U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 2.8	INTEGRATED INFORMATION TECHNOLOGY/ INFORMATION MANAGEMENT (IT/IM) GOVERNANCE FRAMEWORK	DT-17-102
Volume 2:	Information Technology	
Approved By: *Date Approved:* *Cert. Date:*	Victor M. McCree Executive Director for Operations February 24, 2016 N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer Solutions Development Division	
Contacts:	Wil Madison 301-415-7221	Menelik Yimam (for IT/IM Investment Management) 301-415-0200 Edwin Leong (for Enterprise Architecture) 301-415-6704

EXECUTIVE SUMMARY

Directive and Handbook 2.8 establish a single integrated framework to ensure efficient and effective governance of information technology/information management (IT/IM) investments. The Integrated IT/IM Governance Framework encompasses activities spanning the full lifecycle of IT investments, including strategic planning and enterprise architecture, IT investment management, and project management. It also references related processes, such as business process improvement, cybersecurity, and records management, as applicable.

This revision expands and retitles this management directive from “Project Management Methodology (PMM)” to “Integrated Information Technology/ Information Management (IT/IM) Governance Framework”; however, PMM remains a major component of the Integrated IT/IM Governance Framework as referenced in this directive.

TABLE OF CONTENTS

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission (NRC) to ensure efficient and effective governance of all information technology and information management (IT/IM) investments throughout their lifecycle, in a manner that maximizes value and minimizes risk, in accordance with Federal statutes, regulations and guidance. The strategy for implementing this policy is to use an Integrated IT/IM Governance Framework.

II. OBJECTIVES

– Establish the Integrated IT/IM Governance Framework as the strategy for implementing the NRC's policy regarding complete lifecycle governance of the agency's IT/IM investments.

- Outline the roles and responsibilities associated with the Integrated IT/IM Governance Framework, with a focus on the following governance activities and disciplines:
  - Strategic planning and enterprise architecture,
  - IT investment management, and
  - Project management.
- Explain the relationship with other agency processes, such as business process improvement, privacy, cybersecurity, and information and records management.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Chairman

1. Serves as the highest authority for reasonable assurance of internal control throughout the agency as stipulated in MD 4.4, "Internal Control."
2. Maintains contracting authority which is delegated to the Executive Director for Operations (EDO) for the initiation of IT/IM investments that meet the approval thresholds set forth in MD 11.1, "NRC Acquisition of Supplies and Services," and the criteria of this directive and its related handbook.
3. Reviews the IT budget request included in the overall agency budget recommended by the Executive Director for Operations (EDO) and the Chief Financial Officer (CFO), and submits final recommendations to the Commission.

B. Commission

Reviews and approves the agency's IT budget request included in the overall agency budget.

C. Executive Director for Operations (EDO)

The Executive Director for Operations (EDO) has inherent governmental authority, must be a Government employee, and is responsible for the following as it relates to the IT/IM Governance Framework:

1. Establishes the Integrated IT/IM Governance Framework as the strategy for implementing the NRC's policy regarding the management and evaluation of the agency's IT/IM investments.
2. Ensures the NRC's planning and budgeting process for IT/IM investments is consistent and integrated with the agency's overall Planning, Budgeting, and Performance Management (PBPM) process.
3. Ensures that statutory responsibilities regarding IT/IM investments and their oversight are appropriately assigned to the Chief Information Officer (CIO).

4. Provides oversight and leadership for internal control over programmatic operations as defined in MD 4.4, “Internal Control,” in compliance with the Office of Management and Budget’s (OMB) Circular A-123, “Management’s Responsibility for Internal Control,” and other laws and regulations.
5. Ensures that program office and IT/IM officials participate in the PBPM process for IT/IM investments throughout their lifecycle.
6. Reviews and approves the IT/IM Strategic Plan submitted by the CIO.
7. Delegates responsibility to the CIO to approve the Enterprise Architecture (EA) and Enterprise Roadmap.
8. Together with the CFO, reviews and approves the selections and budget for the IT/IM investment portfolio recommended by the Information Technology/Information Management Portfolio Executive Council (IPEC) and submits recommendations to the Chairman.
9. Designates the Designated Approving Authority (DAA) to assume formal responsibility for approving the operation of an IT/IM system at an acceptable level of risk based on an agreed-upon set of implemented security controls, in accordance with the Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, and guidelines set forth by the National Institute of Standards and Technology (NIST).

D. Chief Information Officer (CIO)

The Chief Information Officer (CIO) has inherent governmental authority, must be a Government employee, and is responsible for the following as it relates to the IT/IM Governance Framework:

1. As delegated by the EDO, develops and oversees an agencywide IT/IM Governance Framework.
2. Serves as the agency business line lead for IT/IM.
3. Together with the CFO, Deputy CIO, the IPEC, and the Information Technology/Information Management Board (ITB), provides an executive investment review function, as required by the Office of Management and Budget (OMB).
4. Provides yearly budget formulation guidance for IT/IM investments in conjunction with the CFO.
5. Concurs on the selections and budget for the IT/IM investment portfolio recommended by the IPEC and submits recommendations to the EDO.
6. Co-chairs the IPEC with the CFO, approves its membership, and approves revisions to its charter as needed.

7. Establishes other executive and technical review or advisory bodies, as necessary, to involve program office officials in IT/IM investment planning and management oversight; ensures agencywide coordination; and supports compliance with the Capital Planning and Investment Control (CPIC) requirements for IT/IM investments, EA, security, and information and records management, as stated in Part 7 of OMB Circular A-11 and OMB Circular A-130.
8. Establishes the Architecture Council (AC) and approves its charter.
9. Provides IT/IM guidance and strategic direction to the IPEC, the ITB, and the AC.
10. As delegated by the EDO, approves the EA and Enterprise Roadmap.
11. Facilitates the implementation of a sound, cost-effective, and integrated EA that supports the NRC's mission.
12. Seeks advice, as necessary, from the IPEC, ITB, AC, and other appropriate advisory bodies regarding the mission/business impacts of proposed changes to the EA.
13. Approves all IT/IM contracts, services, and purchases, or delegates authority consistent with the Federal Information Technology Acquisition Reform Act of 2014 (FITARA).
14. Approves submittals to OMB, Congress, and Government Accountability Office (GAO) related to IT/IM investment programs and projects.
15. Reviews the NRC IT/IM Strategic Plan and submits it to the EDO for approval.

E. Designated Approving Authority (DAA)

1. The DAA is a committee consisting of senior executives with authority (designated by the EDO), accountability, and responsibility for approving the operation of an IT/IM system at an acceptable level of risk based on an agreed-upon set of implemented security controls. The DAA has inherent governmental authority, and is comprised of officials who must be Government employees and must have a level of authority commensurate with understanding and accepting such security risks. The DAA for major IT investments is collectively the Deputy Executive Director for Reactor and Preparedness Programs (DEDR), the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital (DEDM), and the CIO. The DAA for non-major IT investments is collectively the Deputy Chief Information Officer (DCIO) and the Director of the Information Security Directorate (OCIO/ISD).
2. The DAA is responsible for determining through the system authorization process if residual risk is acceptable based on the review and recommendation of the Chief Information Security Officer (or designee) and decides if an Authorization to Operate is granted or denied. Upon authorization of system operation, the DAA explicitly

accepts the risk to agency operations, agency assets, or individuals based on the implementation of an agreed upon set of security controls for the system, including any residual risks identified through continuous monitoring. For specific responsibilities, please refer to MD 12.5, "NRC Cybersecurity Program."

F. Chief Financial Officer (CFO)

1. Together with the EDO and CIO, reviews and approves the selections and budget for the IT/IM investment portfolio recommended by the IPEC and submits recommendations to the Chairman, in accordance with the Federal IT Acquisition Reform Act (FITARA).
2. Ensures that the appropriate financial officials participate in the PBPM process for IT/IM investments throughout their lifecycle.
3. Co-chairs the IPEC with the CIO.
4. Coordinates financial system plans with the CIO to ensure consistency with overall agency IT/IM plans and architecture.
5. Ensures that IT/IM investments are implemented, managed, and evaluated in accordance with Federal statutes and regulations by obtaining CIO approval of IT/IM-related portions of the agency's investment submittals to OMB, Congress, and GAO.
6. Maintains an inventory of the agency's capital assets, including internal use software that meets the requirements set by the Federal Accounting Standards Board (FASB) in the Statement of Federal Financial Accounting Standard No. 10, "Accounting for Internal Use Software."
7. Establishes policies and procedures for accounting for internal use software development projects.
8. Ensures that office personnel comply with the guidelines for accounting for internal use software set by the Office of the Chief Financial Officer (OCFO).

G. Deputy Chief Information Officer (Deputy CIO)

1. As delegated by the CIO, implements the agencywide IT/IM Governance Framework, which serves as the strategy for achieving the following objectives, consistent with the NRC policy set forth above:
   (a) Ensures that all IT/IM investments are effectively managed and evaluated throughout their lifecycle, in a manner that maximizes value and minimizes risk, in accordance with Federal statutes and regulations.

(b) Oversees the processes, methods, and guidance for the following activities and disciplines, which span the lifecycle of IT/IM investments:

(i) Strategic planning and enterprise architecture,

(ii) IT/IM investment management,

(iii) Project management methodology (PMM),

(iv) Information and records management,

(v) Cybersecurity policy implementation, and

(vi) Current Federal IT/IM Mandates (e.g., Accessibility, HSPD-12, IPv6).

(c) Ensures that the NRC's IT/IM investments support the agency's mission.

(d) Addresses guidance and requirements from OMB.

(e) Ensures the NRC's planning and budgeting process for IT/IM investments is consistent and integrated with the agency's overall PBPM process.

2. Directs system owners to develop remediation plans for at-risk major IT/IM investments.

3. Works with offices to plan, acquire, and operate all IT/IM hardware, software, and services that are not encompassed by OCIO-managed IT/IM infrastructure services.

4. Assigns staff to provide guidance and training to assist business sponsors, program/project managers, and others in implementing the PMM process and understanding the EA and CPIC requirements, as they relate to IT/IM investments.

H. Director, Information Security Directorate (ISD), OCIO, and Chief Information Security Officer (CISO)

1. Provides cybersecurity requirements, processes, procedures, standards, and templates for IT efforts.

2. Identifies and reports on cybersecurity issues with proposed investments.

3. Provides oversight of IT efforts to identify cybersecurity risks.

4. Provides an assessment of risk and authorization recommendations for IT implementations to the NRC DAA.

I. Office Directors and Regional Administrators

1. Identify and sponsor the IT/IM investments that are used or needed to perform business processes within the office or region.

2. Provide the CIO, CFO, Deputy CIO, IPEC, ITB, and/or OCIO with information on office or regional IT/IM investments, needs, and plans, as requested to support agencywide IT/IM planning, budgeting, and investment control.
3. Establish plans to implement and monitor office or region IT/IM investments, considering budget implications (e.g., reprioritizing resources or requesting additional funding as needed).
4. Define the requirements, project plans, and management approaches needed to support the business needs of the office or region.
5. Support participation in IT/IM investment planning and oversight by designating staff to represent the office or region for agency review or advisory bodies, including the IPEC, ITB, AC, and other bodies established under the authority of this directive (membership reflects the size and scope of the IT/IM investments owned or sponsored by the participating offices/regions).
6. Ensure the PMM processes and procedures are applied to the appropriate level of detail to protect the agency's IT/IM investments.
7. Provide for continuity of operations and compliance with legislative mandates.
8. Ensure office and regional staff involved in IT/IM investment management are trained in and comply with this management directive (MD) as well as records and information management (RIM) and cybersecurity requirements.
9. Ensure IT/IM investments include all required resources for compliance with MD 12.5.
10. Ensure that IT/IM acquisitions, systems development projects, and other related activities adhere to the agency's infrastructure and technology standards established by the SP/EA Program.
11. Accept accountability and ownership of data required or created by the office or region, as negotiated with OCIO staff and adhere to information and records quality principles.
12. Designate office representatives to serve as data stewards to manage office or regional business data in accordance with data administration policies, procedures, and standards including those stated in MD 3.53, "NRC Records and Document Management Program."
13. Manage major IT/IM investments to within 10 percent of planned cost, schedule, performance, and quality goals using the earned value management (EVM) methodology described on the PMM Web site (http://www.internal.nrc.gov/pmm).
14. Manage major IT/IM investments to ensure that they meet the return on investment approved in the business case (in addition to using EVM data to monitor progress).

15. In cooperation with and as directed by the CIO, develop investment improvement plans for at-risk major IT/IM Investments and submit these plans to the IPEC.
16. Designate a qualified project manager for each new and existing IT/IM investment to coordinate the resources, funding, and business impacts for the sponsoring office and to perform the day-to-day operational activities to ensure that the investment is implemented in accordance with this management directive and handbook.
17. Ensure IT/IM investments are protected by storing project artifacts in an approved agencywide configuration management system maintained by OCIO, and by implementing a configuration management process in accordance with the NRC Master Configuration Management Plan using an approved OCIO configuration management tool.
18. Ensure that information is provided to the agency's portfolio management system to track and manage the progress and results of IT/IM investments sponsored by the office or region.
19. Ensure and validate annually that all sponsored IT/IM investments have business benefits that exceed or justify the costs of continued operation and maintenance.
20. Ensure that all sponsored IT/IM investments in which the costs exceed the business benefits are appropriately remediated or submitted for decommissioning consideration within 90 days of this determination.
21. Certify that system security controls listed in the system security plan have been assessed using the methods and procedures described in the system security test and evaluation plan and the contingency plan, are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements for the system.
22. For decommissioned systems, certify that the approved system decommissioning process was followed as explained in current agency cybersecurity policy, and that the system is no longer being used by NRC.
23. Certify that systems meet mandatory requirements for implementing records retention and disposition of records and data as approved by National Archives of Records Administration (NARA) and according to 36 CFR 1234.10.

J. NRC Records Officer

1. In coordination with NRC's senior agency officials, CIO, and DCIO, ensures that the design and implementation of NRC's electronic information systems and documentation incorporate Federal and NRC's requirements for electronic recordkeeping.

2. Provides approval for use of electronic information systems for recordkeeping purposes as defined in MD 3.53, "NRC Records and Document Management Program."
3. Provides records and information management (RIM) guidance and assistance to all organizational levels, including training and outreach to appropriate staff in carrying out their related duties.
4. Manages the NRC's agencywide Information and Records (IRM) Program by applying information and records management principles to all of the NRC's information assets and systems.
5. Audits the IRM Program in all offices to ensure compliance with established policies and procedures, including guidance for maintaining records in electronic form.
6. Serves as senior liaison with NARA, GSA, OMB, GAO, and other agencies on matters relating to records management.
7. Develops records schedules for records in all media created and received by the NRC and obtains NARA approval before implementation.

K. Information Technology/Information Management Portfolio Executive Council (IPEC)

1. The IPEC is a cross-agency executive management body established by the EDO in concert with the CIO to determine the NRC's IT/IM strategic direction and to manage its IT/IM portfolio as required by the Clinger-Cohen Act, OMB Circular A-130, and FISMA. The IPEC is co-chaired by the CIO and CFO, and its members include office directors from major NRC offices as well as technical advisors from OCIO, OCFO, ISD, and the Office of Administration (ADM).
2. The most current and comprehensive information on IPEC responsibilities is available in the IPEC charter. At a high level, the IPEC has the following responsibilities:
   (a) Decides the agency's IT/IM direction, values, information security activities, and risk tolerance to achieve strategic program objectives.
   (b) Establishes the ITB, appoints its co-chairs, and approves its membership and charter.
   (c) Approves major investments that will effectively integrate into the IT/IM portfolio.
   (d) Ensures that NRC's IT/IM investments support the agency's strategic plan, goals, and priorities.
   (e) Reviews the IT/IM investment portfolio in the year of execution to address current fiscal year priorities.

(f) Reviews and prioritizes the IT/IM investment portfolio provided by the ITB in the planning year, ensuring a balance of programmatic and infrastructure support.

(g) Oversees the execution of IT/IM investments by reviewing the portfolio health on a quarterly basis against established direction, values, and risk tolerance.

(h) Serves as a forum for addressing agency-level IT/IM initiatives and issues.

(i) When requested by the CIO, performs the executive review function for significant issues in the management control and evaluation phases of CPIC.

(j) Makes a final determination on ITB recommendations for IT/IM investments with a variance of 10 percent or more from baseline cost, schedule, or performance goals.

(k) Communicates IPEC discussions and decisions to other NRC boards and/or committees.

L. Information Technology/Information Management Board (ITB)

1. The ITB is a cross-agency review body established by the CIO to review new proposals and current IT/IM investments based on IPEC priorities and to conduct periodic performance reviews of IT/IM investments, their alignment with the agency's strategic plan and enterprise roadmap. The ITB is comprised of senior NRC managers who apply their knowledge of the agency's mission, business goals, and processes to direct the investment of IT/IM resources toward those projects that will make the greatest contribution to the mission and performance goals of the agency. The primary focus of the ITB is to analyze business cases; align IT/IM investments and technology standards with the NRC's mission and IT/IM Strategic Plan; oversee investment risks; and make resource, investment, and priority recommendations.

2. The most current and comprehensive information on ITB responsibilities is available in the ITB charter. At a high level, the ITB has the following responsibilities:

   (a) Reviews new IT/IM proposals based on IPEC priorities for the ability to integrate effectively into the EA, alignment with strategic technology direction and standards, and potential risks to the NRC and its IT/IM environment. Based on the defined CPIC levels for the proposal, the ITB will evaluate and make a recommendation for approval or disapproval of all IT/IM business investment needs within the NRC.

   (b) Reviews performance of existing IT/IM investments by—

      (i) Conducting annual control phase reviews on major IT/IM investments as identified in the NRC OMB Exhibit 300 submissions.

      (ii) Making recommendations to suspend or cancel IT/IM investments based on priority changes, heightened risk profiles, excessive costs, and other factors.

(iii) Reviewing and approving changes to the agency's IT/IM investments including related changes for privacy and information and records management.

M. Architecture Council (AC)

1. The AC acts as a control gate in the project lifecycle methodology to ensure that necessary deliverables are produced. The AC oversees and monitors the NRC's IT/IM projects and infrastructure services, serves as a platform to discuss and promote innovative ideas in the application of IT, and provides technical analysis to the CIO and the IT/IM Board (ITB).
2. The most current and comprehensive information on AC responsibilities is available in the AC charter. At a high level, the AC has the following responsibilities:

   (a) Supports the enterprise architecture.

   (b) Manages NRC's architecture and technical standards.

   (c) Oversees all IT/IM projects.

   (d) Leads change and configuration management.

   (e) Coordinates with the ITB and IPEC.

   (f) Fosters innovation.

N. Strategic Sourcing Group (SSG)

1. Provides senior-level oversight of the strategic acquisition business process improvements. The most current and comprehensive information on the SSG responsibilities is available in the SSG charter.
2. Enhances the agency's procurement oversight process by ensuring that proposed procurement actions (i.e., commercial contracts, DOE laboratory agreements, interagency agreements) exceeding $1 million meet agency and programmatic needs and expectations, and that the documentation adequately supports the proposed procurement.

O. IT/IM Portfolio Councils (ITPCs)

1. Conduct centralized IT/IM acquisition planning.
2. Develop strategic sourcing plan.
3. Perform IT/IM spend analysis.
4. Monitor and recommend acquisition performance metrics.

IV. APPLICABILITY

A. The policy and guidance associated with the IT/IM Governance Framework presented in this directive and its related handbook apply to all NRC headquarters and regional employees and support contractors who play a role in IT/IM investments that are planned, selected, acquired, developed, maintained, or enhanced by or for the NRC.

B. In accordance with OMB Circular No. A-130 related to management and oversight of Federal Information Resources, implementation will not impact the independence of the Office of the Inspector General (OIG), nor the authorities the Inspector General (IG) has over the personnel, performance, procurement, and budget of the OIG.

V. DIRECTIVE HANDBOOK

Handbook 2.8 facilitates IT/IM Investments and project management by providing access to relevant guidance, method principles, processes, management tools, and links to the required documents/artifact templates, and other standards to be followed for each of the following major components associated with the Integrated IT/IM Governance Framework:

A. Strategic Planning and Enterprise Architecture (see Exhibit 1 of this handbook),

B. IT Investment Management (see Exhibit 2 of this handbook), and

C. Project Management Methodology (see Exhibit 3 of this handbook).

VI. EXCEPTIONS

A. Exceptions to or deviations from this directive and handbook, as well as the exhibits, may be granted by the CIO on a case-by-case basis.

B. In accordance with OMB guidance on management and oversight of Federal Information Technology, implementation will not impact the independence of the OIG and authorities the IG has over the personnel, performance, procurement and budget of the OIG.

VII. REFERENCES

Code of Federal Regulations

10 CFR 2.390, “Public Inspections, Exemptions, Requests for Withholding.”

10 CFR Part 9, “Public Records.”

10 CFR 73.21, “Protection of Safeguards Information: Performance Requirements.”

36 CFR Part 1194, “Electronic and Information Technology Accessibility Standards.”

Executive Orders

Executive Order 12600, "Predisclosure Notification Procedures for Confidential Commercial Information," June 23, 1987.

Executive Order 13392, "Improving Agency Disclosure of Information," December 14, 2005.

Memoranda

Presidential Memorandum, "The Freedom of Information Act," January 21, 2009.

Attorney General Memorandum, "The Freedom of Information Act," March 19, 2009.

National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, Div. A, tit.

OMB Memorandum M-15-14, "Management and Oversight of Federal Information Technology," June 10, 2015.

Federal Financial Management Improvement Act, 1996.

Circular A-123 – Management's Responsibilities for Internal Control.

OMB Memorandum, "Improving the Accessibility of Government Information," July 19, 2010.

NRC Documents

Charter for the NRC Architecture Council (ML15134A474).

Charter for the NRC Information Technology/Information Management Board (ITB) (ML12094A174).

Charter for the NRC IT/IM Portfolio Executive Council (IPEC) (ML13247A436).

NRC Commission Internal Procedures, Office of the Secretary of the Commission.

NRC Enterprise Roadmap (ERM) (ADAMS Accession No. ML15121A591).

NRC Management Directives—

2.6, "Information Technology Infrastructure."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

4.1, "Financial Management Systems."

4.3, "Accounting Policies and Practices."

4.4, “Internal Control.”

8.8, “Management of Allegations.”

8.14, “Agency Action Review Meeting (AARM).”

10.162, “Disability Programs and Reasonable Accommodation.”

11.1, “NRC Acquisition of Supplies and Services.”

12.1, “NRC Facility Security Program.”

12.2, “NRC Classified Information Security Program.”

12.5, “NRC Cybersecurity Program.”

12.6, “NRC Sensitive Unclassified Information Security Program.”

12.7, “NRC Safeguards Information Security Program.”

NRC Strategic Planning and Enterprise Architecture Program.

NUREG-0910, “NRC Comprehensive Records Disposition Schedule.”

NUREG-1614, “NRC Strategic Plan.”

NUREG-1908, Vol. 2, “Information Technology/Information Management Strategic Plan Fiscal Years 2012—2016.”

Other Documents

Department of Justice, “Freedom of Information Act Guide and Privacy Act Overview” (available in the FOIA/PA office).

Federal Accounting Standards Board, Statement of Federal Financial Accounting Standard No. 10, “Accounting for Internal Use Software.”

NIST 800-64, Rev. 2, “Security Consideration in the System Development Life Cycle.”

NIST SP 800-37, Rev. 1, “Guide for Applying the Risk Management Framework to Federal Information Systems.”

OMB Circular A-11, “Preparation, Submission, and Execution of the Budget,” June 30, 2015.

OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000.

Uniform Freedom of Information Act Fee Schedule and Guidelines, 52 FR 10012, March 27, 1987.

United States Code

Chief Financial Officers Act of 1990, Pub. L. 101–576.

E-Government Act of 2002, Pub. L. 107-347.

Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-347.

Federal Information Technology Acquisition Reform Act (FITARA) of 2014, Pub. L. 113-291.

Freedom of Information Act (5 U.S.C. 552, as amended).

Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), Pub. L. 104-106 (40 U.S.C. 1401 et seq.).

Inspector General Act of 1978 (5 U.S.C. App. 3).

Privacy Act of 1974 (5 U.S.C. 552a).

Open Government Act of 2007, Pub. L. No. 110-175.

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d, as amended).

U.S. NUCLEAR REGULATORY COMMISSION DIRECTIVE HANDBOOK (DH)

DH 2.8	INTEGRATED INFORMATION TECHNOLOGY/ INFORMATION MANAGEMENT (IT/IM) GOVERNANCE FRAMEWORK	DT-17-102
Volume 2:	Information Technology	
Approved By:	Victor M. McCree Executive Director for Operations	
Date Approved:	February 24, 2016	
Expiration Date:	February 24, 2021	
Issuing Office:	Office of the Chief Information Officer Solutions Development Division	
Contacts:	Wil Madison 301-415-7221	Menelik Yimam (for IT/IM Investment Management) 301-415-0200 Edwin Leong (for Enterprise Architecture) 301-415-6704

EXECUTIVE SUMMARY

Directive and Handbook 2.8 establish a single integrated framework to ensure efficient and effective governance of information technology/information management (IT/IM) investments. The Integrated IT/IM Governance Framework encompasses activities spanning the full lifecycle of IT investments, including strategic planning and enterprise architecture, IT investment management, and project management. It also references related processes, such as business process improvement, cybersecurity, and records management, as applicable.

This revision expands and retitles this management directive from “Project Management Methodology (PMM)” to “Integrated Information Technology/ Information Management (IT/IM) Governance Framework”; however, PMM remains a major component of the Integrated IT/IM Governance Framework as referenced in this directive.

TABLE OF CONTENTS

EXHIBITS

I. GENERAL

A. Federal Requirements

The NRC Integrated Information Technology/Information Management (IT/IM) Governance Framework meets the requirements set forth by Congress, including requirements established in the Clinger Cohen Act and the Federal Information Technology Acquisition Reform Act (FITARA), the Office of Management and Budget (OMB), the National Archives and Records Administration (NARA), and Federal Information Security Modernization Act (FISMA). This policy is based on guidance from both OMB and the Government Accountability Office (GAO) and incorporates best practices and standards from the National Institute of Standards and Technology (NIST) and the Project Management Institute (PMI), as well as other industrywide standards.

B. Roadmap

In this handbook, the individual exhibits describe the method principles, processes, document/artifact templates, and other standards established for each of the components associated with the Integrated IT/IM Governance Framework, including strategic planning and enterprise architecture (SP/EA), IT investment management, and project management methodology (PMM).

C. Background

In the previous approach, the PMM encompassed project planning, enterprise architecture (EA), capital planning and investment control (CPIC), security, and other system lifecycle functions as part of a single overarching method. To better support the dynamic and evolving nature of these interrelated functions, this management directive introduces and describes an Integrated IT/IM Governance Framework, in which PMM is one component.

D. Components of the Integrated IT/IM Governance Framework

1. The Integrated IT/IM Governance Framework focuses on the definition and integration of key oversight, as well as the management and delivery capabilities associated with overall management of the agency IT/IM portfolio. The key components of the Integrated IT/IM Governance Framework include—

   (a) Strategic Planning and Enterprise Architecture (SP/EA) (see Exhibit 1),

   (b) IT Investment Management (see Exhibit 2), and

   (c) Project Management Methodology (see Exhibit 3).

2. Although each component of the framework is unique, substantial interdependencies exist that require all individuals working in these areas to understand the context and relationship of the others.

3. These key components of the framework represent the broad pillars used by the agency to help ensure successful IT/IM investment delivery and realization of each investment's intended benefits. These areas as well as the information contained within this handbook and related sites are not intended to fully encompass all aspects of IT/IM management. The Integrated IT/IM Governance Framework supports, and is supported by, a number of related IT/IM functions and their related Federal and agency policies, including but not limited to cybersecurity and records management (see Exhibit 4).

4. For more information on internal controls and risk management, refer to Management Directive (MD) 4.4, "Internal Controls," and OMB Circular A-123, "Management's Responsibility for Internal Control."

II. INTEGRATED IT/IM GOVERNANCE FRAMEWORK

As defined in this management directive, the Integrated IT/IM Governance Framework encompasses the processes, methodologies, and guidance for the following activities, which span the full lifecycle of IT/IM investments.

A. Strategic Planning and Enterprise Architecture (SP/EA)

SP/EA provides an understanding of IT investment opportunities and impacts; helps formulate high-level IT goals, strategies, and initiatives; and provides architectural support for both new development projects and ongoing operations and maintenance. SP/EA accomplishes this by helping define agency IT/IM plans, technical standards, approved technologies, software development patterns, and other guidance to guide the agency's operating environment.

1. The NRC's IT/IM governance functions require the review of new proposals as well as current IT/IM investments; ensure alignment with the agency's strategic goals and priorities; ensure alignment with agencywide architecture; ensure conformance with the agency's approved technology standards; and ensure compliance with the agency's cybersecurity program as defined in MD 12.5. The NRC's IT/IM governance bodies are described in the related exhibits of this handbook and describe in more detail the specific implementation of MD 2.8 related to SP/EA.

2. In NUREG-1908, Vol. 2, "Information Technology/Information Management Strategic Plan Fiscal Years 2012—2016," NRC describes the governance roles, responsibilities, and processes required to effectively and efficiently deliver IT/IM business solutions, balancing compliance with service and efficiency.

B. IT Investment Management

1. IT investment management is responsible for managing the CPIC lifecycle for each system and the overall portfolio, including selection, control, and evaluation of IT/IM by—

   (a) Grouping development activities, along with operations and maintenance activities, into overarching agency investments; budgeting activities at multiple levels (e.g., project level, system level, and investment level).

   (b) Focusing attention at the aggregate level with a primary objective to identify, select, finance, monitor, and maintain the appropriate mix of initiatives to achieve organizational goals and objectives.

2. IT investment management implements a set of processes and procedures to plan, budget, procure, manage during use, and dispose of IT investments. Critical to good IT investment management are mature Capital Planning and Investment Control (CPIC) processes that ensure IT investments align with the agency's mission and support recognized business needs, while balancing risks (technical, financial, mission, and cybersecurity) and maximizing returns throughout the investment's lifecycle. IT investments must include budgeting for full lifecycle funding, including cybersecurity and operations and maintenance through decommissioning.

3. NRC's CPIC policy and processes are implemented and continuously refined through lessons learned and use of best practices to plan, control, select and evaluate the performance of investments in pursuit of the "To-Be" architecture defined in the agency's enterprise roadmap (ERM) with the ultimate goal of achieving an IT portfolio that leverages IT for strategic outcomes.

C. Project Management Methodology

1. Project management methodology (PMM) encompasses the processes and guidance associated with planning and oversight of individual IT/IM projects within the portfolio, and includes reporting of project progress, status and results. Each IT/IM project represents a temporary endeavor that follows a project lifecycle, resulting in, at completion, a transition into an operational state or delivery of outputs. Project management focuses on the extent to which a specific initiative establishes, maintains and achieves its intended objectives within cost, schedule, technical and performance baselines. Project management and the PMM differ from but support software development methods, which apply to projects that intend to build and/or integrate software into the environment. As software development patterns and methods evolve, the PMM will align with and provide appropriate integration points with the development lifecycles approved by the agency.

2. PMM describes the appropriate project methods, activities, and processes required across the IT/IM project lifecycle. The subscribed tasks and the production of artifacts throughout the PMM phases are designed to—

   (a) Promote efficient and effective project planning and execution.

   (b) Provide appropriate integration points to Federal regulations, guidance for cybersecurity, records and information management (RIM), and other related functions.

3. Information associated with the related processes, including the required activities and artifacts for each phase of the PMM lifecycle are identified in the associated PMM 2.0 toolset, accessible through the PMM Web site (http://www.internal.nrc.gov/pmm). The toolset guides Project Managers through the related processes and provides appropriate links and references to standards and templates for required documentation related to project management, cybersecurity, and the records and information management.

III. GLOSSARY

Artifact

A work product or deliverable that is produced as a result of executing an activity.

Authorizations and continuous monitoring

Information systems must have an Authority to Operate (ATO) issued by the NRC Designated Approving Authority (DAA) in order to operate in the production environment. Authorizations may be periodic or on-going, based on implementation of a Continuous Monitoring plan. Re–authorization upon significant changes may also be required. In some cases an Authority to Use (ATU) for applications hosted outside of the NRC domain or in a federally approved cloud may be issued. IT/IM System Authorization and Continuous Monitoring processes are identified and described on the Office of the Chief Information Officer's Information Security Directorate (ISD) Web page (http://www.internal.nrc.gov/CSO/).

Information Technology/Information Management (IT/IM)

The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.

The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its lifecycle.

IT investment management

Groups of activities and acquisitions that focus on achieving an interrelated set of organizational goals and objectives in support of NRC's mission and in accordance with the direction set by NRC's target architecture. Key activities at this level include the identification, sponsorship, preparation, planning, and selection of IT/IM investments within the context of the NRC transition strategy, development of investment business cases, update and maintenance of IT/IM investment documentation, and the monitoring of investment performance.

IT/IM project

A temporary endeavor with a beginning and an end in support of achieving a goal or delivering a specific outcome on an IT/IM investment. Projects may be of various types, including new development or enhancements of information systems, infrastructure, operations or maintenance, service delivery, and organizational strengthening.

Internal use software

Software used to meet a Federal agency's internal or operational needs. It includes software for mission-related, financial, and administrative systems (including those used for project management).

IT/IM portfolio

The NRC portfolio is the enterprisewide view of the history and future of NRC IT/IM investments. Key IT/IM governance activities at this level are environmental scanning for new industry and Federal Government developments, continuous technical and program focused portfolio analysis, the development of transition strategies to move NRC from the current state to the target state, and the compilation and submission of the NRC IT/IM budget.

IT Capital Planning and Investment Control (CPIC)

A management process that overlays the lifecycle of every IT/IM investment. The CPIC process, which is mandated by the Clinger/Cohen Act of 1996, provides the Chief Information Officer (CIO) with the technical and business value analyses necessary for selecting and monitoring the performance of the agency's IT investments. The NRC's CPIC process also provides information to the NRC's Information Technology/Information Management Portfolio Executive Council (IPEC), which prioritizes investments in the IT portfolio.

Lifecycle cost

The total cost of implementation and ownership of a system over its useful life. Lifecycle cost includes the cost of development, acquisition, operation, maintenance, support, cybersecurity and where applicable, decommissioning.

Major IT investment

OMB defines a major IT investment as an IT investment requiring special management attention based on one or more of the following:

- Importance to the mission or function of the Government;
- Significant program or policy implications;
- High executive visibility;
- High development, operating, or maintenance costs[1];
- Use of an atypical funding mechanism;
- Financial systems with annual cost/spending of $500,000 or more, as dictated by mandates and guidance for financial systems, e.g., OMB Circular A-127; and
- Definition as major by the agency’s capital planning and investment control process.

[1] The cost threshold for “high costs” is planning year costs of ≥ 10% of the agency IT budget (for FY 2015, this equates to ≥ $15,000,000).

Non-major IT Investment

An IT investment that does not meet the criteria defined above for a major IT investment.

Information lifecycle management

The management of information as it is created, captured in some form, stored and ultimately destroyed or preserved indefinitely. In Federal agencies, much of the information should be identified as a Federal record; because it documents Government activities or because of the value of the data it contains. Information that is identified as a Federal record is usually placed under records management control, which follows a similar lifecycle: it is identified as a record, captured as a record, stored as a record, and either destroyed or preserved (see NARA policy).

Information system lifecycle

The term “information system lifecycle” means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

Records and information management (RIM) certification

The NRC’s official process for comprehensively evaluating the technical and nontechnical electronic records management features of NRC information systems and determining whether they satisfy applicable electronic recordkeeping criteria.

The RIM Certification process also provides standardized methods for evaluating a system for recordkeeping compliance and recognizes manual and automated approaches to achieving this compliance.

Exhibit 1 Strategic Planning and Enterprise Architecture

A. SP/EA INTRODUCTION

As a major component of the agency's Integrated Information Technology/Information Management (IT/IM) Governance Framework, the Strategic Planning and Enterprise Architecture (SP/EA) Program supports all IT investments at the NRC.

This exhibit describes the NRC's SP/EA Program in compliance with the policies established in Management Directive (MD) 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework." It describes and references different phases of the EA lifecycle. This exhibit also introduces and establishes SP/EA terminology and definitions, providing a common basis for SP/EA contribution to the understanding and communication of all users of the IT/IM investment framework.

Staff should review this exhibit for the applicable policies and processes as well as the references to guidance, templates, tools, and other support materials for the investment of IT systems and applications at the NRC. The details regarding the SP/EA process may be found on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx.

Background

The NRC is subject to several legislative mandates regarding its management of IT investments. In response to these mandates, the Office of Management and Budget (OMB) has issued specific guidance for the establishment of an agency enterprise architecture program and has defined the requirements for alignment of the enterprise architecture program and planning artifacts with all other levels of agency strategic planning. The current versions of the guidance documents may be found on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx. The agency's SP/EA Program recognizes and reinforces that IT should not be the driver for business capability changes; rather, the driver is the organization's desire to improve its business capability and, as appropriate, to use technology to accomplish desired improvements. Offices responsible for executing business processes and achieving desired business outcomes are the owners of business processes. A key element of the SP/EA Program is to document these business processes and, to the extent possible, understand their current performance in terms of operational metrics.

Applicability

The policies, outlined processes, and guidance provided in this exhibit and the associated SP/EA site content are applicable to all IT investments at the NRC, including all headquarters and regional offices. The policies, outlined processes, and guidance also apply regardless of the IT investment type, including new system development, enhancements to an existing system or application, operations and maintenance, or replacement or retirement of IT systems or

applications. Staff must follow and apply the processes and activities described in this exhibit and the associated SP/EA site as required.

The applicability of each step-by-step process, outlined activities, and required artifacts are contingent upon the size, characteristic, and complexity of each specific investment.

Objectives

The following objectives apply to the NRC's Strategic Planning and Enterprise Architecture Program:

I. Provide reference information to support compliance with Federal Enterprise Architecture (FEA) guidance and collaborative EA planning methodology (CPM)—as adapted to NRC needs—and to be fully integrated into the lifecycle of all IT investments.
II. Provide reference information to ensure cybersecurity requirements are fully integrated into the lifecycle of IT investments in conformance with agency cybersecurity policy, available at http://www.internal.nrc.gov/CSO/.
III. Encourage the collaborative partnership between NRC offices and the Office of the Chief Information Officer (OCIO) to initiate, develop, and manage IT investments that provide the best available support to the mission of the agency.
IV. Provide guidance on aligning IT/IM activities with the NRC agencywide Strategic Plan.
V. Promote overarching architectural principles and standards to optimize the agency's return on IT investments.

Detailed information related to IT investments, portfolio management, and SP/EA implementation may be found on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx.

SP/EA Scope

SP/EA Scope begins with the expression of an identified business need or mission-related initiative, the evaluation and approval of a potential investment through the pre-selection phase, comprehensive project planning through the post-selection phase, the project execution phase, the transition phase of the investment into the NRC production operating environment, and through its entire operational life.

B. SP/EA OVERVIEW

This section provides an introduction to the SP/EA components and includes descriptions of how the process is designed to work and interact with other supporting resources to assist users in implementing the process.

Enterprise Architecture

At the core of SP/EA is the NRC Enterprise Architecture Program. Enterprise architecture is the discipline of translating business vision and strategy into effective enterprise change by creating, communicating, and improving the key requirements, principles, and models that describe the enterprise's future state and enable its evolution and transformation from its current state. This transformation process entails the analysis and design of an enterprise in its current and future states from a strategic, organizational, and technological perspective. The goals of EA are to improve the organizational efficiency, effectiveness, and agility by delivering business-aligned, enterprisewide IT/IM systems.

Fundamental to successful enterprise architecture is finding better, more effective ways to analyze, design, and implement solutions that support the business capabilities of the organization. In addition, EA provides an analysis and planning discipline to help ensure that enterprise systems have the agility needed to align with and support changes in business strategy and underlying business capabilities. OMB provides Federal enterprise architecture guidance as the minimum set of EA program requirements for Government agencies. The NRC conforms with the intent of FEA guidance while optimizing that guidance to be more relevant to the agency's needs. Additional information is available on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx.

The EA program maintains a current repository of EA information that is essential for effective IT planning, including business functions, applications, technologies in use, interfaces between IT systems, standards, and sponsoring organizations. Management and staff can apply this EA information to make informed investment planning decisions and identify opportunities for sharing data, applications, and technologies.

The EA process is an essential tool for taking a strategic approach to planning and managing agency IT/IM resources and maximizing the use of IT funding. The EA process—

- Helps ensure the alignment of IT with NRC's Strategic Plan and the NRC IT/IM Strategic Plan so that business needs drive technology decisions.
- Identifies and minimizes redundancies and thus yields potential cost savings.
- Highlights opportunities for streamlining business processes, information flows, data sharing, and data retention.
- Assists in optimizing the interdependencies and interrelationships among the programs and services of the NRC's various component organizations, as well as with external agencies.

- Ensures a logical and integrated approach to adopting new technologies.
- Promotes adherence to agencywide technology standards, interface standards, and other related standards for systems security, privacy, and Information and Records Quality Principles.
- Helps ensures any changes to applicable standards or the production architecture baseline go through the agency's formal change request (CR) process.
- Pinpoints and resolves issues of data governance such as availability, utility, quality, and access.
- Helps to prioritize IT investments.

The EA process provides the staff with the following:

- A clear understanding of the strategic requirements of the enterprise;
- Models representing the current state of the enterprise in terms that assist decisionmaking;
- Models of the future state in terms of goals and strategies, which illustrate what the enterprise should look like across all EA viewpoints in support of the business strategy;
- A roadmap of the change initiatives required to reach the future state; and
- Requirements, principles, standards, and guidelines that will steer the implementation of change initiatives.

EA is an important transformational resource for any organization, large or small, providing the enterprisewide view needed to effectively develop and utilize systems and technology for effectively achieving necessary business outcomes.

Strategic IT/IM Planning Processes

The agency maintains three levels of planning associated with the NRC's IT/IM investment framework. The first-level and primary driver is the NRC's Strategic Plan, which establishes the goals and strategies for mission execution. Second, the IT/IM Strategic Plan consolidates and adapts the agency's strategic plan to IT/IM resources. OMB frequently refers to this level of planning as the Information Resources Management (IRM) Strategic Plan. Third, the Enterprise Roadmap (ERM) defines the activities for meeting the goals and strategies elaborated in the IRM plan. (The current ERM is available at http://fusion.nrc.gov/functions/team/itroadmap/20152019%20Enterprise%20Roadmap%20Draft/ITIM%20FY2015-2019%20Roadmap_v9Final.pdf.) The ERM documents the current and future states of the enterprise architecture and provides a transition plan showing the sequence of planned actions needed to achieve the future desired state during the planning horizon. The ERM refers to planned activities in terms of their relationship to NRC's required business capabilities.

The NRC's business capabilities represent business processes along with the people, tools, and information needed to deliver certain assigned and expected outcomes. For the NRC, these expected outcomes are largely defined by the Atomic Energy Act of 1954, as amended, and

Title 10 of the *Code of Federal Regulations* (all parts). These outcomes are met by the mission areas executing business processes that directly deliver these outcomes. NRC has developed a business capability map with a supporting business capability model behind it. A detailed description of business capabilities and the NRC Business Capability Map and Model may be found on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx.

Additionally, the ERM maintains a direct linkage to the current and future plans for major IT business solutions as listed in the OMB major IT business case and agency IT portfolio summary, which comprise the agency's IT portfolio. To that end, the ERM goals and strategies represent the foundation for the annual budget formulation process.

SP/EA Components

Core Elements

The three core elements of the SP/EA are its roles, artifacts, and activities. The backbone of any enterprise architecture program is the description of who (roles) does what (artifacts) and how (activities) to do it. The notion of when (phases) is a central supplement to help plan and execute a project. Details concerning the roles, artifacts, and activities are discussed within each of the phases on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx. The three core elements, as well as the activity groups, are briefly described below.

SP/EA Roles

A role defines a set of responsibilities in terms of activities that one or more people can perform. A role may be performed by an individual or a set of individuals working together as a team. An individual may also assume multiple roles. Roles are not necessarily related to a person's current job position or to any current organizational role. A role is related to the project and the function (role) an individual is requested to play in the investment's evolution. An individual can play one or more roles, depending on the size and complexity of the effort.

The most significant roles for SP/EA are described briefly below. For the most current list of roles and the responsibilities associated with them, refer to the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx.

Management Roles

Enterprise Architect (EA). The Enterprise Architect is responsible for defining architectural solutions, frameworks, patterns, and reference architectures for use across multiple systems within the agency, and guiding application architects in their understanding and application of the enterprise architecture. Enterprise Architects provide recommendations for technology, data and interface standards to the Architecture Governance Board. Enterprise Architects work closely with application architects to help them formulate architectures for specific applications. They do this by helping them to apply reference architectures and to craft application architectures with enterprise needs in mind. The Enterprise Architect is responsible for

understanding the agencywide Strategic Plan and translating the goals and strategies into those IT/IM solutions can support. The Enterprise Architect is also responsible for understanding the business processes requiring automation and their relationship with other business processes and systems. The Enterprise Architect must also understand the data that will be used by the system and assist in defining system and cybersecurity requirements so that the resulting system conforms to the to-be enterprise architecture, EA standards, and is protected with the appropriate level of security and integrity.

Architecture Council (AC) Co-Chairs. The Architecture Council provides direct guidance and IT/IM-related decision recommendations to other IT/IM governance boards and the CIO. The AC process, led by the AC co-chairs, oversees recommendations submitted by EA and specifically oversees the annual update to the Enterprise Roadmap. The AC ensures that the agency's architecture and technical standards remain current. The AC also oversees the project control gate framework and monitors projects as they go through these gates to ensure that expected outcomes are achieved. As a general rule, the AC should recommend potential business process reengineering or business process improvement (BPR/BPI) efforts; look at existing agency solutions; and consider external options (e.g., E-Gov, cloud), before new system development, system or service acquisition, or system enhancements take place.BPR/BPI improvement is further described in the exhibit on PMM (see Exhibit 3 of this handbook).

Definition

SP/EA Artifacts

An artifact is a work product associated within a given subject area. The subject areas and minimum set or core EA artifacts, definitions, and templates may be found on the SP/EA site at http://fusion.nrc.gov/functions/team/EA/default.aspx. In general, the artifacts define what the agency must deliver in terms of reference models and map to Governmentwide reference models. The artifacts define the as-is state with respect to the application of IT/IM resources. Artifacts are used to factually communicate different views of the agency's architecture for decisionmaking.

Exhibit 2 IT Investment Management

A. IT INVESTMENT MANAGEMENT INTRODUCTION

This exhibit expands upon the Capital Planning and Investment Control (CPIC) components of the legacy Project Management Methodology (PMM) Web site and the CPIC User Guide, in compliance with the policies established in Management Directive (MD) 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework."

Purpose

Information technology and investment management (IT/IM) establishes the fundamental processes, capital IT management requirements, objectives, and standards necessary to implement mature IT investment management—including the planning, implementing, monitoring, and evaluating of capital IT investments—consistent with CPIC requirements and guidance. These fundamental critical processes provide an efficient and effective means for selecting, controlling, and evaluating IT investments in support of the NRC strategic priorities and IT portfolio. The select, control and evaluate processes must be continuously evaluated and refined to achieve mature IT investment management and facilitate the development of a well-balanced IT portfolio aligned with the agency's IT/IM strategic plan and "to-be" enterprise architecture that leverages IT for strategic outcomes in a cost efficient manner and acceptable level of risk.

For additional detail on specific roles, responsibilities, and processes, please refer to the IT investment management at http://fusion.nrc.gov/ois/team/itg/itinvestments/default.aspx.

Background

The Clinger-Cohen Act (CCA) of 1996 requires agencies to use a disciplined CPIC process to acquire, use, maintain, and dispose of IT. The CCA also encourages the use of performance-based and results-based management of these investments. The Federal Acquisition Streamlining Act requires that IT investments align with mission and strategic goals; have cost, schedule, and performance goals; and achieve an average of 90 percent of these goals. The Federal Information Technology Acquisition Reform Act (FITARA) enacted on December 19, 2014 builds upon the requirements set forth in the Clinger-Cohen Act by establishing the Common Baseline for IT Management, representing a set of roles and responsibilities for the agency CIO and other senior agency officials.

Consistent with CPIC processes, IT investment management enables NRC to manage these investments with more transparency, accountability, and responsibility. The frequency and level of control and evaluation applied to an investment should be consistent with the investment type to prevent excessive overhead costs that would adversely affect the return on low-cost investments. For specific investment types, refer to IT investment management at http://fusion.nrc.gov/ois/team/itg/itinvestments/default.aspx.

The IT investment management process comprises all of the elements of the traditional CPIC process, as well as activities focused on the development of NRC's IT budget. Through this process, IT investments are selected and subsequently continually re-selected, monitored, and evaluated until their end-of-life (EOL) to ensure each investment in the portfolio is well-managed, cost-effective, performing as expected, and supports the mission and strategic goals of the organization. By integrating with the other components of the Integrated IT/IM Governance Framework — IT governance boards, enterprise architecture, IT strategic planning, project management, among others — the IT investment management process helps ensure that the required disciplines of IT management drive the alignment of NRC's IT investments with the NRC mission and enterprise architecture.

NRC's IT Portfolio Structure

Structure

NRC formulates, evaluates, and executes the agency's IT budget at the activity level to facilitate transparency for IT costs, support prioritization of IT for inclusion in the IT portfolio, improve the IT budget formulation process, and link the IT budget to actual IT expenditures. To that end, NRC structured its IT portfolio as follows:

- **Segment** refers to a group of related IT services that support the agency's needs within a given business area. For example, the administrative services segment provides IT services to support the agency's administrative functions, including facilities and personnel security, facilities management, and space and property management.

- **Investment/Service** refers to the expenditure of IT resources to enable core functions and processes that support the agency's mission and operational business requirements. An IT investment may include one or more project(s) for the development, modernization, enhancement, or maintenance of a single IT component or group of IT components with related functionality, and the subsequent operation of the component(s) in a production environment. All investments should have a defined life cycle with start and end dates. The end date should represent the end of the currently estimated useful life of the investment as based on (1a) the most current alternative analyses of the components or (1b) the results of the most current operational analysis summarizing the operational performance of its components and (2) the investment's ability to deliver required functionality.

  [Note: Each Investment/Service is assigned a Unique Investment Identifier (UII) for tracking, budgeting, and reporting purposes, both internally and externally to OMB.]

- **Component** refers to an IT system, module, or application; IT network or computing device; physical or virtual computing platform; other IT asset; and/or personnel needed to deliver or support a given IT service. The NRC's goal is to invest in single enterprise solutions to provide a given service to meet common business needs across the agency. Where this is not possible, multiple related components would be associated with the given parent investment/service.

  [Note: Each Component is assigned a Component Identifier (CI) for internal tracking, budgeting, and reporting purposes.]

- **Activity** refers to expenses, projects, tasks, processes, and other undertakings that constitute the costs and resources associated with a given component. Activities are further classified as supporting Operations and Maintenance (O&M) or Development, Modernization, and Enhancement (DME).

Scope

This policy applies to all NRC IT investments, including pilot and prototyping activities throughout the entire investment lifecycle, regardless of the source of funding, whether owned and operated by NRC, or operated on behalf of NRC. In accordance with OMB guidance on management and oversight of Federal Information Technology, implementation will not impact the independence of the Office of the General Counsel (OIG) and authorities the Inspector General has over the personnel, performance, procurement, and budget of the OIG.

Objectives

The following objectives apply to the management of IT assets at the NRC:

I. NRC will select IT activities that support new or existing IT investments (or services) that support the agency mission and align with the agency's IT architecture through the NRC Enterprise Roadmap.
II. NRC will manage all IT investments and associated activities with the goals of balancing risks and maximizing returns
III. NRC will evaluate the performance of all IT investments and associated IT components in accordance with applicable laws and mandates
IV. NRC will not fund IT investments and associated activities unless approved in accordance with IT governance structures and associated processes as outlined in MD 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework."
V. The "as-is" and "to-be" business processes to be supported by an IT investment shall be documented before funding is provided to support that investment.
VI. NRC offices and regional representatives will work through the approval process to gain funding for any IT investment or associated activities they deem essential to the accomplishment of their missions and strategies.

VII. NRC offices and regional representatives will follow the agency's IT acquisition policy and processes utilizing approved acquisition strategies and plans in all procurement actions. Deviations will require CIO approval.

VIII. NRC offices will adhere to the IT investment management processes throughout the lifecycle of all IT investments and associated IT components under their purview.

IX. Project sponsors will ensure that requests for IT resources are based on quantitative and qualitative measures of the business value that is expected to be achieved from the investment and will include evaluation criteria that can be used in measuring the achievement of that value.

These objectives are part of the set of integrated policies defined by NRC's Integrated IT/IM Governance Framework and are based on the Office of Management and Budget (OMB) and Government Accountability Office (GAO) guidance.

Additional references to Federal policy regarding IT investment management can be found in the latest Capital Planning and Investment Control (CPIC) Guidance issued from OMB. Refer to this guidance can be found at the IT investment management site at http://fusion.nrc.gov/ois/team/itg/itinvestments/default.aspx.

B. IT INVESTMENT MANAGEMENT OVERVIEW

The NRC IT investment management component of the Integrated IT/IM Governance Framework consists of a multilayered structure that comprises policy, processes, procedures, standards, and guidelines, with each layer providing an increasing level of detail. The IT investment management process follows the continuous sequence of selecting, monitoring and controlling, and evaluating the investment and associated activities throughout its lifecycle, as depicted in Figure 1.

Figure 1. Overview of the IT Investment Management Process

Select Process: Selecting NRC's IT Investments

The primary activities within this process include the following:

- Evaluate each IT investment request to determine alignment with mission needs.
- Demonstrate an expected return on investment for new requests to be assessed against other IT business needs.
- Prepare cost-benefit and alternatives analyses, to include cybersecurity requirements and current Federal IT/IM mandates (e.g., accessibility, HSPD-12, IPv6) for each new investment request.
- Prioritize IT investments to ensure continued alignment of agency resources to mission needs.
- Facilitate funding decisions for new and existing investments.
- Facilitate the approval of the annual IT budget request.
- Prepare and maintain a portfolio of IT investments.
- Determine system data with "Record" status and approach to records and information management (RIM) requirements (initial verification of RIM).

Control Process: Monitoring and Controlling NRC's IT Investments

The primary activities within this process include the following:

- Institute performance measures and management processes to track actual performance including cybersecurity continuous monitoring.
- Establish tracking mechanisms that enable periodic reporting and review of investments.
- Establish key performance indicators to highlight areas requiring further review, including compliance with cybersecurity requirements under the established continuous monitoring program.
- Monitor project progress to highlight deviations from project expectations and to illustrate project accomplishments.
- Initiate and monitor corrective actions as needed.

Evaluate Process: Evaluating NRC Investments

The primary activities within this process include the following:

- Conduct post-implementation reviews (PIRs) of IT systems to evaluate project results and document lessons learned.
- Evaluate investments to monitor return on investment and to support decisionmaking toward the continuation, modification, or cancellation of an investment.
- Re-assess each IT investment's compliance with key IT investment requirements.
- Provide periodic updates of investment status to executive management.
- Provide periodic reports to the Office of Management and Budget (OMB).

- Initiate and monitor corrective actions as needed.
- Conduct post-certification activities for RIM certification.

For further detail regarding each of the processes, refer to the IT investment management site at http://fusion.nrc.gov/ois/team/itg/itinvestments/default.aspx.

C. Capital Planning and Investment Control (CPIC) Team

In support of the NRC's IT investment management functions, the agency's CPIC team:

1. Facilitates IT SME reviews for policy compliance, security, IT project management, and infrastructure impact, and consolidates the SME recommendations for executive-level and management-level IT investment review boards.
2. Facilitates IT investment reviews (e.g., control reviews, TechStats, CIO TouchPoints) with the CIO and appropriate IT governance boards.
3. Coordinates with the NRC's enterprise architecture (EA) to verify mapping between the NRC's EA and the Federal EA and to ensure that investments align with the NRC's strategic plan, IT/IM strategic plan, and enterprise roadmap.
4. Coordinates with NRC's Project Management Branch, OCIO, to establish project control gates and to ensure project management standards and best practices are implemented throughout the IT investment lifecycle.
5. Coordinates with other functional areas of OCIO, including the Information Security Directorate (ISD), on security-related requirements to support the development and review of IT business cases and project plans and the monitoring and evaluation of IT investments throughout their lifecycle.
6. Assists IT investment owners in their understanding and compliance with the CPIC process and related OMB requirements, including preparation of the NRC's IT portfolio summary and major IT business case submissions.
7. Works with IPTs and IT project managers for each major investment to update major IT business cases and ensure complete and timely submission of updates to OMB
8. Serves as a single point-of-contact for NRC inquiries regarding IT governance and CPIC processes and procedures.
9. Coordinates input to the annual IT planning and budgeting guidance.
10. Maintains an inventory of the agency's capitalized IT investments (i.e., major IT business cases) and provides the current list to the OCFO for inclusion in the NRC's budget justification materials.
11. Provides input to educational outreach activities and training related to CCA, FITARA, and OMB requirements and present training related to CPIC's portfolio and investment management and submission tool, OMB reporting requirements, and the NRC's IT governance to IPTs and all project managers.

12. Sets requirements and criteria for the selection of IT investments comprising the NRC's IT portfolio.
13. Defines and implement processes and procedures to monitor and evaluate IT investments throughout their lifecycle.
14. Provides a secretariat function for the executive- level and management-level IT investment review boards, including scheduling meetings, developing agendas, coordinating briefings and reviews, taking minutes documenting decisions and action items, and tracking action items to completion.

Exhibit 3 Project Management Methodology

A. PMM INTRODUCTION

As a major component of this management directive, the NRC Project Management Methodology (PMM) describes the processes and method by which IT/IM projects must be managed at the NRC. This exhibit defines the overarching framework and processes for initiating, executing and closing IT/IM projects in full compliance with the requirements and policies established by the Federal Government and referenced in Management Directive (MD) 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework." Additionally, the framework and methodologies described in the PMM handbook, PMM Web site and its associated interactive toolset, PMM 2.0, are designed to guide and assist project managers to effectively manage their projects during the project lifecycle.

Background

The NRC, along with all Federal agencies, is subject to several legislative mandates regarding its management of IT investments. In response to these mandates, the Office of Management and Budget (OMB) has issued policies for each agency to implement. These policies are summarized and referenced in OMB Circular A-130, "Management of Federal Information Resources."

OMB Circular A-130 defines the "Information System Life Cycle" as the phases which an information system passes through, typically characterized as initiation, development, operation and termination, and NIST SP 800-64, "Security Considerations in the System Development Life Cycle" defines the System Development Life Cycle (SDLC) as including five phases: initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal.. Historically, NRC's PMM attempted to encompass all aspects of the SDLC. It was primarily used within the agency as the mechanism for complying with OMB Circular A-130 and other Federal requirements as well as mandates intended to ensure that required project artifacts are produced.

As information technology approaches and methods evolve, a number of new more adaptable and effective models in IT/IM project management have emerged, including agile and modular development methods, as well as cloud-based service provisioning and deployment. These new approaches dictated a fundamental shift in IT/IM project management—away from large-scale integration efforts supported by substantial up-front documentation towards leaner, faster models that rely heavily on iterative development.

To help ensure that the PMM remains useful as a resource for the agency's project managers (PMs), the interactive PMM toolset, referred to herein as PMM 2.0, was developed to provide more detailed and dynamic step-by-step process guidance and assistance with access to appropriate tools, methods, and templates for effectively managing an IT/IM project's cost, schedule, quality and risks and to ensure IT/IM systems development and integration activities are in compliance with the agency's cybersecurity and RIM requirements.

Applicability

The described processes and guidance provided in this exhibit and the PMM Web site are applicable to all IT/IM projects at the NRC. The PMM outlines the overarching methodology for IT/IM project management regardless of the project type—new development, enhancement to an existing system or application, or replacement/retirement of IT systems or applications. However, specific activities and required documentation and reporting vary depending on the size, characteristics, and complexity of the projects or the type of solution being implemented.

Objectives

The PMM is intended to accomplish a number of objectives, Including:

I. Ensuring that all IT/IM projects are managed, monitored and recorded in compliances with the applicable policies, standards and processes established by MD 2.8.

II. Providing NRC Project Managers with a general reference source for compliance with the applicable Federal and NRC policies and regulations.

III. Providing NRC Project Managers access to the required artifact templates and tools for managing their project resources while executing, monitoring, and recording their projects activities during their lifecycle.

IV. Ensuring that the NRC work processes are evaluated against best practices and are simplified, improved, or redesigned, when appropriate, before making significant investments in applications or systems to automate those processes.

V. Ensuring that requirements, which include records, cybersecurity, and privacy, are addressed from the early stages of the project lifecycle through project completion.

PMM Scope

The PMM's scope encompasses the project lifecycle, starting from the expression of an identified business need or initiative; its evaluation and approval as an IT/IM project; comprehensive post-selection project planning; project execution and control; and finally transition of the system or application into its production environment or achievement of the goal or deliverables that would mark the end of the project.

PMM OVERVIEW

The PMM is structured on the basis of the following:

- Method Principles
- Lifecycle Processes
- Project Roles
- Project Artifacts
- Related Project Support Functions

In the following sections each of these dimensions is described in more detail.

Method Principles

The PMM was designed to focus on a number of project management principles that must be applied by all project managers in order to ensure successful project outcomes. These project management principles as summarized below are applicable at across the entire IT/IM project lifecycle and should be considered in every project activity.

Principle	Summary
Realize Expected ***Benefits***	The extent to which expected benefits to stakeholders are well defined; whether the implementation is proceeding consistent with expected delivery of benefits; and, as applicable, whether the value is sustained during operation.
Manage ***Risks*** *Effectively*	The extent to which business, technical, and cybersecurity risks, along with their potential impacts to the organization, its operations, industry, and others are identified and managed across the project lifecycle.
Manage ***Costs*** *Effectively*	The extent to which cost estimates are reasonable and complete; whether sources of funding and acquisition are considered; and whether spending is tracked against plan across the project lifecycle.
Manage ***Resources*** *Effectively*	The extent to which leadership is engaged; management and technical skills are identified; and whether those skills are obtained and applied across the project lifecycle.
Manage ***Quality*** *Effectively*	The extent to which the components of quality are defined; whether the components are used to shape the nature of the investment; and whether they are tracked across the project lifecycle.
Leverage Opportunities for ***Efficiency***	The extent to which opportunities to leverage existing capacity, capability, and standards are evaluated and whether they are leveraged during implementation and operation.

Lifecycle Processes

The PMM is organized into four distinct project lifecycle phases as following:

- Pre-Selection Planning
- Post-Selection Planning
- Execution and Control
- Transition

These phases, although higher level than previous iterations of the agency's PMM, are designed to encompass a broader range of IT project types inclusive of not only software integration or development efforts but also hardware, BPI, and other service only efforts which comprise a substantial component of the agency's IT/IM project portfolio. Additionally, the PMM focuses on the 'project' functions of IT planning and delivery rather than the complete systems lifecycle. Thus, the PMM lifecycle is structured to better support different project types and project-specific activities from a framework perspective.

The framework remains the same, but the processes within the phases, particularly in execution space, may be different based on what is being developed and the development methodology (e.g., agile, infrastructure based, traditional approach). For instance, agile is an iterative approach to software delivery that builds software incrementally; while the phases remain the same, the method and steps within the Execution and Control Phase will be will tailored to an agile approach.

The following table summarizes the scope of each phase of the PMM.

Pre-Selection Planning Phase
The pre-selection phase is a critical first step in the agency's project management processes. The purpose of the activities and artifacts required in this phase is to establish the business need for the project, and complete the applicable governance review and approval processes necessary to proceed. The PM must understand the basic solution design, as well as the general costs, benefits and risks including cybersecurity and RIM requirements associated with the project. The requirements for completion of this phase will vary based on the size and nature of the project. For example, a major IT/IM project possesses more requirements and governance oversight related to its pre-selection activities than a minor IT/IM project. This phase may serve as the project initiation from a development perspective and move a project from an idea or notional concept to a formal 'development, modernization and enhancement' (DME) state.
Post-Selection Planning Phase
Post-selection planning is the phase in which comprehensive project execution planning is laid out and therefore requires a structured approach resulting in concise and detailed plans for the project. Documents produced during the Post-Selection phase are living documents and may require refinement as additional details emerge during the project execution and control phase. The amount of rigor employed during this phase is contingent on the size and complexity of the project. The quality of the effort taken during the Post-Selection Planning phase is often indicative of the project's ability to reach a successful conclusion.

Execution and Control Phase
The Execution and Control Phase consists of processes performed to complete the work defined in the Project Schedule and other project plans to satisfy the project specifications. This involves coordinating people and resources, managing stakeholder expectations as well as integrating and performing the activities of the project. This phase includes the development of detailed technical specifications as well as the full execution of the design from planning through development, testing, and implementation. It also includes the building and testing of all functions iteratively on a proven architecture.
Transition Phase
The transition phase prepares and finalizes an IT/IM project's introduction to the users for official use. For software development projects this may include migration from a development environment to its production environment. For a cloud or Software As A Service (SAAS) effort this may include ensuring all required agreements with the service providers are established. Regardless of the type of project, it is vital that, as IT/IM projects prepare to deliver business capabilities. Project managers should ensure that the solution is secure and robust with an established, cybersecurity, continuous-monitoring program, and that communications and training materials are in place to ensure the project is successfully introduced into the production environment. This phase may also serve as the project closeout, transitioning an IT solution into an "operations and maintenance" (O&M) state.

Complementary to this handbook and the NRC PMM Web site, the Project Management toolset known as PMM 2.0 (accessible through the PMM Web site) provides interactive and step-by-step guidance to follow agency project processes as well as access to references and linkages to standards and required documentation templates tailored to the type, complexity and size of each project.

Project Roles

A **role** defines a set of responsibilities in terms of activities that one or more people may perform. A role may be performed by an individual or a set of individuals working together as a team, referred to as an Integrated Project Team (IPT). An individual may also assume multiple roles. Project roles are **not** necessarily related to a person's current job position or to any current organizational role, a common misperception. A project role is related to the project and the function (role) an individual is requested to play in that specific project's evolution. An individual can play one or more roles, depending on the size and complexity of the project. This documentation is specific to Project roles and responsibilities; however, some of these roles

also have System responsibilities and are expected to fulfill system-specific responsibilities as appropriate (e.g., system role-based security training, continuous monitoring, and oversight).

The most significant roles for PMM are described in the following table. For the most current list of roles and the responsibilities associated with them, refer to the PMM Web site, at http://www.internal.nrc.gov/pmm.

Role	Summary
Management Roles	
Business Process Sponsor/System Owner	The Business Process Sponsor or System Owner is the primary stakeholder establishing and validating business needs and system requirements as well as managing expenditures for the system development and operation. The System Owner maintains overall responsibility for the security of his or her IT system including its continuous cybersecurity monitoring. The system owner is an agency official who has inherent U.S. Government authority and must be a Government employee.
IT/IM Program Manager	The Program Manager (PgM) fulfills a formal oversight role related to a defined group of individual projects. The PgM is responsible for ensuring the group of projects are managed in a coordinated way to obtain the desired control and expected benefits not available from managing them individually.
IT/IM Project Manager	The IT/IM project manager (PM) is responsible for planning, managing business case development, and project execution and control of the overall project. The PM may be supported by others playing a project management role, depending on the size and complexity of the project.
Role	**Summary**
Business and Technical Roles	
IT/IM System Architect	The IT/IM System Architect is responsible for the software and hardware architecture. The architect also makes key technical decisions that constrain the overall design and implementation for the project. The architect is also responsible for understanding the business processes that will be automated and their relationship with other business processes and systems. The architect should also understand the data that will be used by the system and design the system so that it is protected to the appropriate level of security and integrity.
Business Analyst	The Business Analyst is primarily involved in eliciting and investigating requirements. The analyst coordinates and documents needs, requirements, and translates business requirements into software requirements using descriptions and graphical representations.

Role	Summary
Business and Technical Roles	
Information and Records Management Specialist	As a member of the IPT, the Information and Records Management (IRM) Specialist is responsible for compliance with the agency's IRM policies (MD 3.53) and meeting all NARA's requirements related to NRC's information and recordkeeping assets.
Configuration Manager	The Configuration Manager is responsible for providing the overall configuration management infrastructure and environment to the development team. The configuration manager creates software releases.
Contract Officer	The Contracting Officer approves acquisition planning and maintains overall responsibility for ensuring that all aspects of contract and task administration are accurate and complete, including insertion of security clauses in solicitations, contracts and agreements, as applicable.
Contracting Officer's Representative	The Contracting Office's Representative (COR) receives and reviews the request for approval for Invoices or Intra-governmental Payment and Collection System (IPACS) statements associated with contracts or agreements for which they are the designated COR.
Developer	The Developer is primarily involved in designing, implementing, or configuring software.
Enterprise Architect	The Enterprise Architect is responsible for defining architectural solutions, frameworks, patterns, and reference architectures for use across multiple systems within the agency, and guiding application architects in their understanding and application of the enterprise architecture. Enterprise Architects work closely with IT/IM System Architects to help them formulate architectures for specific applications. They do this by helping apply reference architectures and to craft application architectures with enterprise needs in mind.
Process Engineer	The Process Engineer tailors the project processes. The Process Engineer also educates and mentors project team members on process-related issues; ensures that valuable project experience is identified and used to improve the process; and leads or supports the frequent status meetings used by the project team to track and manage the development activities.

Role	Summary
Business and Technical Roles	
Information System Security Officer	The Information System Security Officer (ISSO) reviews the results of cybersecurity activities and determines if the system(s) affected by the activities are adequately protected. The system-level ISSO is the designated security representative of an IT system owner. This is a trusted position with special access to and authority over an IT system. This role must not be assigned to an individual who has other trusted responsibilities
System Administrator	The System Administrator maintains the development and test environments, including hardware and software, backups, and other system administration duties. The System Administrator also maintains system related networks and hardware and ensures the underlying security and data infrastructure is stable. When necessary, the System Administrator troubleshoots problems with capacity and upgrades, and assists in testing and applying fixes.
Tester	The Tester manages the system testing processes, including creation of test plans, test cases, and test scripts. The tester also executes tests and analyzes test results.
Tool Specialist	The Tool Specialist installs and configures software development tools to support the development and test environments.

Project Artifacts

An artifact is a work product of a project. A given artifact may serve as both input and output from a set of activities. Artifacts within the PMM typically possess associated guidelines and templates that present information related to developing, evaluating, and using the artifact. Many artifacts are expected to capture the evolving information and detail associated with the project across its lifecycle. A list of the current PMM artifacts, their definitions, and associated templates are available on the PMM Web site, at http://www.internal.nrc.gov/pmm.

Related Supporting Functions

Successful project delivery and compliance rely on a number of supporting functions including:

- Business Process Improvement
- System Security
- Records and Information Management
- Configuration Management
- Operational Support

As important elements in virtually all projects, these functions are summarized in the following sections.

Business Process Improvement

Business process improvement (BPI) involves a change in the way an organization conducts its business. Business process re-engineering (BPR) is the redesign of the organization, culture, and/or business processes using technology as an enabler to achieve material improvements in cost, time, service, and quality. Typically, BPR involves a material redesign of the business processes and/or the organization, whereas BPI focuses on smaller incremental changes. Depending on the scope of the project, either or both may be required as part of the project lifecycle.

Business modeling is an equivalent discipline and terminology used in the PMM, and includes aspects of both BPI and BPR. Business modeling develops a vision of the target organization and, on the basis of this, defines the processes, roles, and responsibilities needed to achieve this desired state.

Technology is not the driver for business process changes; rather, the driver is the organization's desire to improve its business processes; with leadership from the Office of the Executive Director for Operations (OEDO) and potentially the use of technology to accomplish some of the desired improvements. Offices should consider BPI before requesting funding for a new project or system development effort.

A BPI is also required to ensure the agency is in compliance with OMB's A-130, consistent with the Clinger-Cohen Act. OMB A-130 requires agency investments in major information systems simplify or otherwise redesign processes to reduce costs and improve performance. Additionally, it is a sound business practice to carefully analyze and optimize business processes before performing automation projects.

OMB advocates that agencies first consider cloud-based services, commercial-off-the-shelf (COTS), or e-Government initiatives before customized solutions. This advice implies that agencies should—

- Understand their own work processes and be willing to change them.
- Understand work processes embedded in the applicable COTS/e-Government system.
- Utilize best practices embodied in the COTS product where possible rather than customize the COTS product to fit unique processes.

However, the re-use of existing and in-house approved capabilities with acceptable performance track should be considered in addition to OMB's advocated solutions.

The directives from OMB and best practices in general are clear that business processes need to be analyzed and simplified before investments are made in automation efforts. Therefore, OEDO and OIS lead the integration and the use of the BPI methodology as part of the overall PMM system lifecycle. To the extent that the investment level requires a business case (CPIC Tier 1 or Tier 2), BPI activities will be integrated into the project processes.

System Security

The Federal Government has become increasingly reliant on IT systems to support critical day-to-day mission and support operations. Risks to system and data confidentiality, integrity, and availability can impact an organization's ability to execute its mission or its business strategy. To minimize the impact associated with these risks, Federal Cybersecurity policy requires that all IT systems must obtain an Authorization to Operate (ATO) or Authorization to Use (ATU) before being placed into the operational environment; this policy also applies to applications hosted outside of the NRC domain or in a federally approved cloud. To maintain a system authorization, all systems must adhere to any specified ATO conditions and maintain a continuous monitoring program.

The NRC goal is to integrate system security processes within the PMM to help ensure systems are conceived, designed, developed, acquired, implemented, and maintained in adherence with all appropriate Federal guidance and are in compliance with the applicable laws, regulations, OMB circulars, and the agency's management directives. Cybersecurity is considered a discipline in IT project management and therefore the processes within PMM are defined to integrate security into the system development process and across the project lifecycle.

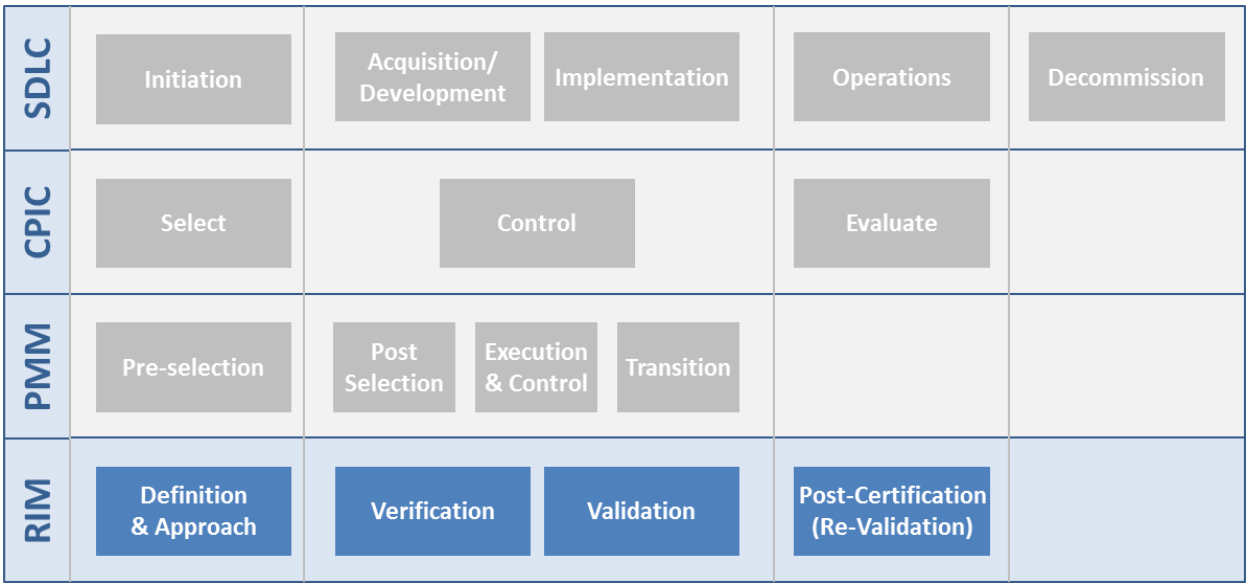
NRC MD 12.5, "NRC Cybersecurity Program," is the defining agency document regarding Cybersecurity. MD 12.5 and the related policies and processes provide system owners and project managers with the required information for satisfying the cybersecurity requirements. All templates for the required system security documentation, plans and reports are available at the ISD Web site (http://www.internal.nrc.gov/CSO) and accessible through links from the PMM 2.0 toolset.

Records and Information Management

The Presidential Memorandum issued on November 28, 2011, requires agencies to begin an Executive Branch-wide effort to reform records management policies and practices. Information which is disseminated or collected through electronic systems and meet the definition of a Federal record must therefore be maintained and managed as Federal records in accordance with the policies and procedures set forth in MD 3.53, "NRC Records and Document Management Program," as well as National Archives and Records Administration (NARA) regulations at http://www.archives.gov/about/laws/fed-agencies.html.

RIM Certification processes document the requirements that help ensure system development project activities are consistent with Federal electronic records management standards and include data and information considerations for designing and implementing electronic solutions. As part of data management, software standards, and application design, agencies incorporate certification controls for Federal information throughout a system's development cycle to reduce the risks of nonconformance of records management relative to Federal and industry best practices.

The RIM Certification Process consists of four phases: Definition, Verification, Validation, and Post Certification. The following diagram illustrates the RIM Certification process relative to CPIC, PMM, and typical SDLC phases.



For detailed information about the RIM certification process and associated activities in each of these certification phases, please refer to the Records and Information Management (RIM) Certification Process in the OCIO Customer Catalog.

Configuration Management

An important aspect of the PMM is helping ensure appropriate configuration management practices are followed for software related projects. The NRC's configuration and change request management system (CM system) holds key information about its systems development, promotion, deployment, and maintenance processes. The CM system retains the asset base of potentially reusable artifacts resulting from the execution of these processes. Only through appropriate configuration and change management can IT/IM investments be adequately protected and managed.

The CM system is an essential and integral part of the overall development processes and relates to the configuration and change control discipline in the PMM. As a result, office directors and regional administrators are required by MD 2.8 to maintain appropriate CM documentation in agency approved repositories, such as JAZZ, Remedy and ADAMS. This responsibility includes verifying that all required artifacts are available and maintained in a current state in an agency system. Additional information associated with accessing and leveraging the agency's configuration management guidelines and toolsets are available on the PMM Web site, at http://www.internal.nrc.gov/pmm.

Operational Support

Operational support, including consolidated test facility services, system deployment support, and telecommunication support are addressed in MD 2.6, "Information Technology Infrastructure." Links to the appropriate guidance and support resources are available on the PMM Web site, at http://www.internal.nrc.gov/pmm.

Exhibit 4 Integrated IT/IM Governance Roles

As illustrated below, the agency's IT/IM governance roles represent an integrated framework designed to ensure alignment of IT/IM investments with agency goals and delivery of technical capabilities in the most efficient manner possible.