



BTA
BUSINESS TRANSFORMATION AGENCY

DoD IT Business Systems Investment Review Process

Business Enterprise Architecture (BEA) Compliance Guidance

April 10, 2006

Table of Contents

- Introduction 1**
 - Purpose.....1**
 - Scope.....1**
 - Effective BEA Version1**

- Architecture Overview 2**
 - Background.....2**
 - Architecture Compliance Objectives.....2**
 - Federated Architecture & Tiered Accountability2**
 - DoD Architecture Framework3**

- Architecture Compliance5**
 - Conditions For Certification5**
 - PCA Role In Compliance Process5**
 - Compliance Defined5**
 - Retained Documentation7**
 - Compliance Assessment Approach.....8**
 - System Certification Decision Criteria.....9**
 - Architecture Compliance Plans10**
 - Compliance Assessment Support10**

- References 11**

- Definitions12**

- Acronyms.....16**

Introduction

Purpose

The purpose of this document is to define Business Enterprise Architecture (BEA) compliance as it relates to the Department of Defense (DoD) Information Technology (IT) business system investment review and certification processes established to meet the provisions of the National Defense Authorization Act (NDAA) of FY 2005 [reference (a)]. This guidance is to be used by Program Managers (PMs), Component Pre-Certification Authorities (PCAs), and the Office of the Secretary of Defense (OSD) Investment Review Boards (IRBs) to execute their roles and responsibilities related to BEA compliance assessments. This BEA Compliance Guidance complements and is aligned to the DoD IT Business Systems Investment Certification and Annual Review Process User Guidance, and the DoD Investment Review Process Overview and Concept of Operations for Investment Review Boards, commonly referred to as the IRB CONOPS.

Scope

This guidance provides the background, objectives and process for assessing BEA compliance for business systems and initiatives. It defines the key business transformation principles of “tiered accountability” and “federated architecture” and describes the:

- (1) Interrelationships among Program, Component, and Enterprise Architectures;
- (2) Architecture products necessary to assess compliance;
- (3) Process used by PCAs to assess compliance;
- (4) PCA role in compliance assessments;
- (5) Compliance categories to be used by the PCAs; and
- (6) Purpose and content of an Architecture Compliance Plan.

This guidance does not establish DoD architecture development requirements and policies contained in references (b), (c), (d), and (e).

Effective BEA Version

The effective version of the BEA to be used for architecture assessments is the current version. However, there will be instances when a compliance assessment is initiated based on a version of the architecture that is no longer current by the time the certification approval is completed. A compliance assessment may also be initiated immediately after a new major release and the architecture compliance staff may not have had time to fully understand the content of a new BEA release.

For these reasons, assessments against a previous BEA version will generally be accepted as long as the completed certification is submitted within six (6) months of the most current BEA release date. In addition, BEA compliance will be reassessed during the annual review for systems that are certified for multiple years. For planning purposes, Components should expect to demonstrate compliance with the following versions of the BEA within the timeframe indicated:

- FY06: BEA V3.0
- FY07: BEA V3.1
- FY08: BEA V4.0

Effective July 1, 2006, systems entering the IRB Annual Review process should demonstrate compliance with BEA V3.1



Architecture Overview

Background

The NDAA of FY 2005 prescribes the establishment of IRBs and requires the Defense Business Systems Management Committee (DBSMC) to develop a BEA to guide and constrain DoD business system investments and a transition plan to implement the architecture.

The BEA is an Enterprise-level architecture that contains a set of integrated DoD Architecture Framework (DoDAF) operations, systems and technical standard views, which depict specific, high priority Business Enterprise Priorities (BEPs) that align to strategic transformational capabilities identified by the business enterprise leadership. The BEA is a critical component of the IRB process and is to be used at each level of investment review to assess whether business investments going through the certification process support DoD Enterprise priorities and requirements. Summary results of these investment reviews are reported annually to Congress.

BEA 3.0 is a foundational architecture that was approved by the DBSMC on September 28, 2005. Regular updates to this release are planned and will incorporate new requirements as defined by the BEPs; accordingly, BEA compliance guidance will be updated as necessary to reflect new versions of the architecture.

Architecture Compliance Objectives

By law, the BEA is to be used during the investment review process to ensure that DoD implements defense business systems to provide an information infrastructure that, at a minimum, enables the Department to—

- (A) *comply with all Federal accounting, financial management, and reporting requirements;*
- (B) *produce timely, accurate, and reliable financial information for management purposes on a routine basis;*
- (C) *integrate budget, accounting, and program information and systems; and*
- (D) *provide for the systematic measurement of performance, including the ability to produce timely, relevant, and reliable cost information.*

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

Federated Architecture & Tiered Accountability

There are many architectures within the DoD enterprise which comprise a “federation” of architectures including the BEA, Component architectures, and Program architectures.

The BEA is an **Enterprise-level architecture** that reflects corporate DoD priorities and requirements for business systems, and provides a common framework to ensure that key information is available to DoD decision-makers Department-wide. The BEA is developed and maintained by the Business Transformation Agency (BTA), which reports to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)), and serves the interests of the entire Business Mission Area (BMA) of the DoD.

Under the principle of “tiered accountability,” DoD Components are responsible for defining and building their own architectures. **Component architectures** reflect critical Component capabilities and are used to



enforce compliance with Component-specific requirements that are necessary to achieve their transformation objectives.

Finally, systems are expected to have **program architectures** that define their operational, system, and technical requirements. Program architectures are typically less robust in the early stages of a system’s lifecycle and become more extensive as the program matures.

Collectively, these architectures establish a **federation of architectures** that can be integrated to and align with the BEA business capabilities, which are reflected in the BEA activities, business rules, and data entities. Once the integration and alignment of these Component- and Program-level architectures have been validated to the BEA, investments that are assessed against and compliant with them would also be compliant with the BEA. Until this validation has occurred, PCAs are expected to assess their systems against both the BEA and their Component architectures during investment reviews.

DoD Architecture Framework

Integrated architecture products are required to support many purposes within the DoD. Guidance related to the development and maintenance of these products is described in several DoD policy documents [references (b), (c), (d), and (e)]. The BEA complies with the applicable DoD policies and includes an integrated set of DoD Architecture Framework (DoDAF) products (e.g. System views (SVs), Operational Views (OVs) and Technical Views (TVs)), but not all of these products are necessary to evaluate business investments. Programs requesting certification should use the information contained in the specified BEA DoDAF products listed in Table 1 below to conduct their BEA compliance assessments.

Table 1. BEA DoDAF Products Used for Compliance Assessments

BEA DoDAF Product	BEA DoDAF Product Name	Used for Compliance
AV-1	Overview and Summary Information	
AV-2	Integrated Dictionary	
OV-2	Operational Node Connectivity Diagram	
OV-3	Operational Information Exchange Report	X
OV-5	Operational Activity Model Diagram and Node Tree Diagram	X
OV-6a	Operational Rules Model Diagram	X
OV-6c	Operational Event-Trace Diagram	X
OV-7	Logical Data Model Diagram	X
SV-1	Systems Interface Description	
SV-5	Operational Activity to System Function Traceability Matrix	X
SV-6	System Data Exchange Diagram	
TV-1	Technical Standards Profile	

Systems are also expected to have integrated architectures, and the DoD has adopted the DoDAF as the standard framework for all architectures developed after 2004. However, it is the architecture-related information contained in these products not the products themselves that is most important for assessing a system or initiative’s compliance to the BEA. Table 2 identifies the program-specific DoDAF products to be used to facilitate compliance assessments at various points in the program’s lifecycle [reference (e)]. As the system matures, more documentation and a greater degree of compliance are required.



Table 2. Program-Specific DoDAF Products by System Lifecycle Milestones

DoDAF Product*	Pre-Milestone A	Milestone A to B	Milestone B to C	Post-Milestone C
OV-3				X
OV-5		X	X	X
OV-6a			X	X
OV-6c			X	X
OV-7				X
SV-5				X

*It should be noted that, as long as compliance can be demonstrated utilizing the process outlined in this document, program-specific DoDAF products are not expected to be developed for the sole purpose of conducting BEA compliance assessments. PCAs may use other appropriate system documentation for systems that have not created all of the specified DoDAF products.



Architecture Compliance

Conditions for Certification

The NDAA requires that funds obligated for defense business system modernizations in excess of \$1M be certified by the designated OSD IRB and approved by the DBSMC [reference (a)]. Systems can only be certified and approved if the investment is:

- (A) in compliance with the enterprise architecture; and/or
- (B) necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or
- (C) 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.

While the certification process focuses only on individual system modernizations, the BEA compliance process takes into consideration the full business system functionality. In other words, both the modernization and the system itself must be BEA compliant in order to be assessed as compliant.

PCA Role in Compliance Process

The PCA's role in the compliance assessment process is extremely important. Under the principle of tiered accountability, PCAs are responsible for assessing compliance with the BEA and the Component architectures, and for pre-certifying that those systems forwarded to the IRB for certification meet one of the conditions for certification described above.

Compliance Defined

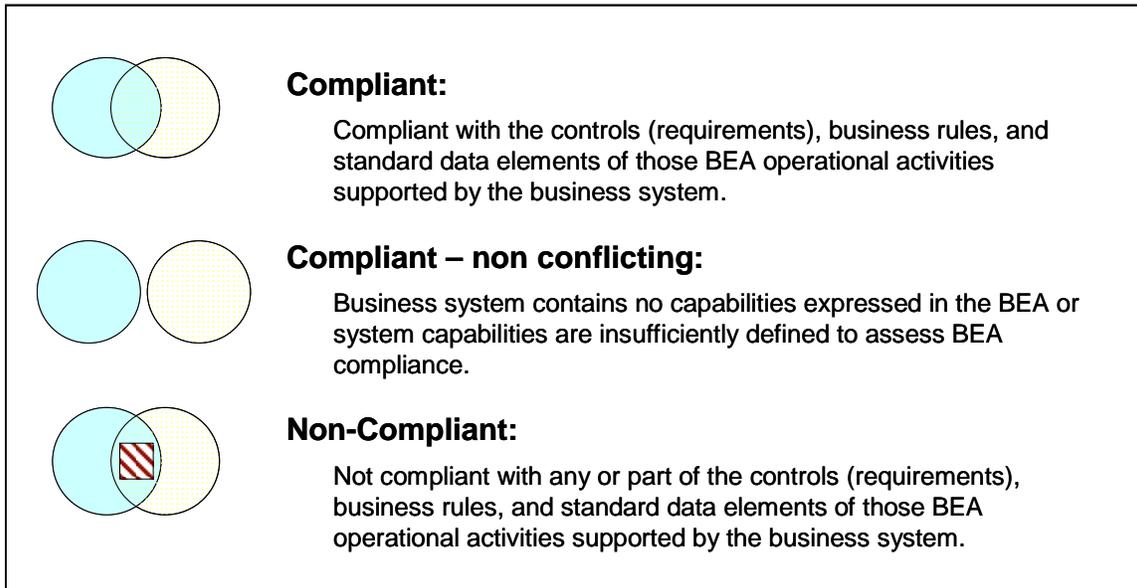
For the FY2007 investment review cycle, architecture compliance is defined as *adherence to the controls (requirements), business rules, and standard data elements of those BEA operational activities that are supported by the system being assessed.*

BEA compliance assessments fall within one of the following categories as shown in Figure 1, and are described in more detail in the sections below:

- **Compliant**
 - Compliant; OR
 - Compliant with Conditions
- **Compliant – non conflicting**
 - Supports no BEA capabilities; OR
 - Premature in system's lifecycle to assess against BEA capabilities
- **Non-Compliant**
 - Does not meet NDAA Condition (A) requirements



Figure 1. BEA Compliance Levels



Compliant (NDAAs Certification Category A)

Systems that are fully compliant with the applicable BEA controls (requirements), business rules and standard data elements are assessed as “Compliant.” These systems meet NDAAs certification category (A). In most cases, a business system will only support a subset of the operational activities in the BEA or will include operational activities in excess of those captured within the BEA. It is important to note that compliance is only assessed against those BEA operational activities (and corresponding requirements, business rules, and standard data elements) supported by the system.

Compliant with Conditions (NDAAs Certification Category A)

Systems that are not fully compliant with the BEA controls (requirements), business rules, and standard data elements at the time of certification, but expect to be fully compliant in the future may be assessed as “Compliant with Conditions” if sound reasons exist to certify the system—including the ability to meet the desired conditions in a reasonable timeframe. This assessment category requires PCAs to:

- Identify the conditions under which the system should be certified;
- Identify the date on which the conditions expect to be satisfied;
- State any risks or dependencies for meeting the conditions;
- Generate and retain documentation that substantiates the program’s commitment to meet the conditions (i.e., an architecture compliance plan); and
- Monitor the system to ensure it meets the stated conditions on time.

The PCA should document the conditions, the target date for meeting the conditions, and the risks or dependencies of the conditions in the PCA letter. Additional conditions may be assigned at any point in the certification and approval process by the Certification Authority (CA) or the DBSMC, respectively.

Compliant - Non-Conflicting (NDAA Certification Category A)

Systems that are not associated with operational activities expressed in the BEA or their system capabilities have not been sufficiently defined to assess BEA compliance (i.e., during initial stage of system development life cycle) are assessed as “Compliant – Non-Conflicting.” For purposes of NDAA compliance, systems certified as Compliant – Non-Conflicting are considered compliant, but that status is subject to change as the architecture and/or the system matures. Depending on the circumstances, cost, and level of risk, systems certified in this category will be monitored at least annually (i.e., during annual review process or when the next year’s funds are requested) to verify their BEA compliance status.

Non-Compliant (Does not meet NDAA Certification Category (A))

Systems that do not satisfy NDAA Certification Category (A) requirements are “non-compliant” to the BEA but they may be certified if they meet one of the following NDAA certification categories:

- **NDAA Certification Category (B)** - Necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or
- **NDAA Certification Category (C)** - 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.

The Department’s goal is for all non-national-security systems (including systems in the development or acquisition phases) to be fully compliant in accordance with *NDAA Certification Category (A)*. However, since the BEA is a “to be” architecture, many currently deployed systems may not fully comply with the BEA. From a PM’s perspective, a program can only obligate funds in excess of \$1M if the system is certified and approved as either Compliant, Compliant with Conditions, Compliant – Non-Conflicting, or meets NDAA certification category (B) or (C). Systems assessed as Compliant or Compliant with Conditions result in the most desirable outcome for both the Department and the PMs. Although the NDAA does not explicitly state that system approvals may contain approval conditions, they are implied and recognized as the only way that the Department can realistically continue to operate while it evolves toward its target state.

Retained Documentation

PCAs are not required to forward system compliance assessment documentation to OSD. However, sufficient documentation, which may include BEA and program architectural products, must exist to support the PCA compliance assessment and should be retained by the PCA for validation and audit purposes.

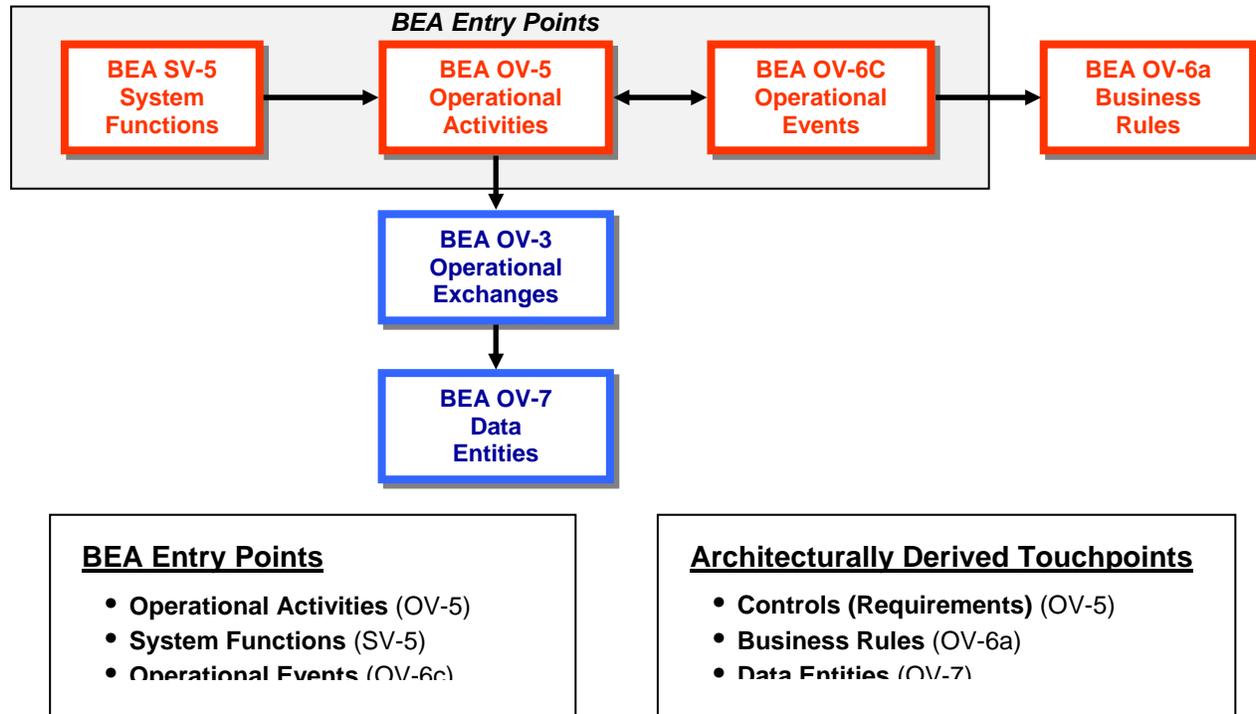
In accordance with the IRB Guidance, Components are required to create and maintain each system’s BEA profile in the DoD Information Technology Portfolio Repository (DITPR). PCAs must ensure this information exists in DITPR.



Compliance Assessment Approach

The compliance assessment process demonstrates adherence to the controls (requirements), business rules, and standard data elements of those BEA operational activities that are supported by the business system being assessed. Ideally, this assessment approach would demonstrate alignment of a business system's relevant DoDAF products (i.e., SV-5, OV-5, OV-6c, OV-6a, OV-3, and OV-7) to the equivalent BEA products. Figure 2 depicts the relationships of these BEA products.

Figure 2. BEA Product Relationships



The compliance assessment process requires analysis and decision-making, and the results may vary from system to system. At a high level, the following four basic steps should be used to assess BEA compliance:

- 1) Identify the system's **known** activities or processes;
- 2) Derive the **possible** BEA touchpoints with system's activities or processes;
- 3) Determine the **relevant** BEA touchpoints with system's activities or processes; and
- 4) Assess BEA compliance against the relevant touchpoints.

The first step in the compliance assessment process is to identify the system's **known** operational activities or business processes, which should be documented in the system's architecture products. Next, compare these activities to the most recent version of the BEA DoDAF Products to derive the **possible** BEA activities or touchpoints that match or contain some element of the system's activities. From the possible BEA touchpoints, determine the **relevant** touchpoints for the system being assessed, and assess BEA compliance against those touchpoints.

PCAs may assess business systems without formal DoDAF documentation, which may be the case in the early design phases of a new system or for legacy systems that were developed before DoDAF

documentation requirements were established. However, BEA alignment must be demonstrated using other relevant system documentation.

The high level compliance assessment approach described above is summarized in the compliance assessment process outlined in Figure 3.

Figure 3. Compliance Assessment Process

- 1) *Identify Relevant Activities*
 - a) *Identify those OV-5 Node Tree Activities within the BEA that are supported by the candidate system using one of the following methods:*
 - i) *Select Activities directly from the OV-5 Activity Model;*
 - ii) *Derive Activities from the capabilities or system functions listed in the SV-5 Activity-Capability-Function Matrix; or*
 - iii) *Derive Activities from the OV-6c Process Model.*
- 2) *Assess Activity Control Compliance*
 - a) *Identify controls for each applicable OV-5 Activity that refer to policy, law, and regulatory requirements; and*
 - b) *Assess whether the system enforces or will enforce these controls as part of its functionality.*
- 3) *Assess Business Rule Compliance*
 - a) *Identify the corresponding OV-6c Processes for each activity selected;*
 - b) *Identify the OV-6a Business Rules that control each OV-6c Process; and*
 - c) *Assess whether the system enforces or will enforce the Business Rules as part of its functionality.*
- 4) *Assess Data Compliance*
 - a) *Identify the OV-5 Inputs and Outputs that are applicable to the system for each activity selected;*
 - b) *Identify the OV-3 Information Exchange Requirements (IER) that corresponds to the full set of Inputs and Outputs, and compile a corresponding list of OV-7 Data Entities that supports these data exchanges; and*
 - c) *Assess whether these system OV-7 Data Entities conform with their corresponding OV-7 Data Entities in the BEA. Compliance will be determined by assessing whether the top level definitions of the Data Entities are in agreement. Data Attributes will not be assessed for compliance at this time.*

System Certification Decision Criteria

The CA's decision to certify a system relies heavily on architecture compliance; however, other criteria may also be considered in the decision-making process (i.e., risk, business case, and functional redundancy) as described in the following examples:

- An investment that is fully compliant to the BEA **may not be certified** due to unacceptable risk, insufficient business case, or significant functional redundancy;
- An investment that is not fully compliant to the BEA and *plans to become fully compliant* may be **certified as Compliant with Conditions** if an "Architecture Compliance Plan" or other acceptable documentation is submitted and approved by the PCA; or

- An investment that is non-compliant to the BEA and *does not plan to become fully compliant* may be **certified if it meets NDAA Certification Category (B) or (C)**.

Architecture Compliance Plans

As a condition of certification for systems that are not fully compliant, the PCA may require the PM to submit an Architecture Compliance Plan. Architecture Compliance Plans have many uses and benefits. For the PMs, they provide a roadmap and a commitment to achieve full BEA compliance. For PCAs, they provide documentation and assurance that the PMs understand and will comply with the plan's requirements. For IRBs and Transition Planners, they identify system gaps and help track the business system transformation progress. For all business system stakeholders, they provide visibility into critical dependencies that could impact successful system implementation and deployment.

Architecture Compliance Plans should include:

- 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 with the BEA; and,
- 4) The risks and critical dependencies (if applicable) that are associated with achieving full BEA compliance.

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

- 1) **Activity Controls**—Identify the applicable policies, laws, and regulatory requirements identified as controls on the BEA OV-5 Activities that are supported by the system, and the degree to which the system conforms to them;
- 2) **Business Rules**—Identify the applicable business rules from the BEA OV-6c processes that are supported by the system and the degree to which the system enforces them; and,
- 3) **Standard Data Elements**—Identify the applicable data elements from the BEA OV-7 (which should align through the corresponding OV-3 Information Exchange Requirements (IERs) to the applicable BEA OV-5 Inputs and Outputs) and applicable data standards (i.e., SFIS) that are supported by the system and the degree to which the system conforms to them.

Architecture Compliance Plans should be reviewed, approved, and retained by the PCA. If a Compliance Plan is required as result of an approval condition levied at the IRB level, then copies of PCA approved plans should be forwarded to the lead IRB by the designated date. (Normally this will be done in conjunction with an annual review.) If an Architecture Compliance Plan was a condition of a PCA approval, then the plan should be retained by the PCA and documented in the PCA letter. Plans should be validated annually and updated to reflect completed actions and milestone revisions. To facilitate transformation efforts, PCAs should ensure that architecture compliance milestones are incorporated into their Component Transition Plans as appropriate.

Compliance Assessment Support

The BTA Investment Management (IM) support team is available to assist Components with the BEA compliance assessment process. The IM support team can be contacted through the BTA website at [Contact Business Transformation](#), and additional information on system certification and BEA compliance can be found at [System Certification Process](#).

References

- (a) Section 332, [Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005](#)
- (b) “DoD Architecture Framework, Version 1.0,” [Volume I](#), [Volume II](#), and [Volume III](#), February 9, 2004
- (c) [DoD Directive 4630.5](#), 5 May 2004, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- (d) [DoD Instruction 4630.8](#), 30 June 2004, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- (e) [CJCS Manual 3170.01B](#), 11 May 2005, Operation of the Joint Capabilities Integration and Development System



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.
Business Capability	The ability to execute a specific course of action. It can be a single business enabler or a combination of business enablers (e.g. business processes, policies, people, tools or systems, information) that assists an organization in delivering value to its customer.
Business Enterprise Architecture	The Business Enterprise Architecture (BEA) is a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. It will provide the basis for the planning, development, and implementation of business management systems that comply with Federal mandates and requirements, and will produce accurate, reliable, timely, and compliant information for DoD staff. PSAs will define the level of specificity for their Core Business Mission areas. In some cases, the BEA will include separately maintained CBM-specific architecture and requirements.
Business Mission Area	A defined area of responsibility with function and processes that contribute to mission accomplishment.
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. (FY05 NDAA) In addition, the DODD 8500.1 further defines a system as a "set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information."
Business System Modernization Investment	The acquisition or development of a new defense business system; or any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services).
Capability	The ability to execute a specified course of action. It is defined by an operational user and expressed in broad terms in the format of an Initial Capabilities Document (ICD), or a Doctrine, Organization, Training, Material, Personnel, and Facilities (DOTMLPF) change recommendation.
Certification 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. P&R - USD (Personnel & Readiness) AT&L - USD (Acquisition, Technology & Logistics) FM - USD (Comptroller) NII - ASD (Networks and Information Integration)



Term	Definition
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.
Core Business Mission	A defined area of responsibility with functions and processes that contribute to mission accomplishment
Defense Business Systems Management Committee	Chaired by the Deputy Secretary of Defense, it is the highest authority providing top-level governance to coordinate defense business system modernization and to link improvements in business capabilities to the Warfighter. Membership includes: Secretaries of the Military Departments and heads of the Defense Agencies; the USD (AT&L), USD (C), USD (P&R); ASD (NII/CIO); Vice Chairman of the Joint Chiefs of Staff; Commander (USTRANSCOM); and Commander (JFCOM).
DoD Enterprise Systems	Systems that have been identified to become the standard across the Department of Defense
DoD 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. 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.
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 an 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 that supports that mission.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the an executive agency (DoD). For purposes of the preceding sentence, equipment is used by an executive agency (DoD) or the equipment is used directly by the DoD or is used by a contractor under a contract with the executive agency (DoD) which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.



Term	Definition
Information Technology (IT) System	<p>Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Any Acquisition Category (ACAT) system that meets these criteria, anything categorized as a National Security System (NSS) or a Mission Assurance Category (MAC) level is, by definition, considered to be an IT system. Other types of IT systems include:</p> <ul style="list-style-type: none"> • DoD-wide, Joint systems • Federal System used by DoD or supported by DoD • DoD System used as a Federal System • Multi- System • Standard System • Major Command Standard System (Echelon 2 or equivalent for Navy and Marine Corps) • Below Major Command System (below Echelon 2 or equivalent for Navy and Marine Corps) • Data Stores/Data Warehouses • Enclaves • Portals (Enterprise) • Automated Information System (AIS) Application
Investment Review Board	<p>Each Certification 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. IRB membership includes representatives from the Components, combatant Commands, and the Joint Chiefs of Staff.</p>
Milestone	<p>The point at which a recommendation is made and approval sought regarding starting or continuing with the next phase.</p>
Modernization	<p>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, contracted services from private sector providers, space occupancy, 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</p>
National Defense Authorization Act for FY05	<p>With the National Defense Authorization Act of 2005 (NDAA), Congress provided the Department a mandated governance structure to provide oversight and direction of Defense business systems developmental activities.</p>



Term	Definition
System	<p>Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.</p> <p>Sub-system: A distinct element of a system that can stand alone outside of its system environment</p> <p>Module: A distinct element of a system that cannot stand alone outside of its system environment.</p> <p>Family of Systems: A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.</p> <p>System of Systems: A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.</p>
Tiered Accountability	An approach to business transformation that is based on dividing the planning and management of programs and initiatives between Enterprise and Component levels.



Acronyms

Acronym	Definition
AT&L	Acquisition, Technology and Logistics
BEA	Business Enterprise Architecture
BEP	Business Enterprise Priority
BMA	Business Mission Area
BTA	Business Transformation Agency
CA	Certification Authority
CONOPS	Concept of Operations
DBSMC	Defense Business Systems Management Committee
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
ETP	Enterprise Transition Plan
FY	Fiscal Year
IM	Investment Management
IER	Information Exchange Requirement
IRB	Investment Review Board
IT	Information Technology
NDAA	National Defense Authorization Act
OSD	Office of the Secretary of Defense
PCA	Pre-Certification Authority
PM	Program Managers
SFIS	Standard Financial Information Structure
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics

