IT Asset Management Policy

Version 1.0

December 2016

U.S. Nuclear Regulatory Commission

Office of the Chief Information Officer

Revision History

DATE	VERSION	SUMMARY OF CHANGES	AUTHOR
12/14/2016	1.0	The NRC developed a policy on its IT asset management based on Federal mandates (e.g., FITARA and MEGABYTE Act); OMB Category Management Policy and other OMB guidance; and GAO recommendations. ADAMS Accession No. ML16309A561	Vickie Smith, OCIO/PMPD/IPMB Approved by David Nelson, CIO

Note: This document establishes the U.S. Nuclear Regulatory Commission's (NRC's) policy for managing information technology (IT) assets throughout their entire lifecycle. The NRC maintains detailed processes and operating procedures in documents separate from policy documents to support continuous refinement of processes and procedures in an effort to continuously mature the NRC's IT management.

Contents

Background and Authorities

The U.S. Nuclear Regulatory Commission (NRC) acknowledges the need to manage its information technology (IT) assets throughout the five lifecycle stages (i.e., planning, acquisition, deployment, management, and retirement and disposal) in a centralized IT asset repository that accounts for the presence and purchase of all hardware and software. Therefore, the NRC is establishing this Information Technology Asset Management (ITAM) Policy and establishing an ITAM program to implement a systematic process that joins contractual, financial, inventory, and IT governance functions to support (1) management of IT assets throughout their lifecycles and (2) strategic decisionmaking for the NRC's IT environment.

The main objective is to correct a lack of formal, centralized ITAM capabilities, including software license management (SLM), a proactive approach to software asset management (SAM), and hardware asset management that has led to higher IT costs, a marginalized ability to negotiate with IT vendors, a higher risk of licensing agreement violations, and an increase to vulnerabilities of a cyberattack on the NRC infrastructure. Implementing the ITAM program will also achieve compliancy with relevant Federal mandates, policy, and guidance, including, but not limited to, the following:

- Public Law 114-210, commonly referred to as the MEGABYTE Act of 2016
- Public Law 113-291, Subtitle D, commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA)
- Public Law 111-292, commonly referred to as the Telework Enhancement Act of 2010
- Public Law 107-347, commonly referred to as the E-Government Act of 2002
- Public Law 104-106, commonly referred to as the Clinger-Cohen Act of 1996
- Executive Order 13589, "Promoting Efficient Spending," dated November 9, 2011
- Executive Order 13103, "Computer Software Piracy," dated September 30, 1998
- Office and Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," revised July 2016
- OMB Circular A-131, "Value Engineering," revised December 2013

- OMB Category Management Policy, issued in a series of memoranda, including, but not limited to,[1] the following:
  - M-16-02, "Category Management Policy 15-1: Improving the Acquisition and Management of Common Technology: Laptops and Desktops," dated October 16, 2015
  - M-16-12, "Category Management Policy 16-1: Improving the Acquisition and Management of Common Technology: Software Licensing," date June 2, 2016
  - M-16-20, "Category Management Policy 16-3: Improving the Acquisition and Management of Common Technology: Mobile Devices and Services," dated August 8, 2016
- M-16-11, "Improving Administrative Functions Through Shared Services," dated May 4, 2016
- M-15-14, "Management and Oversight of Federal Information Technology," dated June 10, 2015
- M-14-03, "Enhancing the Security of Federal Information and Information Systems," dated November 18, 2013
- M-13-02, "Improving Acquisition through Strategic Sourcing," dated December 5, 2012
- M-12-10, "Implementing PortfolioStat," dated March 30, 2012
- "Digital Government: Building a 21st Century Platform to Better Serve the American People," dated May 23, 2012, and resulting Federal strategies, such as the Network Services 2020 Strategy
- "Federal Cloud Computing Strategy," dated February 8, 2011
- Office of Federal Procurement Policy (OFPP) memorandum, "Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings," dated December 4, 2014
- OFPP memorandum, "'Myth-Busting': Addressing Misconceptions to Improve Communication with Industry during the Acquisition Process," dated February 2, 2011
- OFPP memorandum, "'Myth-Busting 2': Addressing Misconceptions and Further

[1] These three memoranda have been issued to date; however, OMB plans to issue additional Category Management Policy memoranda for other IT commodities, as well as Circular A-XXX, "Implementing Category Management for Common Goods and Services."

Improving Communication During the Acquisition Process," dated May 7, 2012

- U.S. Government Accountability Office (GAO) GAO-14-413 "Federal Software Licenses—Better Management Needed to Achieve Significant Savings Government-Wide," issued May 2014

- Federal Acquisition Regulations (FAR), including, but not limited to, the planning provisions established in FAR Subpart 7.1, "Acquisition Plans"; Part 10, "Market Research"; and Part 15, "Contracting by Negotiation," and the postaward provisions in Part 42, "Contract Administration and Audit Services"

Purpose

This document sets forth the ITAM Policy for the NRC. It establishes the business rules and guidelines for consistency and compliance in executing the NRC ITAM process and procedures for managing IT software and IT hardware throughout all lifecycle phases of an IT asset.

Note: The NRC's ITAM program, process, and procedures are a subset of the NRC's service delivery management, which integrates IT asset lifecycle management with release and deployment functions, configuration management capabilities, problem and incident management, information technology service management (ITSM), and IT project lifecycle processes. Although this document is limited to establishing ITAM policy, the success of the policy's execution depends on a cohesive and comprehensive set of integrated staff, processes, and tools supporting the NRC's IT services.

Definitions

Alternative analysis refers to a method for addressing the various options for meeting the performance objectives of an investment, including the estimated return on investment, and, if applicable, the estimated cost savings or cost avoidance of the various options. The analysis is performed before the initial decision to implement a solution and updated periodically, as appropriate, to capture changes in the context for an investment decision. This term refers to best practices outlined in Section I.4, "Alternatives to Capital Assets," and Section I.5, "Choosing the Best Capital Asset," of the Capital Programming Guide.

Business capacity management is the subprocess of capacity management responsible for understanding future business requirements for use in the capacity plan. See also "service capacity management" and "component capacity management."

Capacity management is the process used for ensuring that the capacity of IT services and the IT infrastructure is able to meet agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity management is used to identify all resources required to deliver an IT service to meet both the current and future capacity and performance needs of the business. Capacity management includes three subprocesses: (1) business capacity management, (2) service capacity management, and (3) component capacity management.

Capital programming refers to an integrated process within an agency that focuses on the planning, budgeting, procurement, and management of the agency's portfolio of capital investments to achieve the agency's strategic goals and objectives with the lowest overall cost and risk.

Category management is a structured approach that focuses on defining products and services that behave in a similar manner to create common categories of products and services across Federal agencies and allow the Federal Government to buy smarter and more like a single enterprise. This approach is a fundamental shift from the practice of handling purchasing, analyzing pricing, and developing vendor relationships individually within thousands of procurement units across Government. A coordinated implementation of the category management business model will enable the Federal Government to eliminate redundancies, increase efficiency and effectiveness, and boost satisfaction with the products and services.

Note: OFPP is responsible for promoting economy and efficiency in the acquisition process and regularly implements policies and initiatives, such as category management, to better leverage the Government's buying power to ensure taxpayer dollars are spent effectively and efficiently. The Federal Chief Acquisition Officer (CAO) has issued Category Management Policy in a number of categories of common goods and services, including IT. Category Management Policy for IT commodities is issued jointly with the Federal Chief Information Officer (CIO). While it is the responsibility of an agency's CAO to develop and implement overarching policy and guidance on category management for the agency, it is a shared responsibility with the agency's CIO to develop category management strategies and implementation plans for all IT commodities.

Change management is the process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

Cloud Computing refers to a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks; (2) powerful, inexpensive server computers; and (3) high-performance virtualization for commodity hardware.

Cloud First Policy refers to OMB's Cloud First Policy, launched in December 2010, which is intended to accelerate the pace at which the government realizes the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

Note: Per the Federal Cloud Computing Strategy, agencies shall:

- *Evaluate their technology sourcing plans to include consideration and application of cloud computing solutions as part of the budget process.*

- *Seek to optimize the use of cloud technologies in their IT portfolios to take full advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize costs.*
- *Default to cloud-based solutions when evaluating options for new IT deployments, if a secure, reliable, cost-effective cloud option exists.*
- *Continually evaluate cloud computing solutions across their IT portfolios, regardless of investment type or lifecycle stage.*

Component capacity management is a subprocess of capacity management through which the capacity, use, and performance of configuration items are understood. Data are collected, recorded, and analyzed for use in the capacity plan. See also "business capacity management" and "service capacity management."

Configuration is the generic term used to describe a group of configuration items that work together to deliver an IT service or a recognizable part of an IT service. Configuration is also used to describe the parameter settings for one or more configuration items.

Configuration item is any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management.

Configuration management refers to the technical and administrative activities concerned with the creation, maintenance, and controlled change of configuration items throughout the life of a product.

Cost is defined in Statement of Federal Financial Accounting Concepts No. 1, "Objectives of Federal Financial Reporting," as the monetary value of resources used. Cost is defined more specifically in Statement of Federal Financial Accounting Standards (SFFAS) No. 4, "Managerial Cost Accounting Concepts and Standards for the Federal Government," as the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, for example, to acquire or produce a good or to perform an activity or service. Depending on the nature of the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period) or to an asset account for recognition as an expense of subsequent periods. In most contexts within SFFAS No. 7, "Accounting for Revenue and Other Financing Sources," "cost" is used synonymously with "expense."

Cost avoidance is an action taken in the immediate timeframe that will decrease costs in the future. For example, an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs is a cost avoidance action, as defined in OMB Circular A-131, "Value Engineering," dated May 21, 1993.

Cost savings refers to the reduction in actual expenditures to achieve a specific objective, as defined in OMB Circular A-131.

Demand management is the process used to understand, anticipate, and influence customer demand for services. Demand management works with capacity management to ensure that the

service provider has sufficient capacity to meet the required demand. At a strategic level, demand management can involve analysis of patterns of business activity and user profiles, whereas at a tactical level, it can involve the use of differential charging to encourage customers to use IT services at less busy times or require short-term activities to respond to unexpected demand or the failure of a configuration item.

Hardware asset management is the process of tracking, monitoring, and reporting the physical components of computers and computer networks from acquisition through disposal to provide a comprehensive inventory of hardware assets on the IT infrastructure. This comprehensive inventory visibility supports vendor and lease management and assists in making budgetary forecasts based on the stock of assets and business requirements.

Hardware asset manager is an individual designated by, and reporting to, the CIO responsible for managing, through policy and procedure, all hardware assets and for implementing hardware asset management best practices to track and monitor hardware assets throughout their lifecycle. The hardware asset manager ensures a complete and comprehensive inventory of hardware asset is maintained in a centralized repository to provide visibility and detailed information of what is in the IT environment in support of vendor and lease management and to assist in making budgetary forecasts based on the stock of assets and business requirements.

Incident management is the process for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.

Information system refers to a discrete set of IT, data, and related resources (such as personnel, hardware, software, and associated IT services) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, in accordance with defined procedures, whether automated or manual.

Information system lifecycle means all phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing or decommissioning the system.

Information technology is defined as follows:

- The term “information technology” includes any services or equipment, or the interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency, where such services or equipment is considered “used by an agency” if it is used by the agency directly or if it is used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

- The term “information technology” includes computers; ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance); peripheral equipment designed to be controlled by the central processing

unit of a computer; software; firmware; and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of equipment or services), and related resources.

- The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

IT asset refers to anything (tangible or intangible) that has value to an organization, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software).

Note: Assets are the lowest level at which IT is planned, acquired, implemented, and operated. All IT hardware and software shall be associated with the comprising system/investment and tracked and monitored throughout their lifecycles in accordance with the NRC's ITAM processes.

IT investment refers to the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality and the subsequent operation of those assets in a production environment.

Note: Each investment is assigned a unique investment identifier (UII) for tracking, budgeting, and reporting purposes (both internally and externally to OMB).

IT resources refers to all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the IT lifecycle and acquisitions or interagency agreements that include IT and the services or equipment provided by such acquisitions or interagency agreements, not including grants that establish or support IT not operated directly by the Federal Government.

IT system refers to a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

IT service management (ITSM) is the implementation and management of quality IT services that meet the needs of the business. IT service providers perform ITSM through an appropriate mix of people, processes, and information technology. See also "service management."

Management directives (MDs) are formal documents used to reflect policy decisions already made in some other context and provide the process and guidance for implementing that policy. For example, MDs can reflect enacted legislation, issued Executive Orders, Governmentwide personnel and travel policy, Commission decisions articulated in staff requirements memoranda, and other issuances. They do not propose new policy; instead, they communicate to employees NRC policies, requirements, and procedures necessary for the agency to comply with executive orders, pertinent laws, regulations, and the circulars and directives of other Federal agencies. The NRC prepares and issues directives and directive handbooks, as well as

revisions to these documents, to meet the requirement that all Federal agencies have an internal MD system. For more information, see "MD 1.1, "NRC Management Directives System."

Service asset and configuration management is the process used to ensure that the assets required to deliver services are properly controlled and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

Service capacity management is the subprocess of capacity management responsible for understanding the performance and capacity of IT services. Information on the resources used by each IT service and the pattern of usage over time is collected, recorded, and analyzed for use in the capacity plan. See also "business capacity management" and "component capacity management."

Service level management is the process responsible for negotiating achievable service-level agreements and ensuring that all ITSM processes, operational level agreements, and underpinning contracts are appropriate for the agreed service-level targets. Service level management monitors and reports on service levels, holds regular service reviews with customers, and identifies required improvements.

Service management is a set of specialized organizational capabilities for providing value to customers in the form of services.

Software asset management (SAM) is the process of tracking, monitoring, and reporting the use and ownership of software assets throughout their lifecycle, including licenses, versions, and installed endpoints. SAM is part of an overall service and configuration management process. The goals of SAM include: (1) reducing IT costs; (2) limiting business, legal, and security risks related to the ownership and use of computer software; and (3) maximizing IT responsiveness and end-user productivity.

Software management centralization plan refers a formal, documented plan to join financial, contractual, and inventory functions to support IT asset lifecycle management and strategic decisionmaking for an agency's IT environment. Best practice is to form an ITAM program with a governance framework and set of policies and procedures to centralize the process and implement the plan. OMB M-16-12 requires agencies to establish a baseline inventory of all commercial and commercial off-the-shelf (COTS) software in the IT environment and then utilize this inventory to develop a software management centralization plan that outlines how the agency's software inventory capability will be implemented and identifies the tools that will support inventory management and reporting.

Software license management (SLM) refers to a proactive approach to SAM that enables accurate procurement and deployment of software licenses based on contract entitlements, product use rights, and actual usage.

Software manager is an individual designated by, and reporting to, the CIO responsible for managing, through policy and procedure, all agencywide commercial and COTS software agreements and licenses. The software manager serves as the subject matter expert for available Federalwide and agencywide acquisition vehicles and facilitates the agencywide effort

to centralize purchasing. The software manager develops and executes the agency's software management centralization plan in an effort to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software management best practices.

Vendor management refers to the practice of actively managing relationships with vendors to develop, manage, and control vendor contracts, relationships, and performance for the efficient delivery of contracted products and services; minimize potential business disruption; and drive the most value from vendors. Done properly, this best practice facilitates the development of agency goals and alignment with vendor capabilities and the rapidly evolving IT industry.

Vendor management strategy is a strategy developed and executed to ensure the strategic selection and prioritization of vendors (or their suppliers) and execution of vendor-specific initiatives. A current, well-maintained vendor management strategy and the implementation of processes to improve relationships with suppliers, better understand the marketplace, and support the development of IT sourcing strategies, is key to executing strategic vendor management.

IT Asset Management Policy

All NRC IT assets shall be managed in accordance with Federal mandates, OMB requirements, and agency policy and procedures. This policy establishes the business rules and guidelines below for managing IT assets throughout their lifecycles.

The NRC shall:

1. Act in a fiscally responsible manner, including by implementing an ITAM program to support the optimization of IT costs to perform mission and business functions in the most efficient manner that adds the most value.

2. Establish a comprehensive IT asset inventory by identifying and collecting information using automated discovery and inventory tools. Any tool used for SAM must specifically collect information about software license agreements and track and maintain identified software licenses to assist the agency in implementing decisions throughout the SLM lifecycle.

3. Provide training relevant to SLM to improve understanding of legal and compliance requirements, including what is expected of users with regard to the protection of intellectual property rights.

4. Assess current IT asset inventories and usage and establish controls to ensure maximum use of IT equipment, installed software, and services (i.e., ensure that the NRC needs, and is using, all IT assets that the agency is paying for). This is key to performing demand management.

5. Maintain the comprehensive IT asset data by tracking all assets from purchase to retirement and disposal, including data collected at integration points with ITSM

(e.g., capacity management, configuration management, incident management, service-level management).

6. Analyze usage and other data to make cost-effective decisions and inform IT resource planning, budgeting, and future acquisitions.

7. Right-size the number of IT devices (e.g., mobile phones, smartphones, desktop and laptop computers, and tablet personal computers) issued to employees, consistent with the Telework Enhancement Act of 2010, operational requirements (including continuity of operations), and initiatives designed to create efficiency through the effective implementation of technology.

8. Promote further efficiencies in IT by leveraging appropriate Governmentwide or agencywide IT solutions that consolidate activities such as desktop services, email, and collaboration tools.

9. Maximize the use of acquisition vehicles developed by OMB's Federal Strategic Sourcing Initiative to acquire commodity IT, and only use mandatory agencywide IT solutions if a complete alternative analysis demonstrates that to do so provides better value.

10. Develop, maintain, and communicate to end users this policy and ITAM processes and procedures, and their integration with other policies and processes that support the management of IT assets and services.

11. Build centralized ITAM processes and services around the five lifecycle stages: (1) planning and budgeting; (2) acquisition; (3) deployment; (4) management; and (5) retirement or disposal. Processes should trigger changes to contract terms and conditions to accommodate for changing technology, vendor, and internal requirements.

12. Ensure in the planning and budgeting phase that each IT asset is clearly identified and associated with the comprising system and investment in the NRC's IT portfolio (i.e., is associated with the appropriate UII listed on the Agency IT Portfolio Summary submitted to OMB).

13. Ensure that the SAM lifecycle processes have integration points with the ITSM processes, primarily with configuration and change management because the processes impact each other (i.e., a change to a platform may affect licensing).

14. Ensure that processes include clearly defined roles and responsibilities, proper governance and controls, and integration points with other processes.

15. Acquire and implement an asset management tool to support core lifecycle processes, and, to the extent practicable, integrate the solution with recognized ancillary data sources used to maintain the asset data (e.g., IT help desk).

16. Monitor the performance of the program and software assets by developing compliance reports (reporting, at a minimum, the compliance position of managed software through proper SLM) and by developing key performance indicators (KPIs) to quantify the success of the ITAM program. Some Information Technology Infrastructure Library software asset and configuration management KPIs to consider include the following:

    - percent of software licenses used relative to the total software licenses deployed (i.e., split by license per software application)
    - percent of licenses purchased but not accounted for in the asset repository
    - percent of software assets under maintenance contract

      Note: This KPI monitors the number of deployed software assets that are within their warranty or are related to a valid maintenance contract relative to the total number deployed.

17. Actively manage the NRC's relationships with vendors to develop, manage, and control vendor contracts, relationships, and performance for the efficient delivery of contracted products and services; minimize potential business disruption; and drive the most value from vendors. All preaward communications with vendors shall be conducted in accordance with the NRC Vendor Communication Plan. All postaward management will be conducted in accordance with MD 11.1, "NRC Acquisition of Supplies and Services."

18. In addition to adhering to OMB Category Management Policy and the FAR on all contracting activities, adhere to the following for the acceptance of agreements and for the acceptance and retention of compliance related documents:

    - MD 11.1
    - MD 3.53, "NRC Records and Document Management Program"
    - NUREG-0910, "NRC Comprehensive Records Disposition Schedule"
    - Acquisition guidance and procedures available in the NRC Enterprise Acquisition Toolkit, including but not limited to (1) Acquisition Instruction 2010-10, "Records Management," and (2) the "Acquisition Guidebook for Contracting Officer's Representatives."

19. Perform all software acquisitions in accordance with the MEGABYTE Act, OMB M-16-12, the FAR, and the Federal Information Security Management Act and adhere to MD 11.1. All associated software acquisition documentation shall be retained in a centralized contract repository accessible to only those personnel with the appropriate roles and responsibilities which would entitle them to access.

20. Perform all hardware acquisitions in accordance with OMB Category Management Policy (e.g., M-16-02 and M-16-20) and the FAR and adhere to MD 11.1. All associated hardware acquisition documentation shall be retained in a centralized contract repository accessible to only those personnel with the appropriate roles and responsibilities that would entitle them to access.

21. Acquire only IT assets on the NRC Technical Reference Model (TRM), the standardized list of technologies and versions approved for use in the NRC production environment, if an approved technology meets the business need instead of purchasing duplicative technologies. The process for alternatives and exceptions must be followed for the approval of any nonstandard assets.

22. Ensure that assets are receiving timely patches and are securely configured and maintain version control in compliance with underlying contracts.

23. Ensure that all NRC employees are informed of and comply with the agencywide Rules of Behavior for Authorized Computer Use Policy and OMB Circular A-130. According to the aforementioned policy, users shall not place any unauthorized software on any NRC computing device. Since trial or promotional software will be solely restricted to test environments for the purpose of evaluation before its potential acquisition, the NRC deems such software unauthorized until it is placed on the approved software list. Unauthorized use of a user account or a computing resource is a violation of 18 U.S.C. § 1030, constitutes theft, and is punishable by law. Users will be held accountable for their access and use of NRC computing resources.

24. Adhere to FAR Part 42, “Contract Administration and Audit Services,” in the event of a vendor audit. An audit response team shall be formed and follow the guidance of legal counsel and the applicable contracting officer. The audit response team shall appoint a single point of contact for all communications with the vendor conducting the audit and immediately notify all NRC personnel to cease any/all communications with the vendor.

25. Comply with the NRC property management policy throughout the lifecycle of all assets. When an asset has reached end of “life” or usability, the aforementioned policy shall be followed. In addition, CSO-PROS-2101, “NRC IT System Decommissioning and Disposal Process,” applies for assets associated with the retirement and decommissioning of an IT system.

Responsibilities

Responsibilities of the Strategic Sourcing Group (SSG)

1. Further enhance the agency’s procurement oversight process by ensuring that proposed procurement actions (i.e., commercial contracts, U.S. Department of Energy laboratory agreements, and interagency agreements) exceeding $1 million meet agency and programmatic needs and expectations and that the documentation adequately supports the proposed procurement. This includes IT procurements exceeding $1 million.

2. Monitor the progress and success of category management implementation, including the achievement of agency socioeconomic contracting goals.

3. Provide oversight of category teams, including IT category teams.

4. Provide strategic feedback on strategic sourcing strategies in all categories (including IT), such as leveraging Governmentwide acquisition vehicles and enterprisewide agreements and contracts.

Responsibilities of the CAO

1. Establish policy, process, and procedures to ensure that the OMB Category Management Policy and the principles of category management are applied throughout the NRC while ensuring that the agency's mission and small business goals are met.

2. Establish and oversee the process for analyzing all expenditures under category management and report progress to the SSG and OMB, as required and in accordance with OMB-issued guidance.

3. Establish policy and processes for all vendor communication and management.

4. Ensure contracts do not restrict or prohibit the sharing of all prices, terms, and conditions for commercial and COTS software licenses with other Government entities, including posting said information on the Acquisition Gateway.

5. In consultation with the CIO, ensure that an agencywide process is in place to ensure that all acquisitions that include any IT are: (1) led by personnel with appropriate Federal acquisition certifications, including specialized IT certifications, as appropriate; (2) reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting and use such approaches, as appropriate; (3) supported by cost estimates that have been reviewed by the CIO; and (4) adequately implementing incremental development, as appropriate.

6. Ensure that the agency shall initiate no contract actions or interagency agreements that include IT unless they are reviewed and approved by the CIO or are consistent with the acquisition strategy and acquisition plan previously approved by the CIO.

7. As member of the SSG, approve IT acquisitions exceeding $1 million.

Responsibilities of the CIO

1. Establish an ITAM program within the Office of the Chief Information Officer (OCIO) and ensure executive sponsorship and governance.

2. Define policy, process, and procedures for ITAM to include automated, repeatable processes to aggregate software license and maintenance requirements and associated funding, as appropriate, for commercial and COTS software acquisitions. The processes should include a means to review existing software that is currently in use against the

NRC's approved list of software and provisions for identified software not on the approved list (i.e., consider whether to add the product to the approved list or identify an approved alternative to replace it).

3. Ensure that an agencywide process is in place to ensure that all acquisitions that include any IT are: (1) led by personnel with appropriate Federal acquisition certifications, including specialized IT certifications, as appropriate; (2) reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting and use such approaches, as appropriate; (3) supported by cost estimates that have been reviewed by the CIO; and (4) adequately implementing incremental development, as appropriate.

4. In consultation with the CAO and other senior agency officials, as appropriate, appoint an agency software manager to manage, through policy and procedure, all agencywide commercial and commercial off-the-shelf (COTS) software agreements and licenses.

5. Ensure the maintenance of a continual agencywide inventory of IT assets, including an inventory of all software licenses purchased, deployed, and in use, as well as expenditures on subscription services (including provisional SaaS).

6. Ensure compliance with software license agreements, consolidation of redundant applications, and identification of other cost-saving opportunities.

7. Review and approve all IT acquisition strategies and acquisition plans that include IT. For contract actions that contain IT that is outside of an approved acquisition strategy or acquisition plan, the CIO shall review and approve the action itself (e.g., procurement actions for alternatives or exceptions when existing approved solutions do not meet a business need).

8. In consultation with program leadership, evaluate the appropriateness of IT-related portions of statements of need or statements of work, especially in respect to the mission and business objectives supported by the IT strategic plan and in alignment with mission and program objectives.

9. As member of the SSG, provide advice on all acquisition strategies and acquisition plans that include IT and approve IT acquisitions exceeding $1 million.

10. Ensure effective implementation of continuous diagnostics and mitigation for the agency and integration with the ITAM program and tools.

Responsibilities of the Enterprise Architecture Branch

1. Develop the target architecture and information technology/information management (IT/IM) strategic plan and roadmap to achieve the optimal, cost-effective IT portfolio to best support the agency's mission.

2. Maintain the TRM, the list of technologies and the version(s) approved for the current production environment, the legacy technologies that should be retired/decommissioned,

as well as determine future technologies that align with the target architecture and IT/IM strategic plan and roadmap.

3. Own, implement and maintain the Alternative and Exception process for determining if a technology or version should be added to the TRM and allowed into the production environment.

Responsibilities of the ITAM Program Manager

1. Make key program decisions with the support of executive leadership.

2. Manage and coordinate all aspects of the ITAM program.

3. Ensure proper coordination and seamless process flows with related programs and services.

4. Ensure overall effectiveness and efficiency of the ITAM process and procedures.

5. Oversee ITAM communication and education to all stakeholders, including end users and ITAM staff.

6. Comply with relevant Federal mandates, OMB policy, and NRC policy and procedures.

Responsibilities of the Software Manager

1. Reporting to the CIO, lead an agencywide effort, working in collaboration with the staff in the Acquisition Management Division within the Office of Administration and other organizations, as appropriate, to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software best practices.

2. Manage, through policy and procedure, all agencywide commercial and COTS software agreements and licenses.

3. Employ a centralized SAM strategy that includes development of an approved list of software and an associated implementation plan. This plan should address, at a minimum, the lifecycle phases, funding aggregation, and other considerations, including the use of SaaS.

4. Lead an evaluation of software products in the NRC IT environment to validate that they are meeting business needs based on technical requirements.

5. Increase the use of Governmentwide software license agreements and implement strategies to reduce duplication of products meeting the validated needs.

6. Ensure, through effective market research, that terms and conditions in agency commercial license agreements are consistent with customary practices to the maximum extent practicable and are negotiated to meet the agency's needs.

7. Develop and implement a vendor management strategy that includes processes to improve relationships with suppliers and support the development of IT sourcing strategies.

8. Ensure that the personnel involved in SAM (e.g., legal, acquisition, system administration, technical support, and users (as appropriate)) are trained in relevant software management topics, such as intellectual property and software contracts, license negotiations, license compliance laws, regulations, software audits, security planning, configuration management, provisional services (i.e., SaaS), and compliance with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)).

9. Develop and implement an assessment and approval process to determine the cost and benefit of purchasing software maintenance programs. The process should include a means of assessing operational impacts and risks, including information security and privacy as described in OMB Circular A-130 and other related OMB guidance.

10. Use software policies, processes, and procedures to identify and thwart software piracy and theft.

11. Remain knowledgeable of all available Federalwide and agencywide acquisition vehicles and facilitates the agencywide effort to centralize purchasing.

12. Develop and execute the agency's software management centralization plan in an effort to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software management best practices.

Responsibilities of the Hardware Asset Manager

1. Implement and build controls for the hardware inventory to ultimately associate assets to lifecycle, status, locations, and documentation for all hardware devices.

2. Maintain visibility into hardware asset processes and build controls for hardware assets throughout the lifecycle to maximize value, provide data on hardware assets to support customer demand, maintenance and operations, and strategic decisionmaking.

3. Develop, implement, and promote policies, processes and procedures for hardware asset acquisitions, installations, usage, and disposition.

4. Manage, through policy and procedure, all hardware assets.

5. Remain knowledgeable of all available Federalwide and agencywide acquisition vehicles for IT hardware and facilitate the agencywide effort to centralize purchasing.

IT Asset Lifecycle Management Overview

IT asset lifecycle management is a core process of ITAM that involves managing and optimizing the purchase, deployment, maintenance, use, and retirement or disposal of assets within an organization. Implementation of this process can benefit organizations by improving the ability to forecast needs. IT asset lifecycle management strives for informed purchasing decisions, proactive resource replenishment, improvement of the quality of IT services, and knowledge of the total cost of ownership of an asset. Activities include the development and maintenance of policies, standards, processes, systems, and measurements that enable organizations to manage the IT asset portfolio with respect to risk, cost, control, IT governance, compliance, and established business performance objectives. Figure 1 provides an overview of the ITAM lifecycle management process.

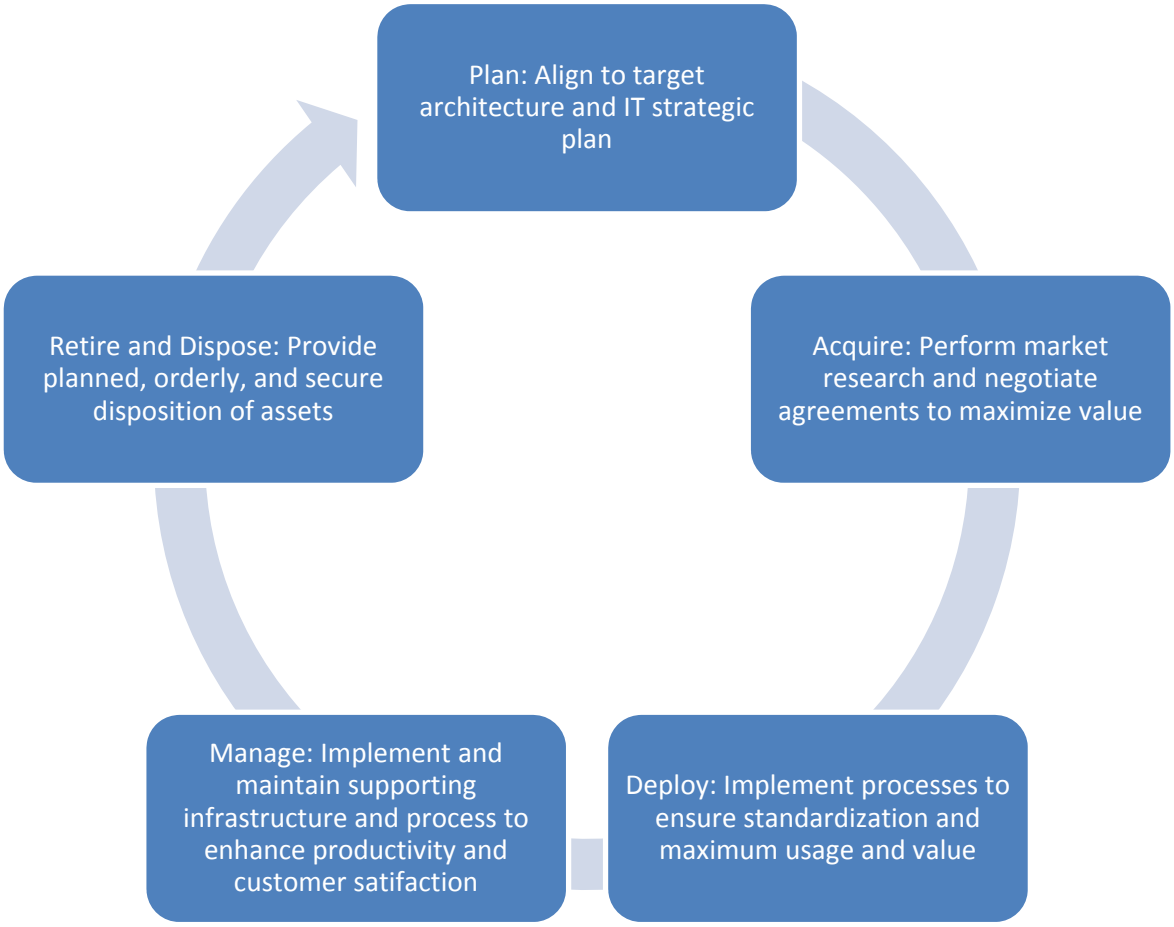

Figure 1. IT asset lifecycle management process

Plan

The planning phase involves the activities performed before procurement of the software, which include evaluating the technical and organizational requirements for the IT asset. Asset

requirements are defined based on an assessment of both service delivery needs and the capability of the existing asset base to meet these needs. Planning activities include, but are not limited to, defining the asset management strategy, planning for uncertainties, documenting business cases, and performing a cost-benefit analysis.

Acquire

For ITAM purposes, the acquisition phase is the process by which an organization plans and then manages the procurement process. This includes receiving a legitimate request and approval for goods and services (including standards, definitions, and supplier identification) and discounting targets and policies under negotiated discounts and contracts. Ultimately, the goal of the procurement process is to enable the best price for the best product and service available to meet the organization's needs while providing full visibility to surplus.

Deploy

The deployment phase involves deploying new software and hardware requests through the defined approval method. If the asset request has been approved, the IT configuration manager will install software and hardware on the user's machine. He or she will ensure that the equipment is fully configured and ready for use. The asset repository must be correct before allocating any equipment. The asset entry should also include all software and hardware installed. Because the information about the asset will never be more accurate than it is at this stage, a best practice is for the IT asset manager to determine the accuracy of the asset as it enters the configuration management database to enable a clean start.

Manage

The management phase involves the monitoring of an asset's maintenance needs and performance, management of refresh cycles, information management, asset valuation, and continuous assessment of the asset's use and functionality. Responsible parties should evaluate the existing asset's base condition, capability, and usage. Accurate recording, identification, valuation, and reporting procedures must be established so that informed decisions to maintain, modify, rehabilitate, find an alternative use for, or dispose of an asset can be made.

Retire and Dispose

The retirement and disposal phase involves the planning and execution of the removal and disposal of assets, closing or cessation of contracts and licenses, and proper deinstallation. The treatment of an asset that has either reached the end of its useful life, is considered surplus, or is underperforming. Retiring an asset can include disposal, replacement, renewal, or redeployment. Responsible parties should comply with relevant approval processes and, where possible, select a method, including retirement, replacement, renewal, or redeployment, that maximizes the financial benefits associated with the method.