Information Technology Asset Management (ITAM)

Software License Management (SLM)
Introduction

15 February 2017

Webinar Information

Audio dial-in number: 1-866-783-7350
Participant code: 6928919#

URL: https://conference.apps.mil/webconf/esiwebinar

- Teleconference audio will be muted for all participants
- Please submit any questions or comments via the webinar chat
- Questions will be addressed at the end, time permitting

DoD ESI Team Introductions

Floyd Groce | *DON CIO IT Strategic Sourcing Lead, DoD ESI Co-Chair*

Leads the DON CIO Enterprise Licensing and strategic sourcing efforts for IT hardware, software and services. One of the DoD points of contact for OMB Federal Strategic Sourcing Initiative (FSSI) SmartBUY software licensing initiative. Previously, held an unlimited contracting officer warrant for IT contracting.

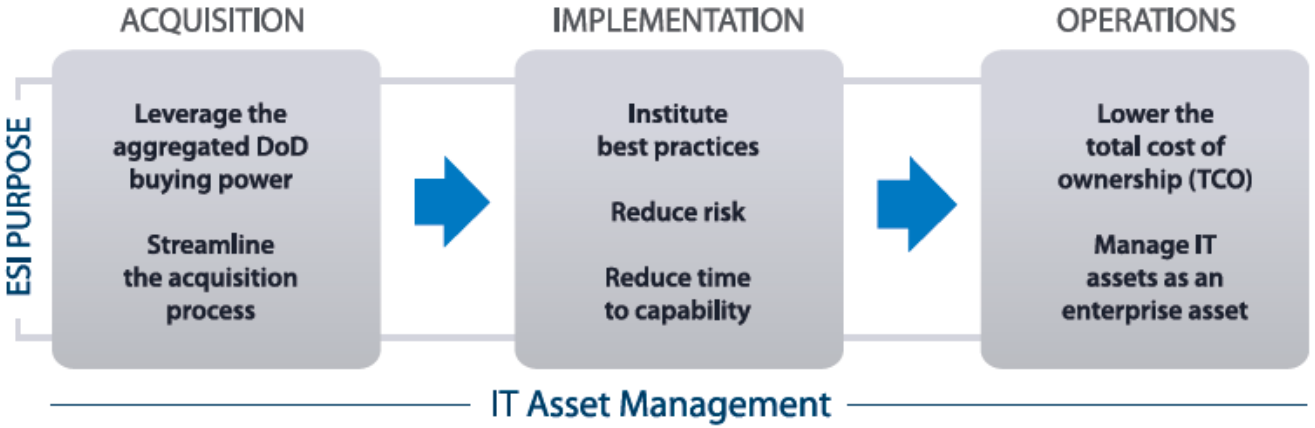
Jim Cecil | *IT Management Consultant, DoD CIO*

Enterprise IT asset management, portfolio management, strategic sourcing, and program management consultant with over 20 years of experience in managing and implementing commercial and custom information technology. Supports DoD CIO in IT Asset Management and Enterprise Software Licensing and Procurement.

PMP, CISM, CISSP, CSEP, CSDP, LSSGB, ITIL-F
DAWIA PM & Purchasing Level II Training

DoD ESI

- DoD ESI is a joint DoD category management and strategic sourcing initiative to save time and money on acquisition of commercial software, IT hardware and services
- Executive Sponsor: DoD CIO
- Goals:
  - *Leverage enterprise scale and efficiencies in COTS IT acquisition*
  - *Coordinate IT asset management across the enterprise*



Webinar Objectives

- Present the high-level need for Software License Management (SLM) capabilities
- Introduce the linkage between Information Technology Asset Management (ITAM) and SLM
- Outline the major elements of an SLM capability
- Review drivers for implementing SLM in Federal agencies and DoD

Agenda

- The need for Software License Management (SLM)
- SLM Challenges
- Information Technology Asset Management (ITAM) Overview
- Software License Management Overview
- SLM Solutions
- Federal/DoD Guidance & Way Ahead
- Resources

The need for Software License Management (SLM)

What is a "software license"*?

A **legal instrument** (usually by way of contract law, with or without printed material) governing the use or redistribution of software. Under United States copyright law all software is copyright protected, in source code as also object code form.[2] The only exception is software in the public domain. A typical software license **grants the licensee**, typically an end-user, **permission to use** one or more copies of **software** in ways where such a use would otherwise potentially constitute copyright infringement of the software owner's exclusive rights under copyright law.

… **ownership** of those copies **remains with the software publisher**…the **end-user must accept the software license**. In other words, without acceptance of the license, the end-user may not use the software at all.

…Software licensing often also includes **maintenance**…The maintenance agreement (contract) contains minor updates (V.1.1 => 1.2), sometimes major updates (V.1.2 => 2.0) and is called e.g. **update insurance**, **upgrade assurance**.

(Wikipedia.org, July 21, 2016)

Software licenses include commercial, custom software, "open source" and other public domain software. Our discussion focuses on **commercial software licenses.*

Common Stakeholders and their needs

Common CIOs questions about software licenses…

- How much do we **spend** on commercial software?
  - *Are we using our existing licenses (**inventory utilization**)?*
  - *Are we paying for software maintenance on **retired licenses**?*
  - *Could we lower costs with **different licensing models**?*
  - *Could lower operating costs by **streamlining** software purchasing?*
- Are we in **compliance** with software license agreements?
  - *Are we using more software than our we own (**over-deployed**)?*
- Could we **substitute** products to lower our costs or improve our capabilities?
  - *How much could we save by **migrating to the cloud or mobile** solutions?*
  - *Who are our **biggest vendors**? Do we manage these relationships well?*
- Are we using **obsolete or insecure** software products?
  - *Are we using **upgrade rights** that we pay for in maintenance agreements?*
  - *Is **unauthorized software** running in our environment?*

System managers software inventory needs…

- Do we have enough software licenses to **satisfy requirements**?
- Are our **existing licenses installed**?
- Is installed software **being used**?
- Is there any **unauthorized software** on corporate computers?
- Can we prove that we are in **compliance** with all software licenses (number of installs, authorized users/usage, correct versions/editions, device/processor class, etc.)?
- Do we have vendor **maintenance support** for software products?
- Are we using **obsolete or insecure** software products?
- How many systems **require patches or upgrades**? Have patches and upgrades been installed?

SLM Challenges

Product Complexity in Licensed Software

Complex Products

- Unique rights for each product / license
- Bundled third-party licenses
- Software embedded in hardware devices
- Tracking upgrades received through maintenance or software assurance
- Identifying and reconciling software products (purchased vs. installed)
- Client Access Licenses (CAL)

Intangible Assets

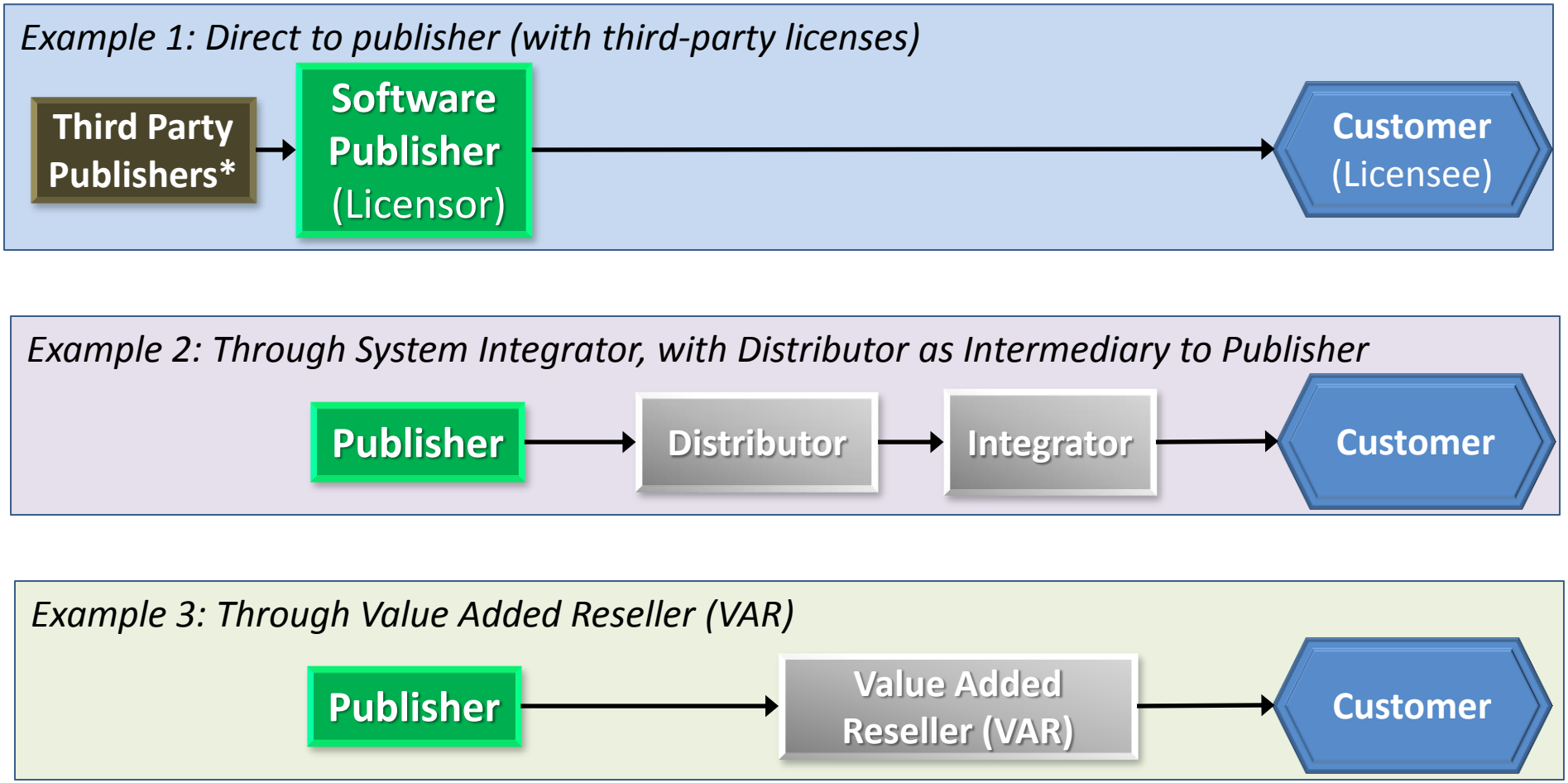
- Cannot see it
- Requires legal compliance
- Users rarely see or read license agreements
- Can be distributed electronically
- Can be virtualized – only existing at run-time
- Authorized usage is defined in a license document – not necessarily within the software program

Evolving Business Models

- Subscription Licensing – How do we pay?
- Enterprise Licenses – How do we count?
- Open Source Software – Who owns the code?
- Cloud computing – Who is operating the software?

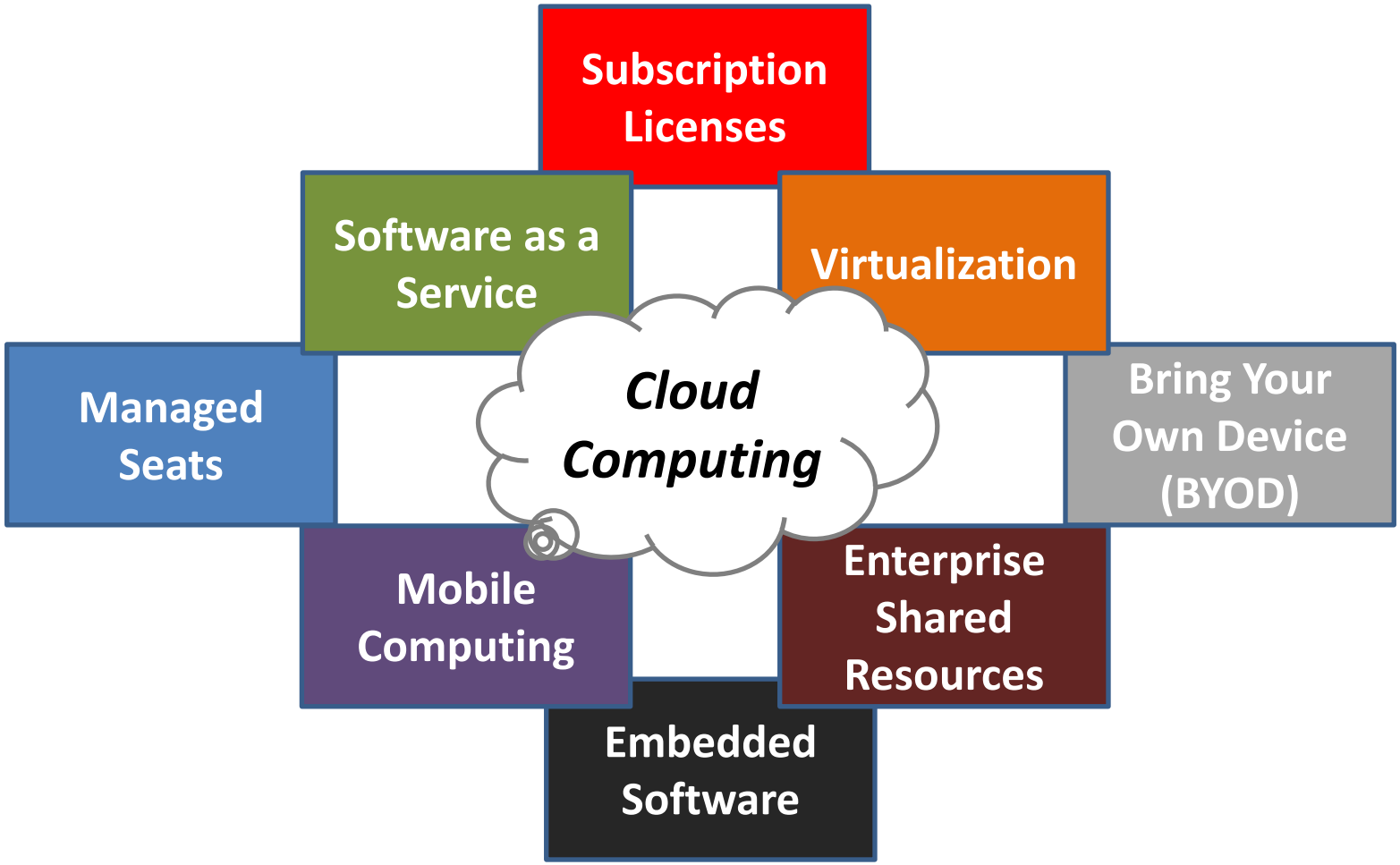
Software Distribution Channels Create Complex Relationships

Often no "privity of contract" with licensor



** e.g. "run-time" licenses, restricted use licenses, third party software developers, open source software*

New Technology and Business Models Present Licensing Challenges



Dynamic Software Industry

Technology Advances & Substitutions

Bundling Products & Features

Agile Development: Rapid Product Releases

Start-ups

Cybersecurity

Industry Standards

Corporate Mergers & Acquisitions

Hardware Advances

High-Level Requirements

WHAT TYPES OF ASSETS DO WE HAVE?

HOW MANY OF EACH ASSET DO WE HAVE?

HOW & WHEN DID WE RECEIVE THEM?

WHERE ARE THEY NOW?

- *Are being used or sitting on a shelf?*
- *Have changes been recorded?*

WHO IS USING EACH ASSET?

Authorized users only?

HOW ARE THEY USED?

- *Is a device a server or a laptop?*
- *Is software used IAW license?*

ARE THE ASSETS BEING MAINTAINED?

ARE THE CONFIGURATIONS SECURE?

WHAT ARE OUR TOTAL COSTS OF OWNERSHIP?

IT Asset Visibility

IT Asset Management (ITAM) Overview

IT Asset Management (ITAM)

ITAM Definition

IT Asset Management is a **systematic process that joins contractual, financial, inventory, and IT governance functions** to support life-cycle management and strategic decision-making to reduce risk and optimize the value of IT assets (hardware, software).

IT Asset Life-Cycle View

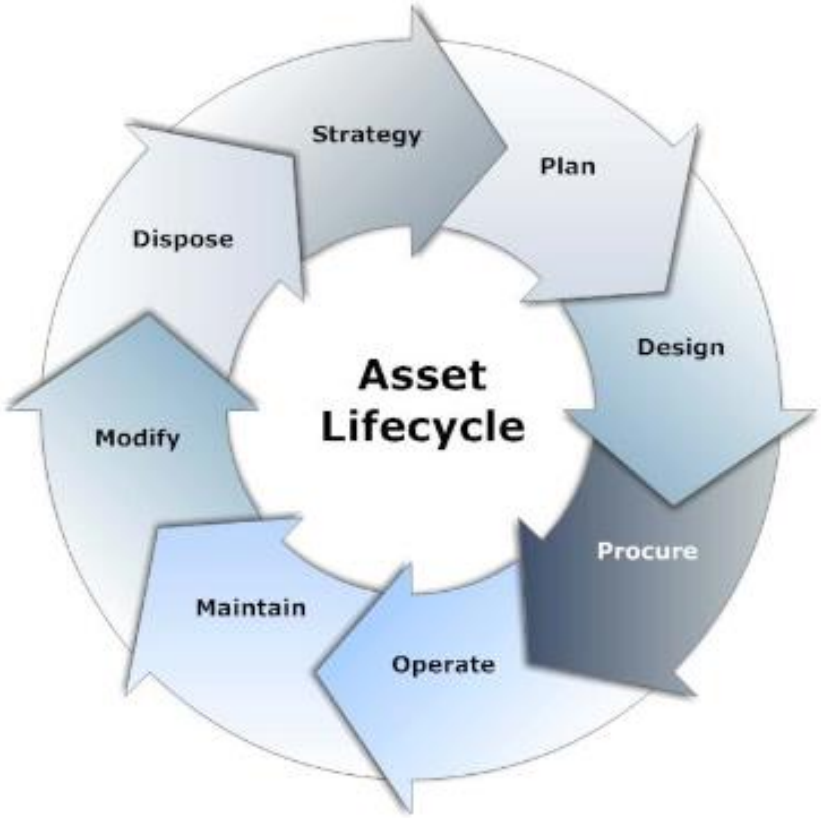


Figure 5.3 Typical Asset Lifecycle[1]

ITAM Benefits

Inventory Control

Know what you have & where it is

- Best business practice
- Basic fiduciary duty
- Enables self audit & compliance

Security

Ensure Security & Integrity

- Identify vulnerabilities
- Prevent unauthorized use
- Ensure patches & updates are deployed

Cost Control

Avoid unnecessary purchases

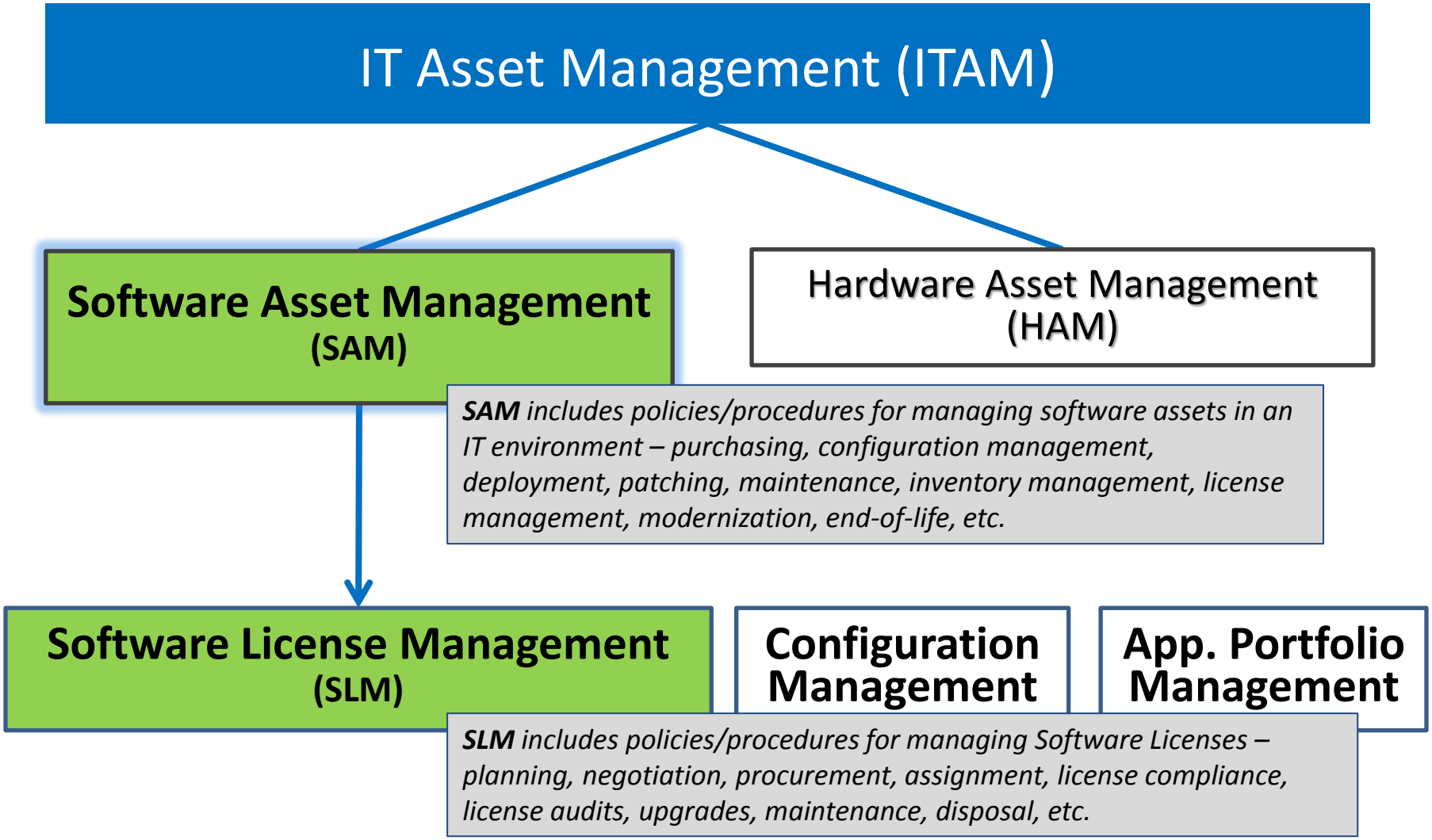
- Entitlement Management
- Strategic Vendor Management

Customer Service

Improve Experience

- Better Service Desk Response
- Better Efficiency
- Faster Response Time

ITAM: Software License Management



Software License Management (SLM) Overview

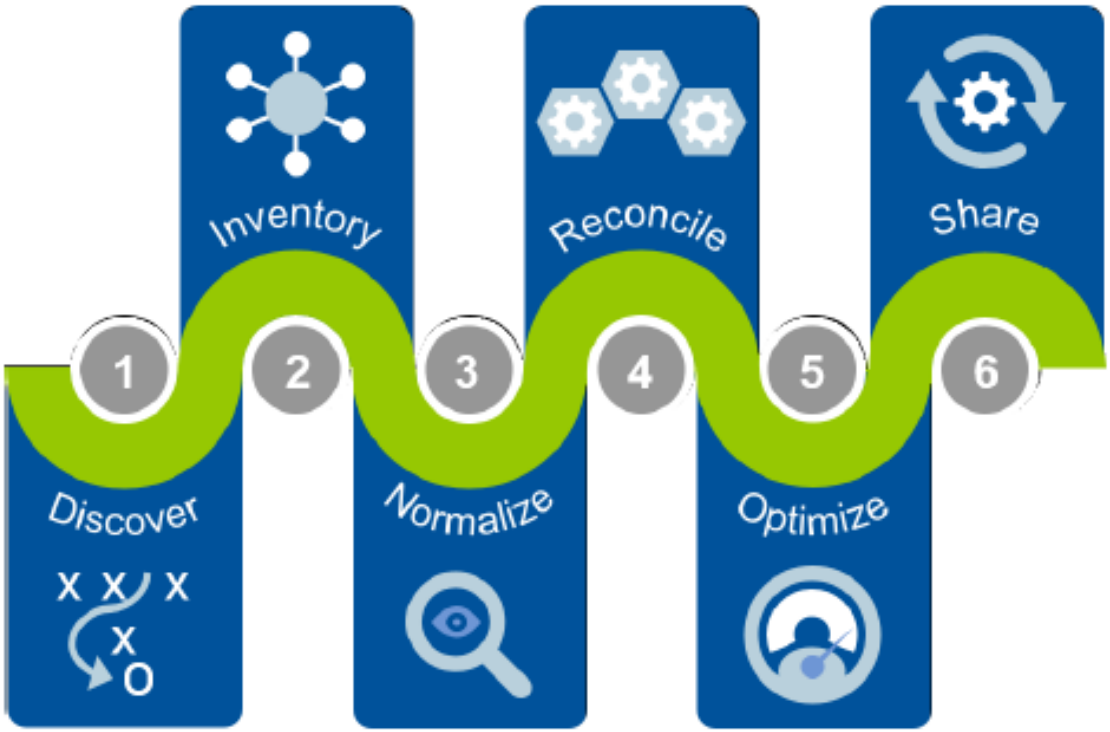
Software License Management (SLM)

A mechanism for **systematically ensuring compliance** with system vendor and independent software vendor (ISV) software licenses — for example, maximum users, maximum nodes and maximum MIPS.

(Gartner IT Glossary, May 7, 2015)

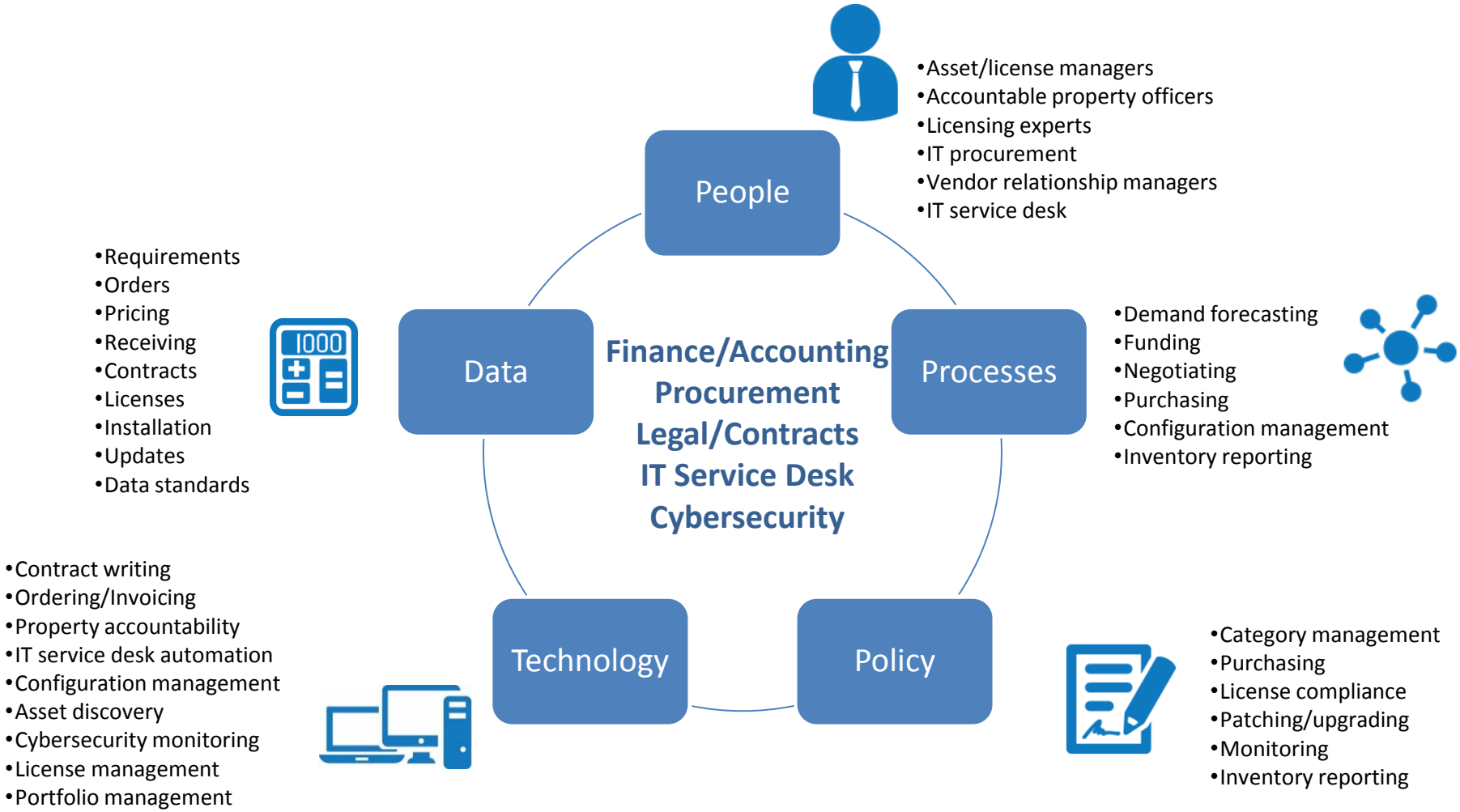
SAM Framework
(Gartner Research)

Figure 1. Gartner's Tool Decision Framework for SAM



Source: Gartner (July 2015)

SLM Solution Elements



Sample SLM Roles

ITAM Director

Establish and Implement ITAM Policies & Procedures

SAM Manager

Manage SAM Processes

SLM Manager

Manage SLM Processes

Procurement & Contract Management

Record and enforce license terms including quantity and use rights

IT Inventory

Record and track all inventory records from receipt through retirement

Financial Management

Record & track all dollar values

Change Management

Implement and execute change management

License Data: *Entitlements*

Contract and License Terms and Conditions

Data categories

- Product information
  - product name, publisher product number (if available), quantity ordered
- Use Rights
  - Entitlements
  - Authorized uses
- Authorized users
- SLAs
  - Service Level Requirements & Performance
  - Penalties & Fees
- Warranty
- Derivative works ownership
- Maintenance and Support

License Types:

- Perpetual
- Term/subscription
- Third party licenses
- Open Source
- Cloud computing/SaaS
- Test/development
- Educational
- Enterprise licensing

Common SLM Life-Cycle Reporting Data

Source/Activity:	Agreement/ Contract	Receiving	Deployment	Changes/ Modifications
Description	License agreement data and a completed, signed copy of the agreement (License Grant).	Compare License receipt with license agreement. Document and resolve discrepancies.	Device and location where software is deployed and used.	Details regarding software updates, patches, fixes, disposal, etc.
Data	• Product • Part Number • Version • Publisher/OEM • Vendor • Agreement date • Quantity • Price • Entitlements	• Order/Agreement number • Date of receipt • Part number • Quantity • etc.	• Date • Quantity • Device • Location • User • Organization	• Date (due & actual) • Quantity • Device • Location of software changes

SLM Solutions

SLM Solution Conceptual Design

Software License Management, Optimization & Reporting

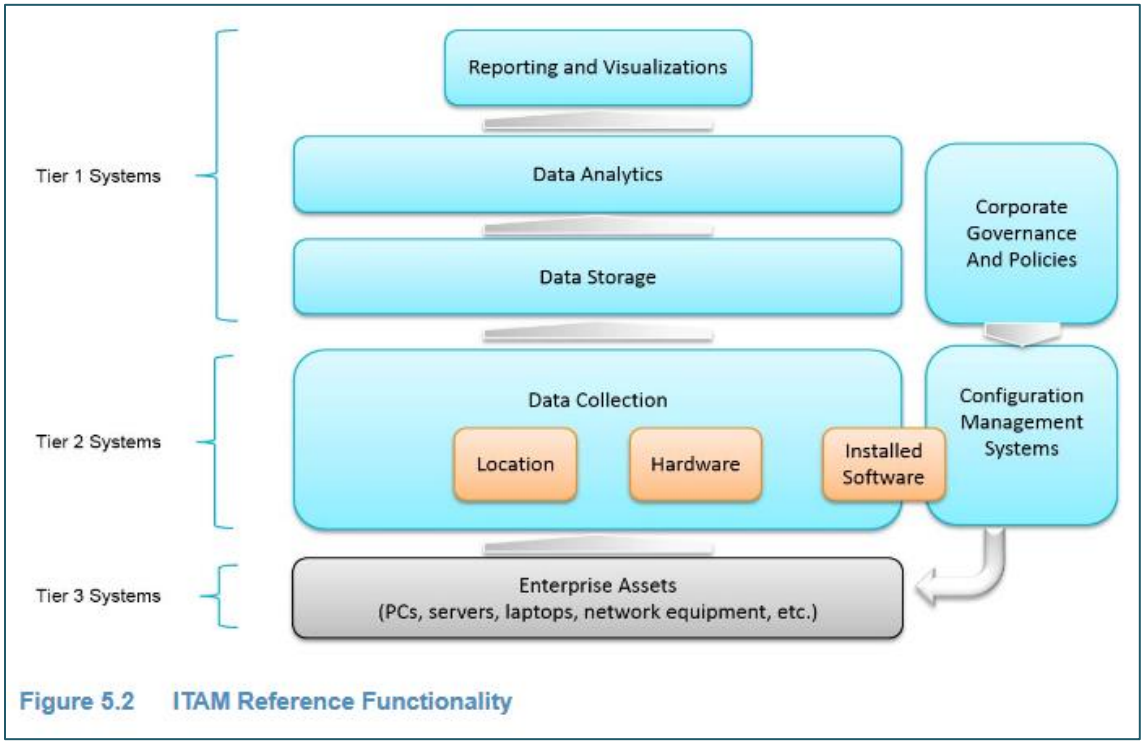


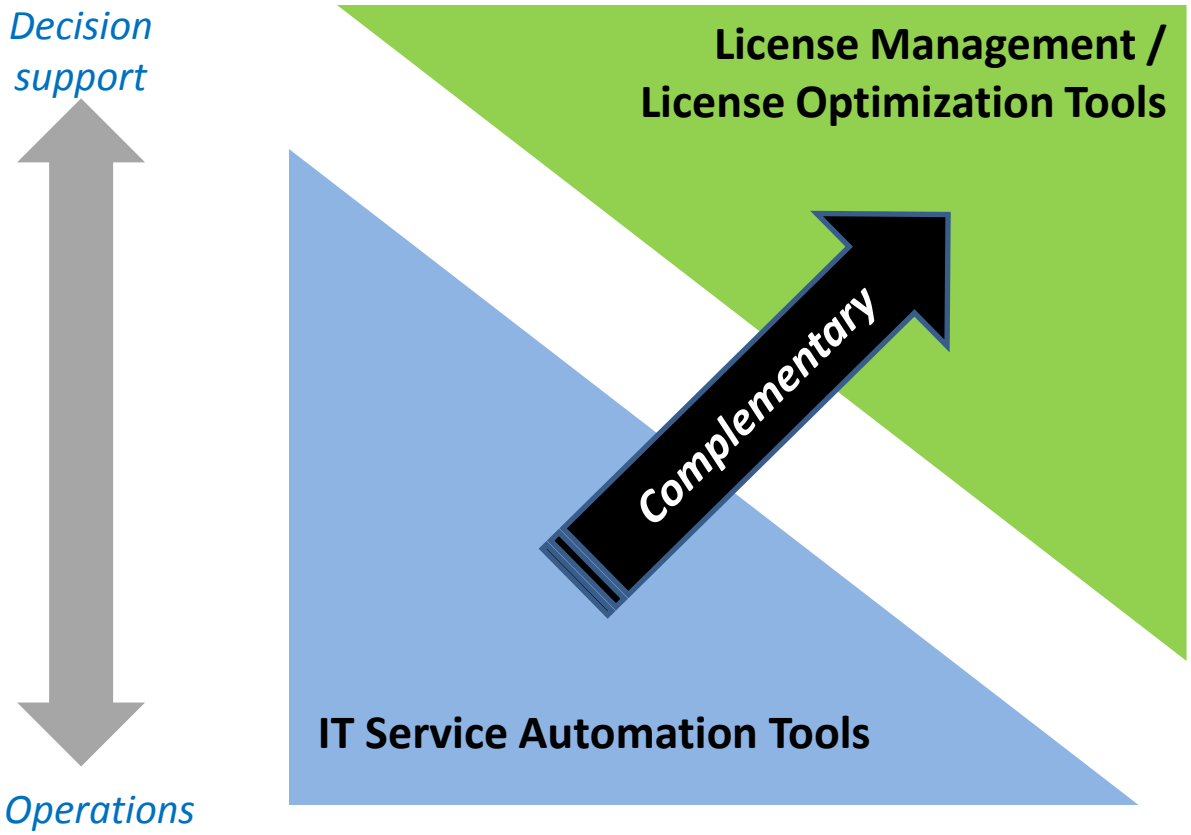
Figure 5.2 ITAM Reference Functionality

Acquisition Systems

Finance & Accounting Systems

ADAPTED FROM NIST SPECIAL PUBLICATION 1800-5b, NIST CYBERSECURITY PRACTICE GUIDE FINANCIAL SERVICES IT ASSET MANAGEMENT Approach, Architecture, and Security Characteristics For CIOs, CISOs, and Security Managers, Draft, Oct. 3015

Commercial ITAM / SLM Tool Landscape



License optimization

Compliance/audit reporting

Software deployment / harvesting

Service desk automation

Vulnerability management

Patching

Asset discovery

Configuration management

Network operations

SAM / SLM Linkage with Cyber Security

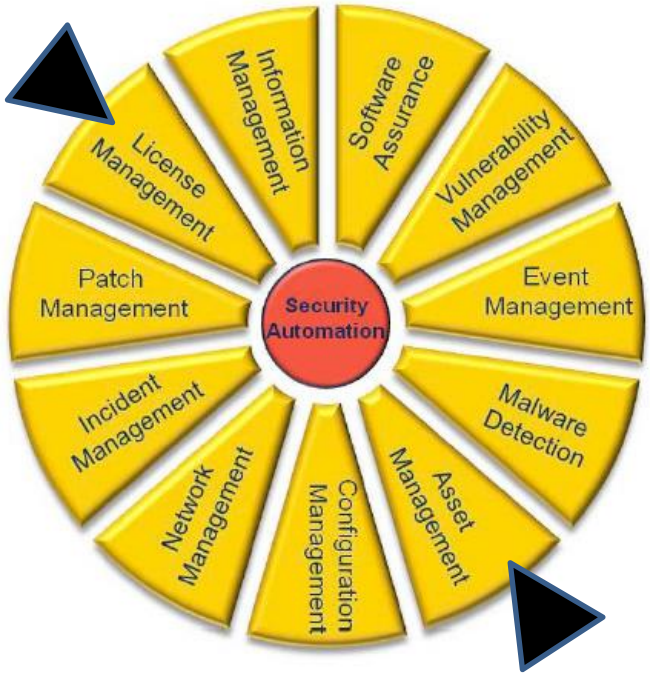


Figure D-1. Security Automation Domains

D.1.4 ASSET MANAGEMENT

Asset management tools help maintain inventory of software and hardware within the organization. This can be accomplished via a combination of system configuration, network management, and license management tools, or with a special-purpose tool. Asset management software tracks the life cycle of an organization's assets and provides tools such as remote management of assets and various automated management functions.

The implementation and effective use of asset management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-8, Information System Component Inventory; and SA-10, Developer Configuration Management.

D.1.7 LICENSE MANAGEMENT

Similar to systems and network devices, software and applications are also a relevant data source for ISCM. Software asset and licensing information may be centrally managed by a software asset management tool to track license compliance, monitor usage status, and manage the software asset life cycle. License management tools offer a variety of features to automate inventory, utilization monitoring and restrictions, deployment, and patches for software and applications.

The implementation and effective use of license management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including CA-7, Continuous Monitoring; CM-8, Information System Component Inventory; and SA-6, Software Usage Restrictions.

Example Tools Used in SLM


Identity Management


CMDB / Common Software Library


Asset Discovery


Problem Reporting


Contract Management


Problem Management


Inventory Management


Change Management


License Management

Software Identification: Standards

ISO/IEC 19770

- 19770-1
  - *SAM Process*
- 19770-2
  - *Software Identification (SWID) Tags*
- 19770-3
  - *Software Entitlement Tags*
- 19770-5
  - *SAM Overview/Vocabulary*
- Certified (signed) tags
- Industry standard

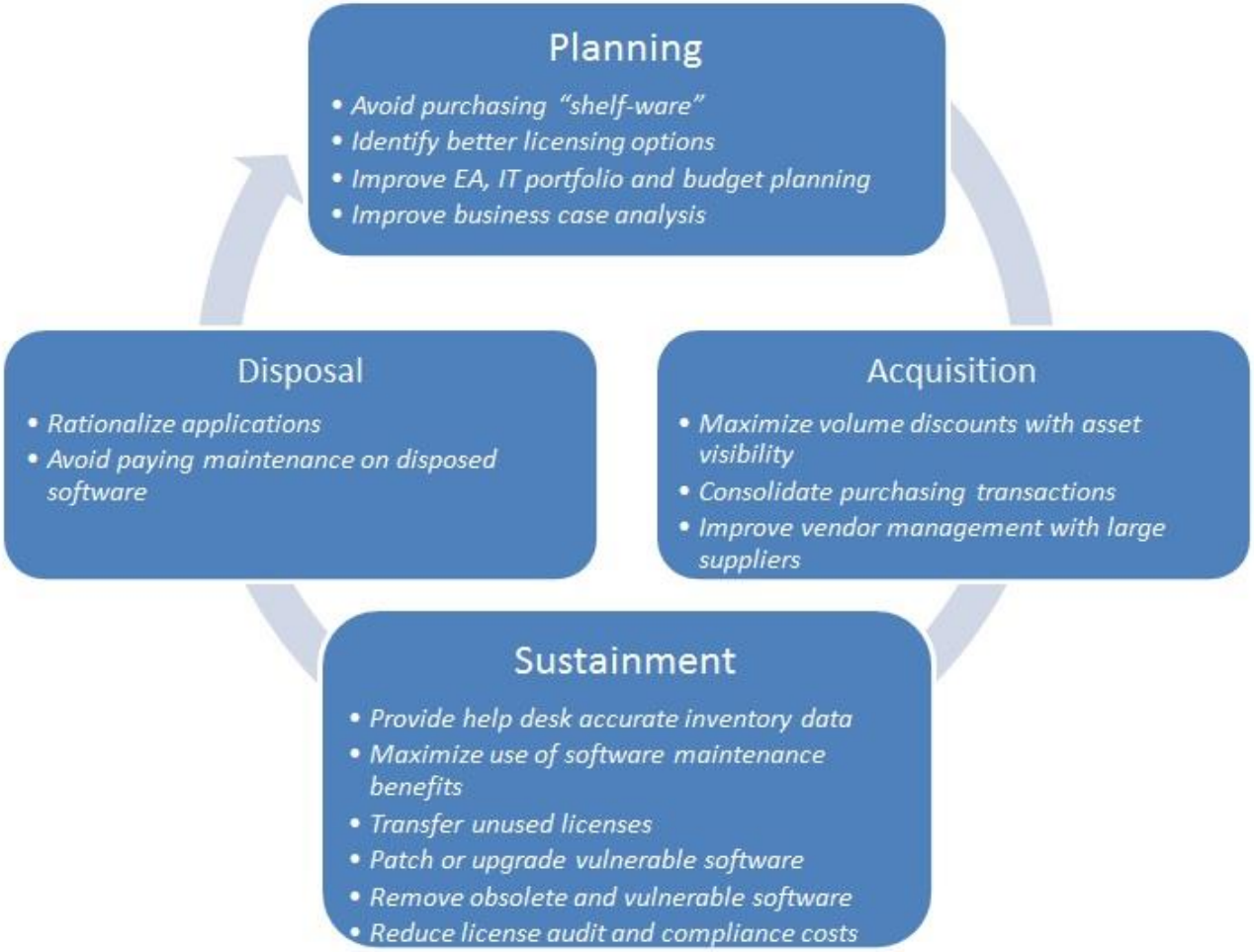
NIST Common Platform Enumerator (CPE)

- Security Content Automation
- Asset naming schema
- Government-driven

Distributed Management Task Force (DMTF)

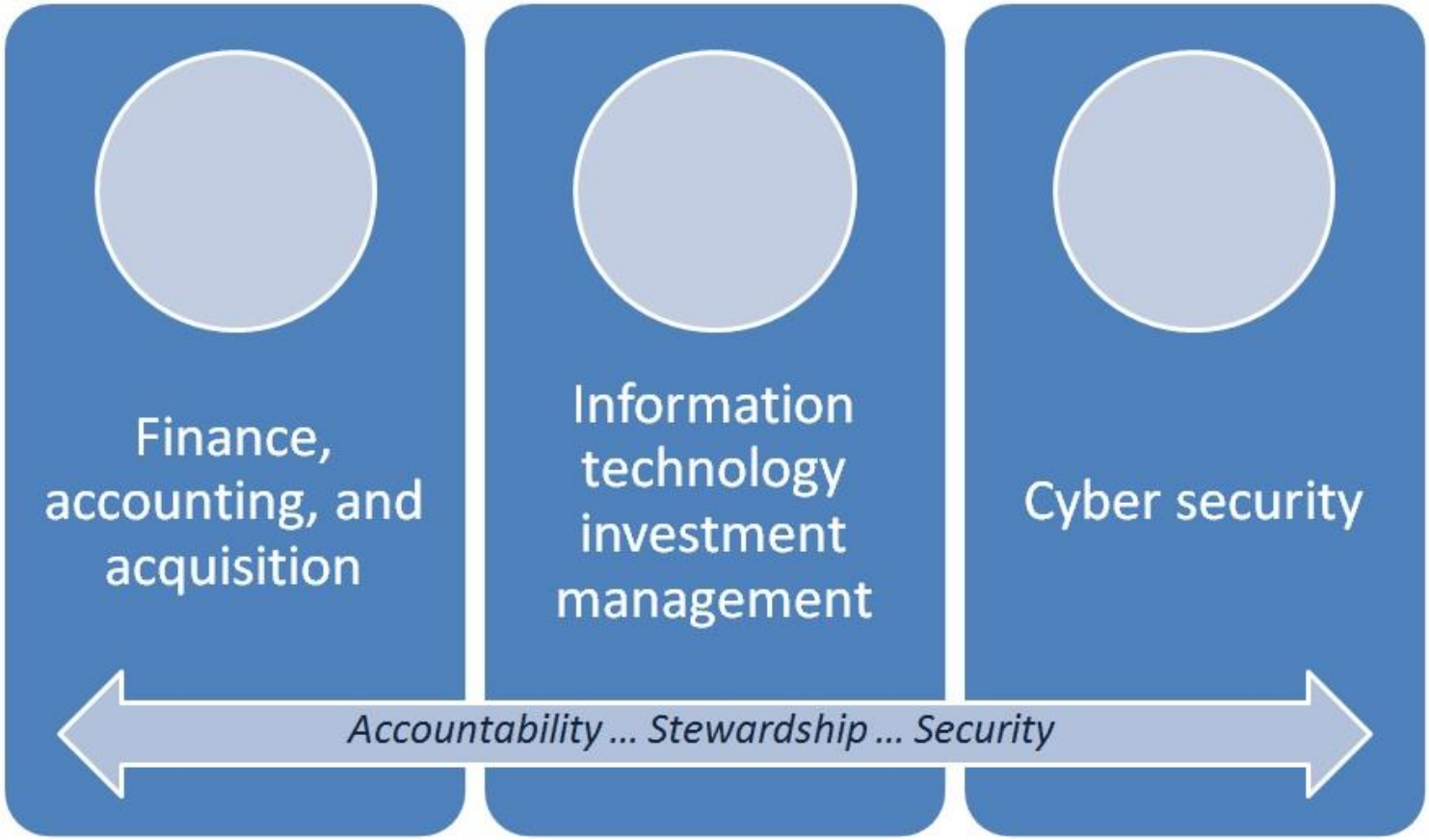
- Infrastructure management data standards
- Vendor-driven

Benefits across the Software Lifecycle



Federal & DoD Guidance

SLM in Policy



Federal SLM Government Policy & Guidance: Foundation

	Federal Policy & Guidance Reference	Description
1.	**Clinger-Cohen Act (1996) / USC Title 40 CIO Act / USC Title 10 DoD CIO**	Designed to improve the way the federal government acquires, uses and disposes IT. Title 10 defines additional responsibilities for DoD & MILDEP CIOs.
2.	**Executive Order 13103 – Computer Software Piracy (December 1998)**	Prevent and combat computer software piracy by U.S. Government Agencies. Establish procedures to ensure that the agency has present on its computers and uses only computer software not in violation of applicable copyright laws, including: (1) installed software inventories of the software on its computers; (2) authorization software inventories; and (3) adequate recordkeeping systems.
3.	**Executive Order 13589 – Promoting Efficient Spending (November 2011)**	Sec. 4. IT Devices. Assess current device inventories and usage…ensure that they are not paying for unused or underutilized IT equipment, installed software, or services…consider agency-wide IT solutions for desktop services, email, and collaboration tools.
4.	**NIST Information Security Continuous Monitoring (SP 800-137)**	SP 800-137: (Asset Management) Maintain inventory of software and hardware within the organization. (License Management) Track license compliance, monitor usage status, and manage the software asset life cycle.

Federal SLM Policy & Guidance: Current Priorities

	Federal Policy & Guidance Reference	Description
5.	**GAO-14-413 Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide**	May 2014 report that recommends adoption of leading practices for software license management across the Federal government
6.	**Federal IT Acquisition Reform Act (FITARA) / FY15 NDAA**	Includes provisions that require the federal government to: inventory all IT and develop a federal strategic sourcing initiative for the use of government-wide software user license agreements. FITARA was included NDAA FY15.
7.	**OMB Category Management Policy 16-1: Improving the Acquisition and Management of Common IT: Software Licensing (June 2016)**	Implements FITARA provisions for commercial software licenses. Requires agency CIOs to establish comprehensive software license management policy to: compile agency-wide license inventory; analyze inventory data to ensure compliance, consolidate redundant applications, and identify cost-savings opportunities; increase use of government-wide "best in class" purchasing agreement to reduce duplicative contract vehicles; ensure appropriate personnel have received adequate training in SLM; and, collect and report metrics on cost savings.
8.	**NEW! MEGABYTE Act (Making Electronic Government Accountable By Yielding Tangible Efficiencies, Public Law 114-210, July 2016)**	Requires OMB to issue a directive on the management of software licenses, requiring executive agency CIOs to develop comprehensive SLM policy that requires: establish a comprehensive license inventory using automated discovery and inventory tools; regularly track and maintain software licenses; analyze software usage to make cost-effective decisions; provide SLM training; establish SLM goals and objectives; and, consider the software license management life cycle phasesto implement effective decision making and incorporate existing standards, processes, and metrics.

New! MEGABYTE ACT & OMB Category Management Policy 16-1 for Software Licenses: Agency Software Manager

- Agency CIOs must coordinate with Acquisition and Comptroller to improve software license management policies and procedures:
  - *Aggregate software license requirements*
  - *Establish funding mechanisms for pooling software license requirements for bulk purchases*
  - *Establish controls/enforcement mechanisms for using designated purchasing vehicles*
- Agency CIOs must designate a “Software Manager” to:
  - *Implement commercial software license policy to optimize acquisition and asset utilization*
  - *Implement a centralized software license management strategy*
  - *Increase use of government-wide and agency-wide best-in-class purchasing vehicles*
  - *Maintain agency-wide software license inventory*
  - *Implement controls for compliance with OMB & agency licensing policy*
  - *Ensure staff are qualified and/or trained in license management*
  - *Implement a vendor management strategy*
  - *Report cost savings metrics for improvements in software license management*
- The Federal Enterprise Software Category Management Team (ESCT) will provide criteria for “best in class” software purchasing vehicles and designate selected contracts for government-wide use

Recent DoD Policy & Guidance

	Policy Reference	Description
1.	**FY14 NDAA Section 935 & FY13 NDAA Section 937**	DoD Software License Inventory Reporting Plan and DoD Selected Software License Inventory data call
2.	**Information Security Continuous Monitoring: JTF-GNO CTO 07-12 Deployment of Host Based Security System (HBSS), etc.**	Cyber Security Analytic Cloud (CSAC), Continuous Monitoring and Risk Scoring (CMRS), Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), etc.
3.	**DON Software Acquisition Training Requirements**	DASN AP memorandum requiring specialized software licensing training for all applicable DON contracting personnel. Related: DON IG: The Navy's Management of Software Licenses Needs Improvement (August 7, 2013)
4.	**DoD ESI / DFARS 208.74**	Enterprise software agreements
5.	**Financial Improvement and Audit Readiness (FIAR)**	• "Strategy for Internal Use Software," USD(C), September 30, 2015. Establishes accountability requirements for Internal Use Software (IUS), including commercial software licenses. • DODI 5000.xa (draft) Pending USD(AT&L) policy for Management and Accounting of IUS.

NEW! FY17 NDAA Sec. 1653

Plan for information security continuous monitoring capability and comply-to-connect policy; limitation on software licensing.

(a)(1) **PLAN AND POLICY** — DoD CIO and USCYBERCMD shall jointly develop:

a plan for a modernized, Department wide **automated information security continuous monitoring** capability

a comply-to-connect policy that requires systems to automatically comply with the configurations [standards/requirements]

6) **SOFTWARE LICENSE COMPLIANCE** MATTERS:

The plan and policy required by paragraph (1) shall comply with the software license inventory requirements of the plan issued pursuant to [FY13 NDAA Sec. 937 and FY14 NDAA Sec. 935]

(b) **LIMITATION ON FUTURE SOFTWARE LICENSING.**

(1) …***none of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2017 or any fiscal year thereafter for the Department of Defense may be obligated or expended on a contract for a software license with a cost of more than $5,000,000 in a fiscal year unless the Department is able, through automated means—***

(A) to **count the number of such licenses in use**; and

(B) to determine the security status of each instance of use of the software licensed.

(2) EFFECTIVE DATE.—Paragraph (1) shall apply—

(A) beginning on January 1, 2018, with respect to any contract entered into by the Secretary of Defense on or after such date for the licensing of software; and

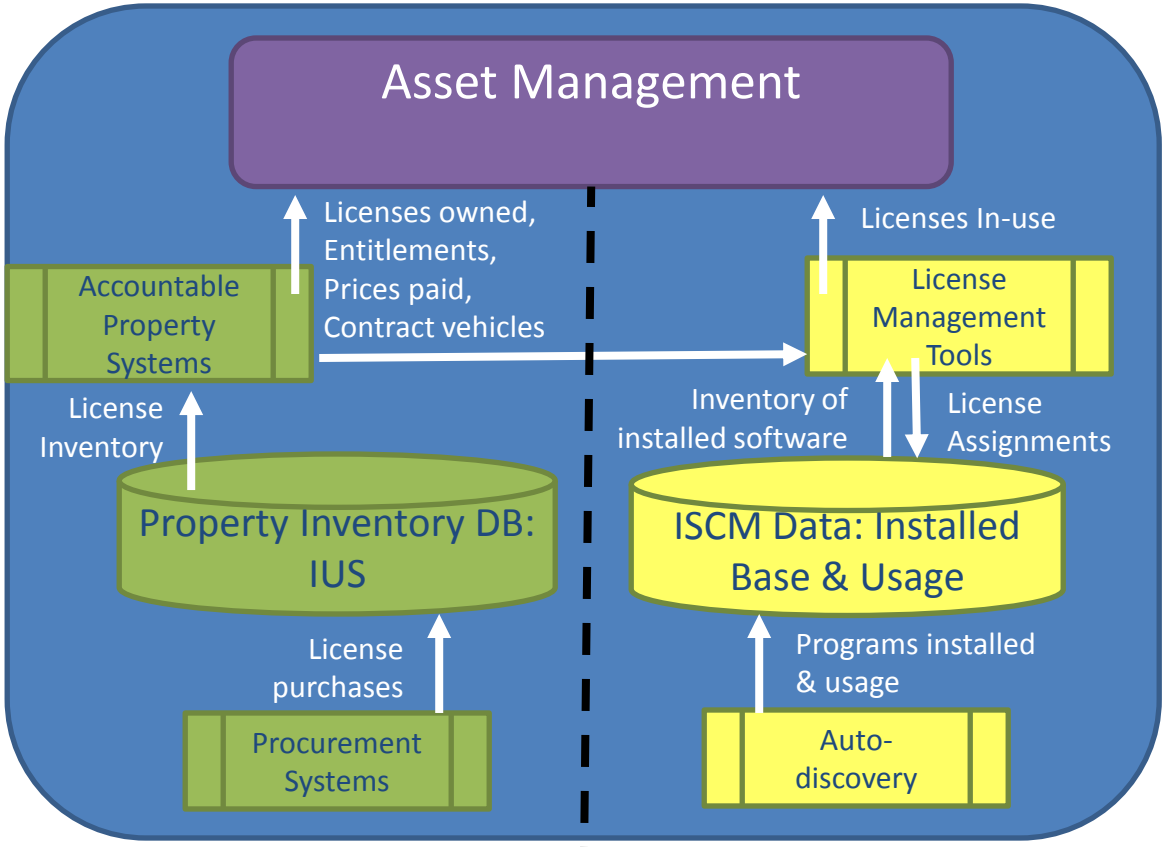
(B) beginning on January 1, 2020, with respect to any contract entered into by the Secretary for the licensing of software that was in effect on December 31, 2017.

DoD Way Ahead

DoD Software License Inventory Reporting Plan

- **Requirement:** FY14 NDAA Section 935 required DoD CIO to provide a software license inventory reporting plan that uses automation to regularly report the inventory of commercial software licenses for which any MILDEP spends at least $5M annually. The solution must support optimizing the acquisition and use of software licenses.
- **Approach:** Implement basic license inventory summary reporting using data from acquisition systems and continuous monitoring
- **Implementation Strategy:** *Use ongoing investments as foundation for FY14 NDAA Sec. 935 requirements*
  - ***Financial data & audit trail:*** *Leverage Financial Improvement and Audit Readiness (**FIAR**) Internal Use Software (IUS) policy, guidance, business systems, and reporting processes*
  - ***License inventory status:*** *Leverage Cybersecurity Information Security Continuous Monitoring (**ISCM**) data, processes, and reporting*
    - *ISCM Domains: Asset Management, Configuration Management, License Management*
  - ***Analysis & Reporting:*** *Implement reports and dashboards in ISCM reporting environment*
  - ***License Optimization:*** *Leverage the **DoD Enterprise Software Initiative (DoD ESI)** & for IT enterprise category management, including enterprise licenses and enterprise purchasing vehicles*

DoD Software License Inventory Plan Overview



Resources

Resources

SLM Methodology and Best Practices	Software Management Standards	IT Management Frameworks
Int'al Assn of IT Asset Managers (**IAITAM**) *ITAM Professional Association*	**ISO/IEC 19770** *IT Asset Management*	IT Infr. Libr. Service Asset Config. Mgmt (**ITIL SACM**) *Maintains asset information across the entire life cycle*
Business Software Alliance (**BSA**) *Pioneers compliance programs for legal software use*	***TagVault.org*** *Neutral not-for-profit certification authority for software tagging*	Control Objectives for Information & Related Technology (**COBIT**)
Int'l Business Software Management Assn (**IBSMA**) *Nonprofit assn of bsns-focused software mgmt (SAM) professionals*	**NIST Common Platform Enumerator (CPE)** *Structured naming scheme for information technology systems, software, and packages*	**NIST SP 800-137** **NIST SP 800-53** *Continuous Monitoring & Security Controls*
GSA IT Acquisition Gateway *Software Corridor* (hallways.cap.gsa.gov/ITSoftware)	Distributed Management Task Force (**DMTF**) *Industry standards org. to simplify manageability of network-accessible technologies*	**ISO/IEC 20000** *IT Service Management*

Example DoD Component ITAM/SAM Policy

- Air Force Manual 33-153: IT Asset Management *(March 19, 2014; rev. Aug. 28, 2014)*
  - *ITAM roles and responsibilities*
  - *Hardware asset management inventory and reporting requirements*
  - *Software asset management procurement, anti-piracy, and change management*
- Marine Corps MARADMIN 623/10: IT Asset Management Program
  - *IT hardware accountable property guidance*
- Navy: Mandatory Use of Enterprise License Agreements (ASN(RD&A), Feb. 22, 2012)

Questions?

Please submit your questions via webinar chat or use "Ask an Expert" function on www.ESI.mil.

Briefing slides are posted to www.ESI.mil for download.

Visit

www.ESI.mil

For additional IT acquisition resources and training information