Army Business System IT Certification

The Army Business System IT Certification process is a very structured review process that includes multiple responsible offices and culminates with the certification of funds by the Defense Business Systems Management Council (DBSMC). The certification process is largely driven by statutory requirements along with OSD and Army implementing instructions. This paper will provide an elementary understanding of the process and is intended to accompany a presentation which will inform the Under Secretary of the Army of his role in IT certification acting as the Chief Management Officer of the Army.

Statutory Basis for IT Certification

In addition to the Title 10 requirements for the Office of the Secretary of the Army to provide Information Management and Financial Management, Congress has passed legislation that requires the Army to follow specified procedures for IT management and investments. The first legislative mandate was in 1996 with the Clinger-Cohen Act (CCA) (also called the Fiscal Year 1996 National Defense Authorization Act (FY96 NDAA). This act established the requirement for:

- All Federal agencies to incorporate a more structured process for reviewing Information Technology (IT) investments
- Federal agencies to designate a Chief Information Officer
- Directs the Office of Management and Budget (OMB) to create the Federal Enterprise Architecture (FEA)

OMB created implementation guidance in the form of OMB Circular A-123, which requires Federal agencies to submit a business case (Exhibit 300) for major IT investments as part of their annual budget submission.

The next major legislative mandate was the Fiscal Year 2005 National Defense Authorization Act (FY2005 NDAA) which directed Department of Defense to establish the Defense Business Systems Management Council (DBSMC) and specified Internal Review Boards (IRBs) with specific requirements for reviewing investments of IT modernization requiring over $1M. Subsequently, this requirement has been interpreted to mean requiring over $1M of Research, Development, Testing and Evaluation (RDT&E) funds in a single year or cumulatively over multiple years. It can also include the expenditure of over $1M in Other Procurement Army (OPA) funds for significant enhancements to existing IT systems.

The FY2005 NDAA requires the IRBs to review and approve IT systems modernization and mandates that the DBSMC "certify" the investment prior to the obligation of funds. Specifically the Congressional Language is as follows:

(a) In General.--(1) Chapter 131 of title 10, United States Code, is amended by inserting before section 2223 the following new section:

``Sec. 2222. Defense business systems: architecture, accountability, and modernization

``(a) Conditions for Obligation of Funds for Defense Business System Modernization.--Effective <<NOTE: Effective date.>> October 1, 2005, funds appropriated to the Department of Defense may not be obligated for a defense business system modernization that will have a total cost in excess of $1,000,000 unless--

``(1) the approval authority designated for the defense business system certifies to the Defense Business Systems Management Committee established by section 186 of this title that the defense business system modernization--

``(A) is in compliance with the enterprise architecture developed under subsection (c);

``(B) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or

``(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; and

``(2) the certification by the approval authority is approved by the Defense Business Systems Management Committee.

``(b) Obligation of Funds in Violation of Requirements.--The obligation of Department of Defense funds for a business system modernization in excess of the amount specified in subsection (a) that has not been certified and approved in accordance with such subsection is a violation of section 1341(a)(1)(A) of title 31.

More recently, Congress has passed laws as part of the FY2008 and FY2009 National Defense Authorization Acts which have created the OSD Chief Management Office (CMO), Deputy CMO and Business Transformation Agency (BTA) as well as the Chief Management Offices and Office of Business Transformation (OBT) for each Military Service. The duties outlined within each of these Laws specifically address IT investment review responsibilities.

The Fiscal Year 2010 National Defense Authorization Act (FY2010 NDAA) added a specifically stated requirement for the CMO of the Military Services to "certify" that Business Process Re-engineering (BPR) had been completed for all major IT investments. Because of the criteria within the FY2010 NDAA language, the OSD implementation guidance has equated the BPR requirement with systems that have been certified by the DBSMC.

Criteria for OSD Business Systems

The OSD implementation of the FY2005 NDAA requirements includes the definition of what is a "business system." In practice, the Army has followed the OSD definition of business systems.

As the Army has matured it's IT management we have questioned whether the OSD definition applies within the Army environment. The CMO legislation points towards a broader definition of Army Business Management than the DBSMC requirements and may include other "business" systems some of which are not required to go before the DBSMC review process.

OSD and Army Policies

The Office of the Secretary of Defense (OSD) and the Department of the Army (DA) have established review procedures to implement the legislative requirements referenced above. OSD has published Directive-Type Memorandum (DTM) 08-020, Investment Review Board Roles and Responsibilities, as their guidance for IRB and DBSMC review procedures. Department of Defense developed and published the DOD Architectural Framework (DODAF) to establish a technical guide for development of IT systems within a common architectural framework. All major IT systems must comply with the DODAF as part of the review process.

The Army has developed an SOP to implement the rigorous review process. The following steps outline the high-level requirements of the Army IT review process:

1. Investment proponent develops the business case and architectural documents to describe the system's functional and technical requirements.
2. Domain reviews business case for viability, redundancy and alignment to the Transformation plan. Domain hold governance boards and reviews investment.
3. Business Case is presented to OBT for review and approval.
4. Investment proponent indentifies funding through the PPBE process.
5. Investment proponent submits certification documents to Army Portfolio Management Solution (APMS).
6. Domain reviews certification documents and creates the domain assertion memorandum and uploads to APMS. Domain also ensures the investment is included in the Enterprise Transition Plan or Domain Transformation Plan.
7. Business Certification Team reviews package for data quality and adjudication and sends out for Army wide staffing and concurrence.
8. The following offices review certification package: Army Architecture Integration Center (AAIC); Army Budget Office (ABO); CIO/G-6 Acquisition Compliance and Certification (ACC); CIO/G-6 Information Resource Integration Directorate (IRI); Army Network Enterprise Technology Command (NETCOM), CIO/G-6 Privacy Office, Office of the Deputy Assistant Secretary of the Army for Cost and Economics (ODASA-CE).
9. OBT reviews and garners CMO signature. Package is uploaded to IRB portal.
10. Respective IRB reviews.
11. DBSMC Reviews.

These procedures are required for the initial approval of all IT investments that meet the OSD defined criteria. Additionally systems are required to be reviewed annually, each time additional funds are required and de-certification when funds will not be expended in a specific year.

Under the current DBSMC procedures the Army has certified 97 IT systems since the process was first implemented. Currently the Army has 53 IT systems currently under modernization or being reviewed as a special interest item by the DBSMC process. The distribution of these systems by OSD IRB categories are:

OSD IRB	Number of Army IT Systems Currently being Managed
Financial Management (FM)	3
Real Property & Installation Lifecycle Management (RP&ILM);	18
Human Resources Management (HRM)	21
Weapon System Lifecycle Management/Materiel Supply and Service Management (WSLM/MSSM) – combined IRB	11

Army Mission Areas and Domain Portfolio Areas

Department of Defense Directive 8115.01, Oct 2005, established policy and assigned responsibilities for the management of DoD information technology (IT) investments as portfolios that focus on improving DoD capabilities and mission outcomes consistent with Subtitle III of title 40, United States Code (formerly Division E of the Clinger-Cohen Act of 1996).

This guidance directed that portfolios would be nested and integrated at the Enterprise, Mission Area, and Component levels. It designated that the Enterprise portfolio would be divided into Mission Area portfolios, which were defined as Warfighting, Business, DoD portion of Intelligence, and Enterprise Information Environment (EIE) and that Mission Area and Component portfolios may be divided into sub-portfolios (e.g., domains) or capability areas that represent common collections of related, or highly dependent, information capabilities and services.

The Army followed the DoD structure that is organized as follows:

Business Mission Area (BMA) – Domains: Acquisition, Financial Management, Human Capital Management, Installations and Environment, Logistics

Warfighter Mission Area (WMA) – Domains: Focused Logistics, Battlespace Awareness, Force Application, Force Protection, Net-Centric, Force Management, Training, Command & Control

Enterprise Information Environment (EIEMA) – Domains: Computing Infrastructure, Information Assurance, Core Enterprise Services, Networks. EIEMA represents the common, integrated computing and communications environment of the Global Information Grid.

Proposed Changes to the Army IT Review Process

As a result of the designation of the Under Secretary of the Army as the certification authority for Army IT investments and in concert with the definition of the roles and missions of the Office of Business Transformation, there are some recommended improvements to the current Army IT Review Process. The most significant recommendation is to interject an OBT led business case review earlier in the requirements determination step. By doing this, it will ensure the investment is aligned with the business modernization strategy prior to the significant expenditure of time and resources and it will ensure business systems re-engineering is accomplished prior to any IT investment is initiated.

Additionally, we have the opportunity to clarify and sharpen the Army definition of business responsibilities. This would ensure any IT development is linked with the business area strategy. This may suggest some adjustments to the IT funding review process.

Lastly, the Army definition of a business system should conform to the CMO's responsibilities and not the OSD definition of what is a business system. The exclusion of specific systems at the OSD level should not necessarily dictate the Army's portfolio of a business system.