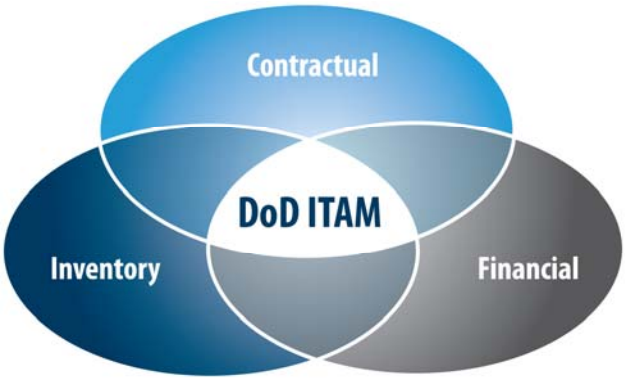
IT Asset Management (ITAM)

The Department of Defense (DoD) Chief Information Officer (CIO) and the CIOs of the DoD Components are establishing an enterprise DoD ITAM framework to optimize acquisition and utilization of commercial off the shelf (COTS) Information Technology (IT) hardware and software assets. ITAM includes policies, processes, tools, and people that manage IT assets:

> ITAM entails collecting inventory, financial and contractual data to manage the IT asset throughout its life cycle. ITAM depends on robust processes, with tools to automate manual processes. Capturing and integrating autodiscovery/inventory, financial and contractual data in a central repository for all IT assets enables the functions to effectively manage vendors and a software and hardware asset portfolio from requisition through retirement, thus monitoring the asset's performance throughout its life cycle.[1]

DoD CIO's objectives include instilling best practices for ITAM across the DoD, providing enterprise-wide visibility into COTS IT assets to improve IT decision-making, and optimizing acquisition and use of IT assets across the Department.



Optimizing Inventory

A 2014 publication by Brainware Group[2] cites industry research that reports initial savings on COTS IT ranging from 15% to 35% from implementing effective software license management solutions and ongoing savings between 5% and 10%. Organizations have realized these savings by improving visibility into asset inventories and purchases and by identifying requirements to align the supply of software and hardware with organizational demand.

Ongoing savings can be achieved by "harvesting" and redeploying underused assets, providing better asset data for more efficient IT support processes, lowering cyber security costs by identifying and removing obsolete products, and aligning assets with enterprise architecture plans. Organizations can also leverage asset visibility for volume purchase discounts and to improve contract negotiations.

ITAM is a best practice that should be implemented in any organization, as evidenced by the inclusion of Service Asset Configuration Management (SACM) process in the IT Infrastructure Library (ITIL) version 3.0, and the establishment of the International Standards Organization (ISO) IT Asset Management standard, ISO 19770.

Regulatory Requirements

The Clinger-Cohen Act of 1996 and the Office of Management and Budget (OMB) circular A-11 require Agency CIOs to maintain IT asset inventories and to optimize IT procurement and utilization. In addition, Executive Order 13103 requires software license management processes that minimize the risk of software piracy.

New legislation has been included in recent National Defense Authorization Acts (NDAAs)[3] that directs the DoD CIO to develop a plan for an enterprise-wide process for reporting commercial software inventories, reporting software license compliance, and ensuring that software inventory reports are supported by an audit trail. The goal is to improve alignment between the licenses owned by DoD and the Department's needs. In addition, the FY15 NDAA includes requirements to expand use of Federal-wide IT strategic sourcing initiatives, which require asset visibility.

Further interest in improving government-wide license management is evidenced by a recent GAO study[4] that recommends that agencies adopt five leading practices to improve software license management.

[1] Gartner IT Glossary: IT Asset Management, Research, www.gartner.com/it-glossary/it-asset-management-itam, Dec. 22, 2014

[2] "ROI analysis of license management projects," Stratenwerth, Wolfgang (brainwaregroup), Mar. 2014

[3] Fiscal Year 2013 (FY13) NDAA Section 937 and FY14 NDAA Section 935

[4] "Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide", U.S. General Accountability Office (GAO), GAO-14-413, May 22, 2014.

Cyber Security

ITAM is foundational to the DoD cyber security Information Security Continuous Monitoring (ISCM) strategy. ISCM relies on IT asset data and other information systems monitoring data to defend DoD networks, IT assets, and information from vulnerabilities and threats.

DoD's ISCM approach aligns with the NIST Continuous Monitoring framework[5], which includes asset management and software license management as two of the eleven security automation domains that support continuous monitoring: "The Asset Management data domain is important and complex and acts as the foundation for the other domains within security and IT management."[6]

ISCM will provide visibility into the IT asset inventory, and over time, will ensure that appropriate controls exist for effective software license management.

Enterprise Asset Visibility

DoD CIO is planning an enterprise-level COTS software asset reporting solution that will leverage data collected across the software asset lifecycle to improve decision making.

Ready access to enterprise-wide IT asset data – coupled with enterprise-wide ITAM data standards –will improve IT resource management by enabling CIOs across the Department to optimize acquisition, utilization, and support of COTS software.

DoD ITAM Community

DoD enterprise ITAM efforts are coordinated through the DoD ITAM Integrated Product Team (IPT), which includes representatives from the military services and other Defense Agencies. Recent efforts have targeted FY13 and FY14 NDAA requirements for COTS software license inventory reporting.

DoD ITAM representatives are active in related DoD, Federal and industry working groups: DoD cyber security; DoD Financial Improvement and Audit Readiness (FIAR); Defense Enterprise Service Management Framework (DESMF); Federal IT strategic sourcing and ITAM activities; and, industry working groups for ITAM standards.

The DoD ITAM IPT serves as the primary forum for communicating department-wide ITAM objectives and strategies, and for collaborating to adopt common ITAM approaches and data standards across DoD. Representatives from all DoD Components are welcome to join

Resources

DoD	DoD Enterprise Software Initiative (ESI)	www.esi.mil
	DoD Host Based Security System (HBSS)	www.disa.mil/services/cybersecurity/hbss
INDUSTRY	International Association of ITAM	www.iaitam.org
	ISO/IEC 19770 IT Asset Management	www.iso19770.com
	International Software Business Management Assoc. (IBSMA)	www.ibsma.com
	Information Technology Infrastructure Library (ITIL)	www.itil-officialsite.com
	Business Software Alliance (BSA)	www.bsa.org
	NIST Common Platform Enumeration (CPE)	nvd.nist.gov/cpe.cfm
	NIST SP 800-173: Information Systems Continuous Monitoring for Federal Information Systems and Organizations	csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
	NIST IR 7800: Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains (DRAFT) (Jan. 2012)	csrc.nist.gov/publications/drafts/nistir-7800/Draft-NISTIR-7800.pdf

DoD Point of Contact

Mr. Bob Smith, DoD CIO ITAM Program Manager	robert.j.smith84.civ@mail.mil

[5] Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST Special Publication 800-137, Sept. 2011.

[6] NIST Interagency Report 7800 (Draft), Jan. 2012, p. 7