federation. The members of the federation participate to produce interoperable, effectively integrated enterprise architecture. The federation sets the overarching rules of the federated architecture, defining the policies, practices and legislation to be followed, as well as the inter-federate procedures and processes, data interchanges, and interface standards, to be observed by all members of the federation. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture supporting the mission.
Investment Review Board	Each Approval Authority is required to establish and charter an IRB to provide investment review of its business systems. Each IRB will assess modernization investments relative to their impact on end-to-end business process improvements that support warfighter needs.
Interoperability	The ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner (section 3601(6) of title 44, United States Code).
Milestone	The point at which a recommendation is made and approval sought regarding starting or continuing with the next phase.
Modernization	All costs, of any type of funding, incurred to design, develop, implement/deploy and/or functionally enhance/technically upgrade an information technology system. These costs include, but are not limited to, personnel, equipment, software, supplies, and contracted services from private sector providers, space occupancy, and intra-agency services from within the agency and inter-agency services from other Federal agencies. Does not include sustainment costs. Sources, OMB A-11, A-130.
Operational Activity	A business function that creates or transforms information.
Process Step	A specific task within a business process that produces a certain outcome.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions Department of Defense Architecture Framework (DoDAF).
Tiered Accountability	A management approach, whereby DoD Components are empowered with responsibility and accountability for business investment management.

Acronyms

Acronym	Definition
ACART	Architecture Compliance and Requirements Traceability
ACP	Architecture Compliance Plan
BEA	Business Enterprise Architecture
BEP	Business Enterprise Priority
BMA	Business Mission Area
BTA	Business Transformation Agency
CA	Certification Authority
DBSMC	Defense Business System Management Committee
DITPR	Defense Information Technology Portfolio Repository
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
EA	Enterprise Architecture
EHRIS	Enterprise Human Resource Information Standard
EI	Enterprise Integration
EP&I	Enterprise Planning & Investment
ETP	Enterprise Transition Plan
FV	Financial Visibility
HTML	Hyper Text Markup Language
IRB	Investment Review Board
IT	Information Technology
LRP	Laws Regulations and Policies
OV	Operational View
PCA	Pre-Certification Authority
PSA	Principal Staff Assistant
PM	Program Manager
PV	Personnel Visibility
RPI	Real Property Inventory
RPIR	Real Property Inventory Requirements
SFIS	Standard Financial Information Structure
SME	Subject Matter Expert