Form 1221-002
(May 2022)

UNITED STATES
DEPARTMENT OF THE INTERIOR BUREAU OF LAND MANAGEMENT

HANDBOOK TRANSMITTAL SHEET

Release	1-1835
Date	04/30/2024
Office Code	HQ-500

Subject: Capital Planning and Investment Control (CPIC) Handbook Update

FOIA Designation Letter: P

1. Updates, supersedes, or rescinds:

CPIC Handbook dated 12/29/2016, Release 1-1784

2. Explanation of Materials Transmitted:

This release transmits Information Technology Investment Management policy as a new Handbook update. This Handbook provides policy direction for conducting Capital Planning and Investment Control (CPIC) activities for the Bureau of Land Management's IT investments. CPIC is the process the BLM uses for managing internal IT investment portfolios.

3. Reports Required:

None

4. Delegations of Authority Updated:

None

5. Filing Instructions: File as directed below.

REMOVE	INSERT
H-1265-1 (Rel. 1-1784)	H-1265-1 (Rel. 1-1835)
(Total: 82 Pages)	(Total: 73 Pages)

S:/ James Rolfes, Assistant Director
Division of Information Management and Technology

U.S. Department of the Interior
Bureau of Land Management

Capital Planning & Investment Control

CPIC Handbook

Table of Contents

1 Introduction

1.1 Purpose

This document describes the Bureau of Land Management's (BLM) Information Technology (IT) Capital Planning and Investment Control (CPIC) process. The CPIC process outlines a framework for managing the BLM IT investment portfolio. The CPIC process enables the BLM to address strategic needs, optimize the allocation of IT resources, and comply with applicable regulations and guidance.

CPIC is a structured, integrated approach for managing IT investments. It ensures that all IT investments align with the BLM mission and support business needs while minimizing risks and maximizing returns throughout the investment's lifecycle. It relies on a systematic process of pre-selection, selection, control, and on-going evaluation ensuring each investment's objectives support the business and mission needs of the BLM.

The Clinger-Cohen Act of 1996 requires Federal agencies to use CPIC processes and was further strengthened with the passage of the Federal IT Acquisition Reform Act (FITARA) in 2014. To assist agencies in implementing these laws the Office of Management and Budget (OMB) issues circulars A-11 and A-130 annually and provides guidance for meeting these requirements. In addition, there are numerous other legislative, bureau, and departmental policies that are related or directly impacted by CPIC.

1.2 Legislative Background & Associated Guidance

Federal agencies, by statute, are required to continually evaluate their organization and revise their operational and management practices to achieve greater mission efficiency and effectiveness. Some of the key legislation in effect includes:

Clinger-Cohen Act of 1996 (CCA)
Also known as the Information Technology Management Reform Act (ITMRA), the CCA emphasizes an integrated framework of technology aimed at efficiently performing the business of Federal agencies. Additionally, the CCA provides specific direction to agencies in the review and approval of their IT investments. It also establishes the role of Chief Information Officer (CIO) as responsible for developing, maintaining, and facilitating the implementation of an integrated IT architecture.

Chief Financial Officers Act of 1990 (CFO Act)
The CFO Act establishes a leadership structure, provides for long-range planning, requires audited financial statements, and strengthens accountability reporting. The CFO Act impacts Federal financial managers at all levels of Government.

Government Performance and Results Act of 1993 (GPRA)

The GPRA provides for the establishment of strategic planning and performance measurement in the Federal Government. The purpose of the GPRA is to improve the effectiveness and accountability of Federal programs by focusing on program results, quality, and customer satisfaction.

Federal Acquisition Streamlining Act of 1994 (FASA)
The FASA simplifies and streamlines the Federal procurement process by reducing paperwork, facilitating the acquisition of commercial products, enhancing the use of simplified procedures for small purchases, transforming the acquisition process to electronic commerce, and improving the efficiency of the laws governing the procurement of goods and services.

Paperwork Reduction Act of 1995 (PRA)
The PRA requires agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending proposals to OMB. The PRA requires agencies to seek public comment on proposed collections, certify to OMB that efforts have been made to reduce the burden of the collection, and have in place a process for independent review of information collection requests prior to submission to OMB.

Government Paperwork Elimination Act of 1998 (GPEA)
The GPEA requires Federal agencies to allow individuals or entities that deal with agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form; and it encourages the Federal Government to use a range of electronic signature alternatives.

Federal Information Security Management Act of 2002 (FISMA)
The FISMA requires that each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency.

E-Gov Act of 2002
The E-Gov Act requires all Executive Branch agencies to conduct a privacy impact assessment before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or initiating, consistent with the PRA, a new electronic collection of information in identifiable form for 10 or more persons.

Federal Information Technology Acquisition Reform Act of 2014 (FITARA)
The FITARA Act of 2014 modified the framework governing the management of IT within the Federal Government to require presidential appointment or designation of the CIO in 16 specified Federal agencies, designate the Chief Information Officers Council as the lead interagency forum for improving agency coordination of information resources investment, and require the Comptroller General to examine the effectiveness of the Council. The FITARA outlines specific requirements related to the agency CIO authority enhancements; enhanced transparency and improved risk management in IT investments; portfolio reviews; expansion of training and use of IT cadres; Federal Data Center Consolidation Initiative (FDCCI), more recently known as the Data Center Optimization Initiative (DCOI); maximizing the benefit of the Federal Strategic Sourcing Initiative; and Government-wide Software Purchasing Program.

OMB Circular A-11 Preparation, Submission, and Execution of the Budget
The Circular A-11 provides updated guidance for budget formulation annually for IT Investments. It contains instructions for Major IT Business Cases, Major IT Business Case details, and the Agency IT Portfolio Summary.

OMB Circular No. A-130 – Managing Information as a Strategic Resource
The Circular A-130 establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.

1.3 Point of Contact

Responsibility to oversee the CPIC process falls within the organizational purview of the BLM's Information Management and Technology (IMT) Directorate. For further information about this Handbook or the CPIC process, contact the Chief, Division of Investment Management (InvM).

1.4 Scope of CPIC

All BLM investments expended upon IT-based goods and services must comply with the policy mandates of this Handbook.

1.5 Roles and Responsibilities

1.5.1 Decision Making Body, Support Staff, Offices, and Personnel

The Information Technology Investment Board (ITIB) –The ITIB is responsible for building an IT investment foundation and developing and maintaining a complete IT investment portfolio. The purpose of the ITIB is to: provide governance for agency-wide information technology and management goals, strategies, and initiatives; ensure that information management programs and policies are strategically aligned to effectively advance the BLM's mission; and to lead high program performance through effective management. The ITIB also serves as the IT investment review board.

The ITIB is the decision-making board for all IT investments. The ITIB governs the full spectrum of information technology and data management programs including, but not limited to, infrastructure, data, systems, and personnel. The scope of the ITIB includes congressional and administration mandates to improve mission performance of the Federal Government, specifically through more effective strategic, financial, and acquisition management practices.

Membership to the ITIB consists of the BLM Deputy Director of Administration and Programs, Associate Chief Information Officer (ACIO), Assistant Directors (AD), State Directors (SDs), District or Field Manager, Center Directors (CD), and shall include an ex officio (non-voting) member from

the Business Management Council.[1]

The Executive Leadership Team (ELT): The ELT is a senior management forum for the discussion and resolution of major policy issues. The ELT leads the development of BLM-wide strategic objectives, personnel policies, programs, and budget priorities that support Administration, Department, and Bureau goals. It also monitors the BLM's progress toward those objectives and goals.

The Field Committee (FC): The FC is responsible for daily operations as the BLM carries out its mission. It's a senior leadership forum of operational decision makers who assure the uniform implementation of BLM operations and provide insight and advice on sensitive issues for national and state policy. The FC also serves as a nexus between field operations and the ELT.[2]

The Business Management Council (BMC): The BMC facilitates improvements and assures consistency in the operational, programmatic, and support functions of the BLM. It advises the appropriate directorate and/or the Field Committee of support functions that may impact and/or enhance implementation of the BLM mission and its strategic goals and leads and/or participates on national initiatives and committees to provide field-level input and operational feasibility.[3]

The Data and Geospatial Steering Committee (DGSC): The BLM's DGSC is responsible for providing strategic direction and oversight to the Geospatial and data programs for the BLM. The focus of the DGSC is on providing strategic direction and oversight for the ELT's vision of One GIS, setting priorities for the Geospatial and data program, and providing executive level coordination. Membership to the DGSC consists of the ADs of HQ; SDs, Director of the NOC, and the Senior Geospatial Program Manager.[4]

Rating and Ranking Committee (RRC): The role of the RRC is to review and assess the health of all BLM IT Investments, and to make recommendations for further improvement. The RRC will rate and rank the BLM IT Investments in accordance with the rating and ranking criteria established by the committee and approved by the ITIB. Membership to the RRC is determined by the ITIB.

Associate Chief Information Officer (ACIO): The ACIO is a position required by DOI's FITARA implementation plan and is the senior information management and information technology (IT) leader for the bureau. The ACIO maintains purview of the establishment and oversight of bureau IT and its alignment with objectives and expected outcomes of the Secretary, DOI CIO key priorities, and BLM mission and program objectives. BLM's ACIO is also the Assistant Director of Information Management and Technology (IMT), vice-chair of the ITIB, and a member of the ELT.

Division of Investment Management: The Investment Management Division (InvM) is responsible for planning, budgeting, acquisition, compliance, and oversight of the BLM IT capital assets. The role of the InvM is to ensure that the BLM is maximizing the value and highest use of IT funds; achieve strategic performance goals and objectives of the BLM investment portfolio at the lowest life-cycle costs and least risk; provide oversight of the BLM capital plan and business case and the IT

[1] Appendix C-1
[2] Appendix C-2
[3] Appendix C-3
[4] Appendix C-4

investment portfolio; ensure policy oversight and monitor compliance for the national acquisition of IT contractual goods and services; and support the ITIB.

States, Centers, and Directorates (S/C/D): Are responsible for reviewing, prioritizing, and approving all their S/C/D IT needs; aligning with mission objectives; and ensuring budgetary resources are sufficient to cover needs. S/C/D are also responsible for communicating this information and ensuring compliance with CPIC process objectives and all other existing IT policy.

Investment Sponsor or System Owner: The business official responsible for the strategic business processes under development or enhancement and for ensuring their integrity; also serves as the primary user interface to the CIO and the ITIB. The Investment Sponsor is responsible for funding the investment once it is approved by the ITIB. The Investment Sponsor is also responsible for ensuring that the system is evaluated annually and receives an appropriate level of funding for the Operations and Maintenance (O&M) of the system.

Program and Project Manager (PM): The trained or experienced official responsible for management and completion of one or more IT investment projects. The PM is assigned the responsibility for accomplishing a specifically designated work effort or group of closely related efforts established to achieve stated or designated objectives, defined tasks, or other units of related effort on a schedule, within cost constraints and in support of the program mission or objective. The PM is responsible for the planning, controlling, and reporting of the project, and for the management of required functions, including acquisition planning, developing the requirements, business case development, performance of the schedule, and formulation, justification, and execution of the budget. The PM is responsible for effectively managing project risks to ensure effective systems and services are delivered through a total life-cycle approach to the end user on schedule, within budget and at the required levels of performance.

An IT project manager (ITPM) must be assigned to Bureau major and non-major IT investments. To ensure compliance with all IT project management requirements and to facilitate access to IMT resources to support IT project success, all IT project management activities will be overseen by the IT Project Management Division regardless of whether the assigned ITPM is assigned from within IMT or from a different organization. To ensure compliance with certification and experience requirements all ITPMs must be approved by the IT Project Management Division Director. ITPMs will attend all status and coordination meetings as required by the IT Project Management Division. PMs assigned to Major Investments must be senior-level certified Federal Acquisition Certification for Program and Project Managers (FAC-P/PM). PMs for Part-1 Non-Major Investments must be, at a minimum, mid-level certified FAC-P/PM.[5]

Information Technology Leadership Council (ITLC): The ITLC is established within the IMT Directorate as a Cross-IT Division Review Council established by and reporting to the Associate Chief Information Officer (ACIO) and is charged with making IT management and operational decisions for the delivery of bureau-wide IT services.

[5] Appendix C-6

Enterprise Solutions Committee (ESC): The ESC provides IT Strategic Planning and Enterprise Architecture (SP/EA) oversight and support and is led by the Bureau Chief Technology Officer (CTO). The goals of the ESC are to improve organizational efficiency, effectiveness, and agility by delivering business-aligned, enterprise-wide IT solutions. The ESC reports to the ITLC and supports governance over the planning, development, deployment, and utilization of secure and sustainable enterprise-level IT solutions that meet Federal requirements and supports the BLM's mission and operational needs. This includes supporting established priorities of IT initiatives, ensuring alignment with BLM's strategic objectives, and optimizing the use of technology to enhance efficiency and effectiveness across the organization. The ESC fosters collaboration among various BLM divisions and stakeholders to identify common IT requirements, streamline processes, and enforce consistency and utilization of available IT services. Where enterprise IT solutions are not available, the ESC provides governance and direction to ensure new technology and services are supportable, sustainable and align with enterprise IT strategic architecture and vision. By doing so, it facilitates the adoption of innovative technologies and IT best practices, ultimately enabling the BLM to identify and realize the benefits of improved services and operational efficiencies.

1.5.2 Relationships

Figure 1-1 provides a summary of the relationship between the ITIB and other committees and organizations within BLM.

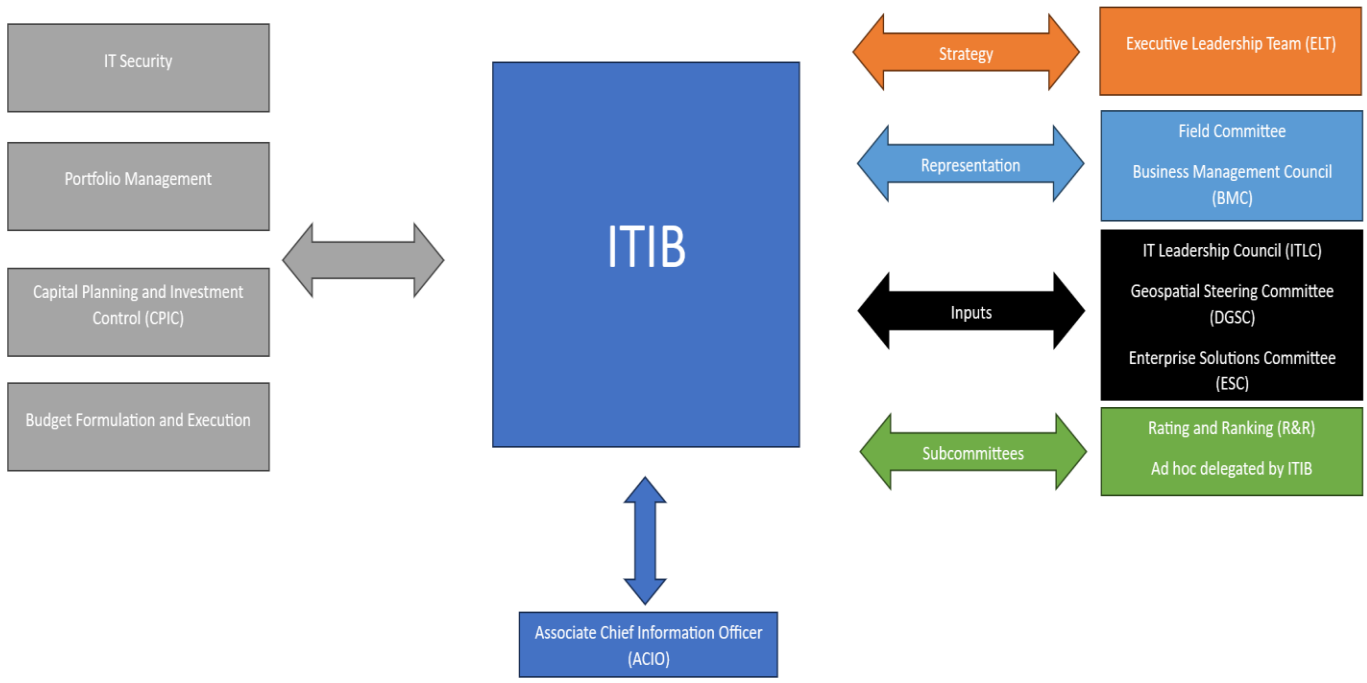


Figure 1-1: Relationship

1.6 CPIC Integration with Other Management Processes

The CCA, OMB Circular A-11, and the FITARA governs the CPIC process and emphasizes three areas of focus: effective CPIC; adherence to the overall policies for all capital planning; and the resource planning to accomplish both objectives. To understand the role of IT capital planning within the IT management process, it is important to recognize how it complements other BLM planning and management processes. What follows is a summary of linkages between the BLM IT CPIC process and related management processes and events.

IT Security

IT security is an inherent component of the CPIC process. All IT investments must demonstrate that costs for appropriate IT security controls and privacy controls are incorporated into the lifecycle planning of all systems in a manner consistent with the FISMA and the OMB guidance for IT investments. Cost effective security of the BLM information systems must be an integral component of business operations.

Federal requirements for baseline system security configurations are outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series and DOI Security and Privacy Control Standards.

IT security is a critical element of the business case criteria for the review and evaluation of investments through the IT CPIC process.

Each business case should include costs associated with all aspects of the Security and the Privacy program ongoing expenses (e.g., authority to operate (ATO) requirements, risk identification, and mitigation activities; privacy impact assessment; and day-to-day investment level security operations activities).

Records Management

Electronic Record Information System (EIS) requirements are set forth in MS-1270 §2.15 and underlying 36 CFR 1220.34(e); 36 CFR 1222.24; 36 CFR 1236.12; 36 CFR 1224.10. IT investments must follow all Records Management Board requirements. If you have any related questions, please contact the Bureau Records Officer.

Technology Business Management (TBM)

Technology Business Management (TBM) is a value-management framework instituted by CIOs, CTOs, and other technology leaders. Founded on transparency of costs, consumption, and performance, TBM gives technology leaders and their business partners the facts they need to collaborate on business aligned decisions. Those decisions span supply and demand to enable the financial and performance

tradeoffs that are necessary to optimize run-the-business spending and accelerate business change. The framework is backed by a community of CIOs, CTOs, and other business leaders on the TBM Council.

In accordance with OMB Circular A-11, agencies must submit their IT investment budgets to OMB using the TBM taxonomy, which enables agencies to disaggregate their IT investment budgets into smaller cost categories provided by the TBM framework. Additionally, the Capital Planning Guidance (CPG) requires BLM to report their full IT spending within applicable IT Cost Pool and IT Tower fields and each Investment identified in the Agency IT Investment Portfolio Summary must have a Unique Investment Identifier (UII).

Budget Formulation and Execution

In accordance with the requirements of OMB Circular A-11, Section 55[6] the BLM is required to annually submit its IT investments as part of the DOI's budget request. This will include existing investments, enhancements to existing investments, and new initiatives. Budgets must utilize the TBM taxonomy, which enable agencies to disaggregate their IT investment budges into smaller cost categories provided by the TBM framework. During the budget process, the rationality of the cost estimates is examined, and agencies are held accountable for meeting the cost goals of their IT investment portfolio. The proposed IT budget should be presented and assessed in a manner consistent with the agency's overall budget request and should be informed both by historical spending levels and by any plans for future expenditures required to meet IT performance objectives. The agency's analysis of its IT spending should align with the prior year's estimated or enacted budget and the estimated or enacted budget for the current year.

An Alternative of Analysis (AoA) is conducted for applicable IT investments, scaled to the size and complexity of individual requirements, and the selection and prioritization of alternatives is based on a Cost Benefit Analysis (CBA). The CBA uses a systematic analysis of expected benefits and costs. Estimates of risk-adjusted costs and benefits show definitively the performance, budget changes, and risk inherent in undertaking the investment.

The BLM's IT CPIC process is closely aligned to its budget cycle. This includes reviews by the respective sponsors of the IT-related funding requests developed by the BLM during the formal budget formulation process. All budget requests will be reviewed and prioritized based on projected requirements as approved by the ITIB and the ACIO. New investments are justified based on the need to fill a gap in the BLM's ability to meet strategic goals and objectives while providing risk-adjusted cost and schedule goals with measurable performance benefits.

IT Leadership Council (ITLC)

The ITLC in coordination with ACIO supports the ITIB as well as BLM's mission vision and strategic direction for IT service delivery. The group ensures coordination, collaboration, and oversight of information, management, and technology resources across the Bureau. The ITLC strives for agility in its approach to respond appropriately to changes in the regulatory environment; technical and business

[6] Appendix C-12

environment; as well as the BLM mission space. The ITLC is responsible for identifying all IMT supportable enterprise IT technology, architecture, solutions, and services within the BLM.

Enterprise Solutions Committee (ESC)

The ESC is responsible for designing, documenting, and supporting the execution of effective enterprise services for the Bureau which align with the needs of the mission, and that can be efficiently sustained by the IMT. This committee acts as a control gate in the delivery of IT services to mission customers and will define processes that ensure new or changed service requests are evaluated for their alignment with existing enterprise solutions and services strategy. Existing services will be continually evaluated to ensure IT services meet the needs of the Bureau and where deficient will establish "to-be" technology roadmaps and service strategies. The ESC supports the ITLC by enforcing BLM strategic enterprise IT solution delivery and service alignment. It monitors and provides guidance to the Bureau's IT projects and infrastructure teams; serves as a forum to discuss and promote innovative ideas in the delivery of enterprise IT; and provides technical analysis support to project teams in support of ITIB approval processes.

Modular Approaches

Modular approaches involve dividing investments into smaller parts in order to reduce investment risk, deliver capabilities more rapidly, and permit easier adoption of newer and emerging technologies. Modular development focuses on an investment, project, or activity of the overall vision and progressively expands upon the BLM's capabilities, until the overall vision is realized. Investments may be broken down into discrete projects, increments, or useful segments, each of which are undertaken to develop and implement the products and capabilities that the larger investment must deliver. [7]

By following a modular approach, the BLM can recognize the following benefits:

- Delivery of usable capabilities that provide value to customers more rapidly as agency missions and priorities mature and evolve;
- Increased flexibility to adopt emerging technologies incrementally, reducing the risk of technological obsolescence;
- Decreased overall investment risk as agencies plan for smaller projects and increments versus "grand design" (each project has a greater overall likelihood of achieving cost, schedule, and performance goals than a larger, all-inclusive development effort);
- Creation of new opportunities for small businesses to compete for the work;
- Greater visibility into contractor performance. Tying award of contracts for subsequent contracts to the acceptable delivery of prior projects provides agencies better visibility into contractor performance and allows a greater opportunity to implement corrective actions without sacrificing an entire investment;
- An investment can be terminated with fewer sunk costs, capping the risk exposure to the agency when the following occurs:
    - priorities change,

[7] Appendix C-7

- a technology decision does not work, or
- a contractor's performance does not deliver results.

Agile Software Development

Agile software development is a method of software development that utilizes an iterative and incremental development process, designs software based on "just-in-time" user needs, and constantly improves software from continuous user feedback. Agile software development principles apply to both pre-award and post-award contexts. The method is based on close collaboration among a cross-functional team. It is a methodology that anticipates the need to adapt to change by introducing flexibility into the delivery of the finished product. The focus is on keeping requirements small, testing often, and delivering functional bits of the application as soon as they are ready.[8]

Per the OMB Digital Services Playbook, Agile software development is the preferred methodology for software development contracts that contribute to the creation and maintenance of digital services, whether they are websites, mobile applications, or other digital channels. It supports frequent changes, updates, and enhancements to the software. By breaking up the development process into small, manageable pieces (each with desired segments of functionality), having end users involved throughout the process, and being guided by the Product Vision, users receive software that better meets their needs (in terms of both functionality and usability) without wasting money and time on unused or unusable features.

Earned Value Management (EVM)

EVM is a program management technique that uses an investment's past performance and work to evaluate and forecast the investment's future performance. This enables the PM to make changes that keep the investment at or bring the investment closer to planned expectations.

Earned value analysis is part of a performance-based management system required by OMB for certain systems or programs that are determined to be major acquisitions because they require special management attention as determined by the Agency. These types of system acquisitions are typically done as cost- or incentive-type contracts and do not typically include commercial product or service contracts at any value. Earned Value analysis is built into the business case (BC) template. The PM plans Work Breakdown Structure (WBS) tasks and builds budget estimates for each task in the project plan. As the plan is executed, the PM tracks actual progress and expenditures at the completion of each WBS against planned figures to obtain cost and schedule variances (SV). These variances can then be used to identify schedule and cost overruns or underruns so they can be resolved as quickly as possible.

1.7 IT Investment Parts

An IT Investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality, and the subsequent operation of those assets in a production environment. IT Investments should have a defined life cycle

[8] Appendix C-8

with start and end dates, with the end date representing the end of the currently estimated useful life of the Investment, consistent with the Investment's most current alternatives analysis if applicable. When the asset(s) is essentially replaced by a new system or technology, it may be appropriate for the replacement to be reported as a new, distinct Investment. Per OMB Circular A-11 Section 55 an agency's IT Investments should be consistent with their budget materials and be categorized in the following three parts:

- Part 1: IT Investments for Mission Delivery- "IT investments that directly support the delivery of the agency's mission."
- Part 2: IT Investments for Mission Support Services- "Mission support services consist of activities that are common across all agencies and include functional areas such as financial management, human resources, contracting, travel, and grants management."
- Part 3: Standard IT Investments- "IT investments for technology goods and services common to all agencies such as IT Infrastructure, IT Security, and IT management."

1.8 Major IT Investment Criteria

All expenditures of IT resources must comply with this CPIC Handbook. This ensures IT Investments are adequately aligned and can be supported by available and sustainable enterprise managed solutions and services. It prevents duplication, enhances IT security, and promotes IT affordability within the Bureau.

OMB Circular A-130 requires that agencies execute processes for planning, budgeting, procurement, management, and assessment, commensurate with the size, scope, duration, and delivery risk of an investment. The following investment types and processes are outlined to support this requirement.

Major Investment

Per the OMB Circular A-11 Section 55, a Major IT investment refers to an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or defined as major by the agency's capital planning and IT investment control process. Agency CIO's can use their discretion to classify any investment as a major investment. The DOI's Major IT investment criteria include at least one of the following:

Financial Thresholds:

- $30M Total Lifecycle Funding (3-year total; PY through BY) or

Qualitative Criteria:

- Importance to the mission or significant role in administration of programs, finances, property, or other resources;
- Identified by executive leadership as critical;
- High risk as determined by departmental or bureau enterprise risk management processes, OMB, GAO, Congress and/or the CIO;
- Classified as a High Value Asset (HVA); and
- E-Government initiatives and enterprise-wide (involves multiple bureaus and offices).

Non-Major Investment

Per OMB Circular A-11 Section 55, Non-Major IT Investments are those that are not designated major by the agency or OMB, or are designated as a "Standard IT Investment," "IT Migration Investment," or "Funding Transfer Investment."

1.9 Process Overview

This section outlines the formal process for Part 1: IT Investments for Mission Delivery as well as any IT Investment the ACIO identifies and designates should adhere to them. The CPIC is a structured process in which proposed and ongoing IT investments are continually monitored and evaluated throughout their lifecycle. Successful investments, as well as terminated or delayed investments, are evaluated to assess the impact on future proposals and to compile lessons learned. The BLM's CPIC contains four phases for a systems' lifecycle. These are pre-select, select, control, and evaluate. As detailed in this document, each phase contains the following common elements:

- Purpose – a description of the objectives of the project expected to be completed in each phase;
- Entry Criteria - describes the requirements and thresholds for entering the given phase;
- Process - the type of justification, planning, and review that will occur in the phase; and
- Exit Criteria – documentation of the action, evaluation methodology, and associated metrics used to determine the project is successful and may reasonably proceed to the next phase.

Completing one phase is necessary before beginning another. The work to document the project activities and provide justifications for the ITIB review is undertaken by the project staff. Each phase is overseen by the ITIB, which ultimately approves or rejects an investment's advancement to the next phase. This ensures that each investment receives the appropriate level of managerial review, coordination, and accountability.

At the highest level, the CPIC process can be represented as a circular flow of BLM's IT investments through four sequential phases as shown in Figure 1-2 and described below:

- **Pre-Select Phase:** In the initial screening process, when IT investments are proposed, executive decision-makers assess each proposed investment's support of the BLM's strategic and mission needs and potential for business improvement. If sufficient benefit potential has been demonstrated, further analysis is carried out to prepare the investment for more detailed review in the Select Phase;
- **Select Phase:** In this phase, IT investment comparison, evaluation, and prioritization are performed. An analysis is conducted with the ITIB selecting and prioritizing IT investments that best support the BLM's mission. Prior to selection, details of how the application can be integrated into the current BLM technical operating environment and architecture will also be addressed. Once approved, the project will officially transition to the OMB's prescribed portfolio management process;

- **Control Phase:** Through timely oversight, quality control, and executive review, the BLM ensures that IT initiatives are executed and developed according to pre-approved schedules and milestones in a disciplined, well-managed, and consistent manner.
- **Evaluate Phase:** In this phase, investments are assessed to determine if planned objectives are being met. Actual results of the implemented projects are compared to forecasted expectations to evaluate investment performance. This is done to assess the investment's impact on mission performance, identify any investment changes or modifications that may be needed, and revise the investment management process based on lessons learned. Matured systems are evaluated to ascertain their continued effectiveness in supporting mission requirements, cost effectiveness of continued maintenance support, potential technological opportunities or upgrade, and if they should be considered for retirement or replacement.

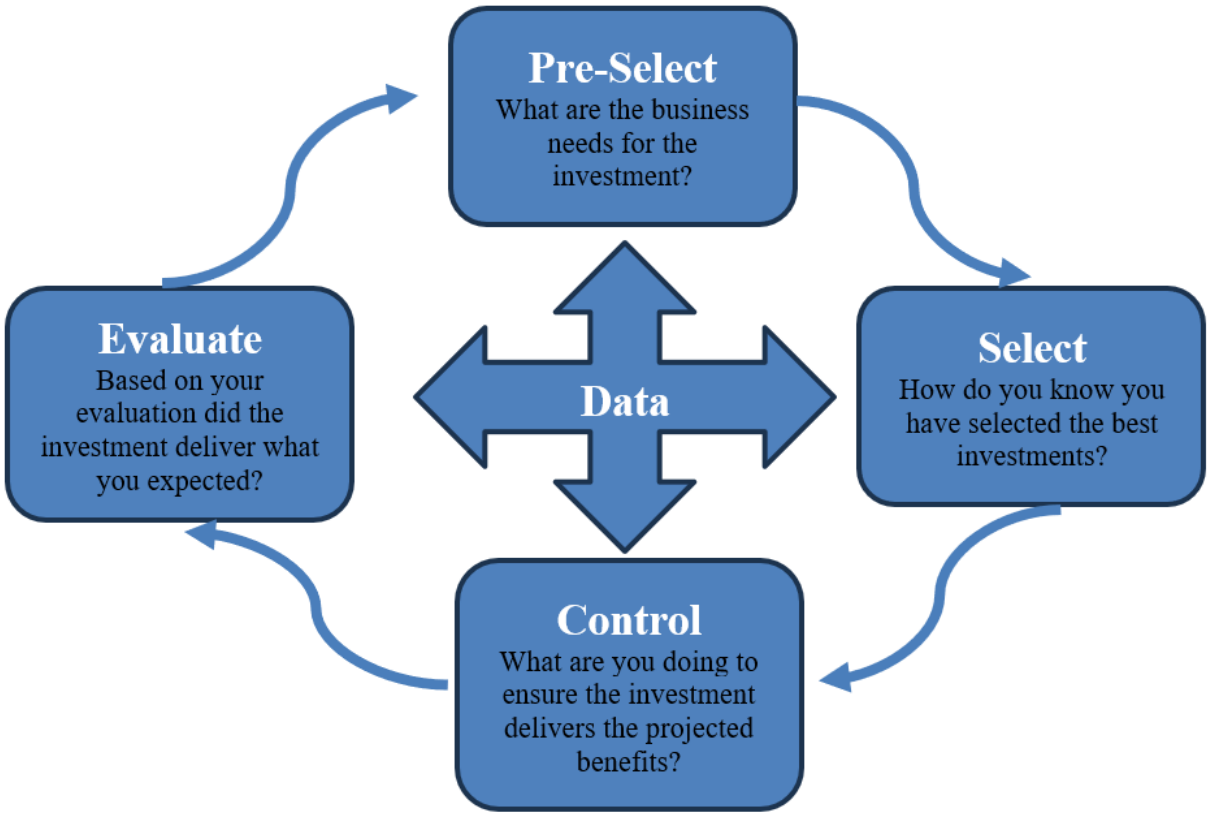


Figure 1-2: CPIC Information and Process Flow

2 Pre-Select Phase

2.1 Purpose

The Pre-Select Phase provides a process to assess a proposed investment or proposed development, modification, or enhancement to a pre-existing investment and determine the degree to which it supports the BLM's operating plan and mission. During this phase the business or mission need is identified and the relationships to the BLM's strategic planning efforts are established. The Pre-Select Phase enables the project proponent to begin defining business needs and associated capabilities, risks, benefits, and costs.

2.2 Entry Criteria

Prior to entering the Pre-Select Phase, the Business Managers generate ideas for the next budget cycle based on BLM missions and strategic goals. Proposed investments must have a new concept which addresses the BLM mission needs. It is expected to include an IT component.

2.3 Process

During the Pre-Select Phase, a Mission Needs Statement (MNS) is prepared (template is available on BLM CPIC website[9]). Completion of the MNS results in the identification of a business opportunity and consideration of an IT solution. The level of required detail varies and should be commensurate with the magnitude, complexity, and cost of the proposed investment. The analysis and corresponding development of a MNS is closely linked to the BLM's strategic planning process.

Figure 2-1 provides a summary of the Pre-Select Phase process, as well as the individual(s) and/or group(s) responsible for completing each process step.

[9] Appendix-D

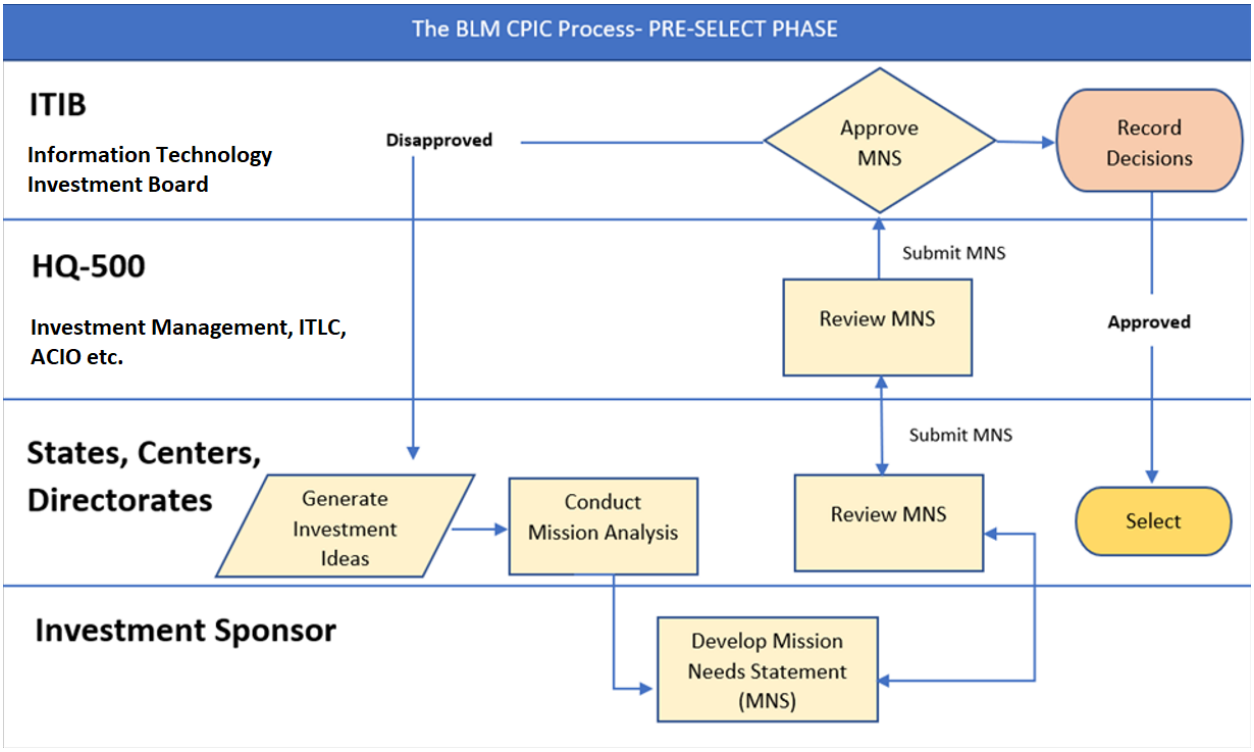


Figure 2-1: Pre-Select Phase Process

2.3.1 Generate Investment Ideas

New ideas or recommendations for enhancement to a current investment are submitted by the Business Managers, Investment Sponsors, or PMs to their ADs, SDs, or CDs (center) for approval.

2.3.2 Conduct Mission Analysis

A mission analysis is a strong, forward-looking analytical activity to evaluate the capacity of the BLM's assets to satisfy existing and emerging demands for services.

The mission analysis enables the BLM to assess and prioritize the most critical capability shortfalls and best technology opportunities to improve overall security, capacity, efficiency, and effectiveness in providing services to customers. Mission analysis is conducted within the framework of the BLM's long-range strategic goals. Concurrently, the mission analysis contributes strongly to the evolution of strategic planning and the BLM's IT enterprise architecture development.

The mission analysis allows the BLM to identify critical needs. Also identified are preliminary resource allocations to specific mission needs within the context of the BLM's overall resource projections and within the constraints of future BLM's budget authority projections. The results of the mission analysis provide micro- and macro-level views as well as key data for strategic planning efforts to include estimation of resources required to complete Select Phase process. More refined resource quantification, including the acquisition of hardware, software, and service contracts, is conducted during the Business Case development in the Select Phase if the investment is selected as part of the BLM's portfolio. The

resource estimate for MNS development will be early in the investment process and therefore is likely based on limited early information. Where available, MNS should include resources (infrastructure, service contracts and staff) as a function of the benefit to the BLM and the mission area, the cost of not addressing the need (e.g., poor customer responsiveness, increased maintenance cost, lost productivity, etc.), and the likely extent of required additional investment or changes to the BLM's infrastructure.

If the mission analysis reveals a non-IT solution (e.g., a policy change, operational procedural change, or transfer of systems between sites) that can satisfy a capability shortfall and can be achieved within approved budgets, it can be implemented as a non-IT initiative, and will not be managed within the CPIC process.

A complete mission analysis should also identify the business drivers (e.g., the BLM's mission, vision, goals, objectives, and tactical plans). Business drivers often involve the need to assist customers in a particular service area such as recreation on public lands.

Once the key business drivers have been identified, a preliminary business requirements analysis is conducted. The business requirements analysis identifies how personnel conduct business activities to fulfill mission requirements, meet objectives, and perform tactical plans.

While MNSs will be generated from the mission analysis, any individual or organization may propose an investment based on a perceived capability shortfall or technological opportunity. Examples of potentially valid needs that could originate outside BLM lines of business include those related to socioeconomic and demographic trends, the environment, statutory requirements, or an industry-developed technological opportunity. These shortfalls and opportunities should be communicated to the project sponsor. The project sponsor will then determine how the mission analysis should be conducted to validate, quantify, and prioritize the proposed need.

The following four principal activities must be addressed while conducting the mission analysis:

1. Identify and quantify projected demand for services. This should be based on input from strategic planning for services needed in the future as well as performance and supportability trends of current systems and projected technological opportunities that will enable the BLM to perform its mission more efficiently and effectively.

2. Identify and quantify existing and projected services that defines what is in place and what is approved for implementation. This includes a preliminary determination of how investments identified might be aligned and supported by existing enterprise solutions and services.

3. Identify, analyze, and quantify capability shortfalls (e.g., the difference between demand and supply) and technological opportunities to increase quality of service, efficiency, and effectiveness.

4. Identify the user and customer base affected.

When the analysis identifies a capability shortfall or technological opportunity, the results are summarized in the MNS (template is available on the BLM CPIC website[10]). The MNS must clearly

[10] Appendix D

describe the capability shortfall and the impact of not satisfying the shortfall or the technological opportunity and the increase in efficiency it will achieve. The MNS also must assess the criticality and timeframe of the need and estimate the resources the BLM should commit to resolving the shortfall based on merit, criticality, and the scope of likely changes to the BLM's IT asset base. This information forms the basis to establish the priority of this need within the context of an enterprise view of all the BLM's needs.

The MNS is a summary document that describes a new opportunity or operational problem and presents the major decision factors that the ITIB should evaluate when considering the need satisfied by the proposed investment.

2.3.3 Review MNS

The InvM verifies with Subject Matter Experts (SME) the current and planned capabilities that are proposed in the MNS and works with applicable organizations to ensure that no redundant IT investments provide or can be modified to provide similar capabilities. Business process owners must simplify or otherwise redesign their existing processes so that services can be provided by existing Investments before initiating new systems investing in new IT programs. Plans for redesign or business process re-engineering (BPR) should be discussed as part of the MNS. The InvM reviews the MNS before final submission to the ITIB. If any modifications or updates are required, the MNS is referred back to the project sponsor for review and update. Final review results are presented to the ITIB for decision.

2.3.4 MNS Approval

The ITIB will review and evaluate the submitted MNS. Approved investments are progressed to the Select Phase for business case development. The ITIB's decision is recorded in the minutes and appropriate parties are notified. A disapproved MNS is sent back to the project sponsor.

2.4 Exit Criteria

Prior to exiting the Pre-Select Phase, the sponsor must obtain ITIB approval of the MNS.

For an approved MNS, the InvM team will collaborate with Bureau Finance personnel to create a Work Breakdown Structure (WBS) code to track preliminary design activities required by FITARA and Statement of Federal Financial Accounting Standard (SFFAS) 10.

Table 2-1 provides a summary of the documents generated during the Pre-Select Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For ITIB Approval
MNS	X	X
ITIB Decision & Meeting Minutes	X	

Creation of preliminary design WBS	X	

Table 2-1: Summary of documents generated during the Pre-Select Phase

3 Select Phase

3.1 Purpose

In the Select Phase, the BLM ensures the IT investments that best support the mission are chosen. Trained, experienced, qualified, and certified PMs are assigned, and risk management is initiated. PMs assigned to Major Investments must be senior-level certified FAC-P/PM. Non-Major Part-1 PMs must be, at a minimum, mid-level certified FAC-P/PM. Investments are reviewed to ensure no duplication of e-Government initiatives or existing system applications. Individual investments are further evaluated in terms of technical alignment with other IT systems and projected performance as measured by Cost, Schedule, Benefit, and Risk (CSBR). For each investment, a high level WBS with proposed milestones and review schedules is established.

In this phase, the BLM prioritizes each investment and decides which investments will be included in the portfolio. Business case submissions are assessed against a uniform set of evaluation criteria and thresholds as identified in OMB Circular A-11, Part 7—Planning, Budgeting, Acquisition, and Management of Capital Assets. The investment's CSBR are then systematically scored using objective criteria and ranked and compared to other investments. Finally, the BLM's ITIB decides on investments that will be included in the BLM's portfolio.

3.2 Entry Criteria

Prior to entering the Select Phase, investments must have an ITIB approved MNS.

3.3 Process

The Select Phase begins with an ITIB approved MNS and moves through the development of the Business Case. These supporting documents lay a foundation for success in the subsequent phases. The Select Phase culminates in a decision whether or not to proceed with the investment.

Figure 3-1 provides a summary of the Select Phase process as well as the individual(s) and/or group(s) responsible for completing each process step.

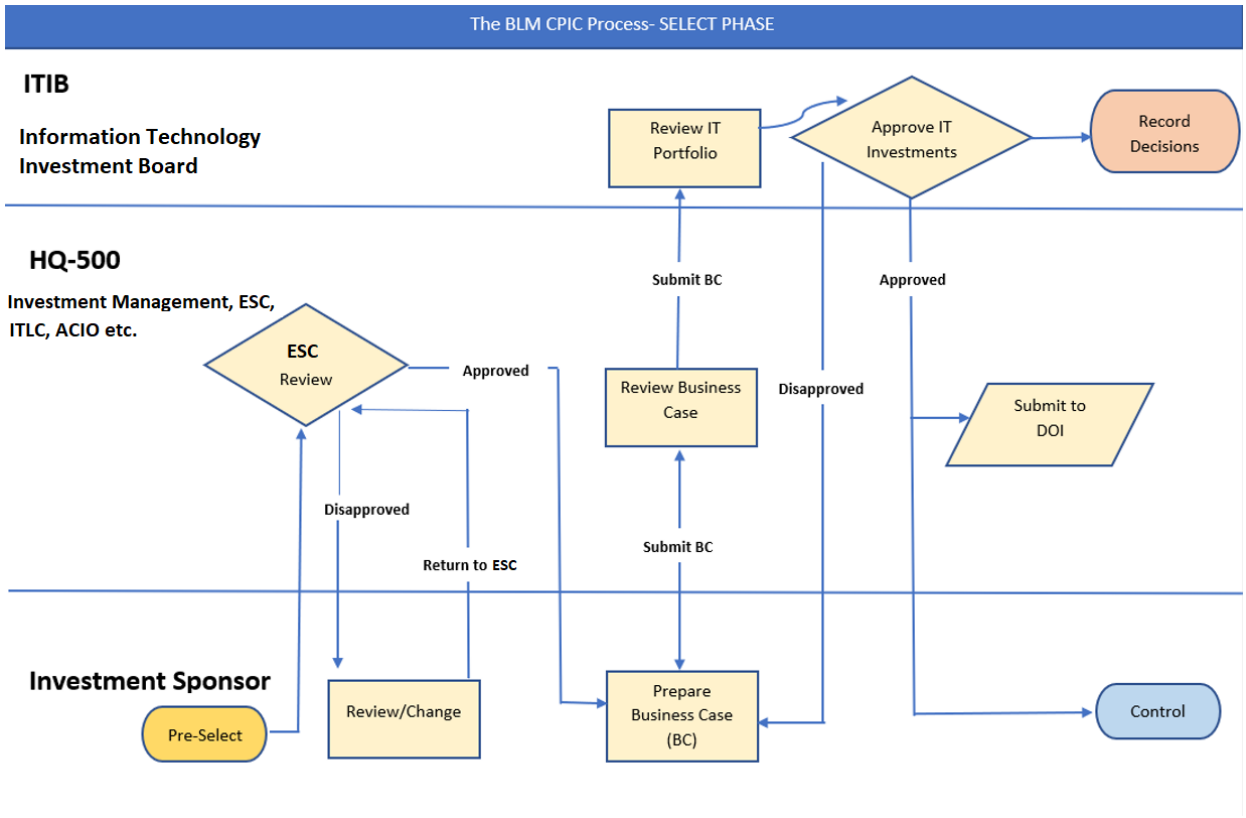


Figure 3-1: Select Phase Process Steps

3.3.1 Review by the ESC and Update of MNS

The Enterprise Solutions Committee (ESC) reviews the investment to ensure alignment with existing enterprise solutions and the Bureau's IT service strategy.

The Investment Sponsor and Business Manager reviews the MNS and other documentation completed during the Pre-Select Phase and are responsible for making any necessary changes.

3.3.2 Develop Business Case and Supporting Materials

The PM prepares the Business Case and supporting materials for the Business Case. The Investment Sponsor ensures that, for each investment, the below listed documents and activities are completed and the results are submitted to the InvM (Guidance and document templates are available on the BLM CPIC website[11]). The InvM may assist with coordinating responses to various sections of the Business Case with the SME as needed.

[11] Appendix-D

The below listed documents are living documents and will be continuously updated as the investment moves through the CPIC lifecycle. Not all documents will be required for all Business Cases. The InvM will work with the PM to identify the required documents, which may differ depending on if the investment is for a new or existing investment. The Portfolio Management CPIC required artifacts do not include other potential Bureau requirements (from IT Security, Records, IT Operations, ESC, etc.) that will be communicated directly from the relevant stakeholders (if applicable).

Business case for new investment:

- Alternative of Analysis (AoA)
- Acquisition Plan
- Investment Charter
- Risk Management Plan (RMP)
- Risk Register

Business case for existing investment:

- AoA
- Revise and resubmit any existing artifacts that are not up to date (if applicable)

Please note: All AoA's must include at least three viable alternatives including the status quo (if applicable), include supporting details for financial information, and meet all OMB and Department mandated requirements (subject to change). For details or questions, please contact InvM.

3.3.3 Review Business Case

The Sponsor reviews and approves the Business Case and Supporting Materials and submits them to the InvM. The InvM, and ITLC reviews the Investment for compliance with BLM strategic, legislative, and budgetary goals. Review results are presented to the ITIB for decision.

3.3.4 Review of the BLM IT Portfolio by the ITIB

The ITIB reviews the IT investment portfolio, recommendations and suggestions from the business case review, and other assessments. The ITIB prioritizes and analyzes the investments to optimize the IT Portfolio based on value, business analysis, risks, and alignment.

3.3.5 Approve IT Investments

After reviewing the portfolio, the ITIB makes final investment decisions. If the investment is approved, it will progress to the Control Phase where funding can be requested or existing funding reprogrammed for development and implementation. The ITIB's decision is recorded and appropriate parties are notified. If the business case is disapproved, it is returned to the sponsor for corrective actions.

3.3.6 Submit to the DOI

The InvM submits approved business cases to the DOI. For the DOI to consider an IT initiative for inclusion in the overall DOI IT portfolio, it must be reviewed, approved, and vetted through the CPIC process. In the interim, the InvM performs the following functions:

- Preparing budget and supporting materials (all investments);
- Revising baseline cases based on new guidelines or changes from the OMB (majors only).

3.4 Exit Criteria

Prior to exiting the Select Phase, investments must have executed the following activities:

- Established performance goals and quantifiable performance measures;
- Developed a high-level project plan which details quantifiable plans and objectives such as high level acquisition schedule, project deliverables, and costs;
- Identified CSBR;
- Established security, Section 508 (IT accessibility), drafted, submitted, and accepted Privacy Impact Assessments (PIA);
- Documented data requirements sufficient for successful Control Phase execution based on investment risk, complexity, and development approach;
- Established an ITIB investment review schedule for the Control Phase;
- Finalized the project charter with approval from the project sponsor and the ITIB; and
- Obtained ITIB approval to enter the Control Phase.

Table 3-1 provides a summary of the documents generated during the Select Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For ITIB Approval
Business Case*	X	X
Supporting Documents*	X	X
Creation of development WBS	X	
* Living documents that will get updated as the investment proceeds through the CPIC lifecycle		

Table 3-1: Summary of documents generated during the Select Phase

4 Control Phase

4.1 Purpose

The objective of the Control Phase is to ensure, through timely oversight, quality control, and executive review, that IT initiatives are implemented in a disciplined, well-managed, and consistent manner. Investments should be closely tracked against the various components identified in the initial Project Management Plan. This phase also promotes the delivery of quality products and results in initiatives that are completed within scope, on time, and within budget. During this process, the ITIB monitors the progress and performance of ongoing IT investments against projected cost, schedule, performance, and delivered benefits. For major investments, the BLM also submits regular updates to the DOI for additional oversight.

Based on control reviews, the ITIB will conduct a portfolio analysis to determine the performance of the BLM's IT portfolio. The reviews focus on ensuring that projected benefits are being realized; cost, schedule, and performance goals are being met; risks are minimized and managed; and the investment continues to meet strategic needs. Depending on the review's outcome, decisions may be made to continue, modify, or terminate investments, suspend funding, or make future funding releases conditional on corrective actions.

4.2 Entry Criteria

Prior to entering the Control Phase, investments must satisfy the Select Phase exit criteria:

- Established performance goals with quantifiable measures;
- Formulated a high-level project plan which details quantifiable objectives such as a high-level acquisition schedule, project deliverables, and costs;
- Identified initial costs, schedule, benefits, and risks;
- An approved funding plan;
- Established requirements for: security, Section 508 (IT accessibility), Privacy Act assessment, data, and architecture goals and measures; and
- Obtained ITIB approval to enter the Control Phase.

4.3 Process

Throughout the Control Phase, the PMs submit Status Reports to the InvM. In turn, the InvM provides the ITIB with investment reviews to assist them in monitoring all investments in the portfolio. The Status Reports provide an opportunity for PMs to raise issues concerning the IT developmental process, including security, network requirements, enterprise architecture alignment and more.
The PM is responsible for evaluating project performance and reporting material variances.

All investments are required to provide cost and schedule baseline and performance information to the InvM on a monthly basis. Ongoing performance reporting enables InvM to conduct investment and portfolio-level analysis in accordance with the OMB reporting requirements.

A Corrective Action Report (CAR) is required if the project performance variance exceeds ten (10) percent from the project's established baseline or the ITIB is otherwise dissatisfied with project progress.

Figure 4-1 provides a summary of the Control Phase process as well as the individual(s) and/or group(s) responsible for completing each process step.

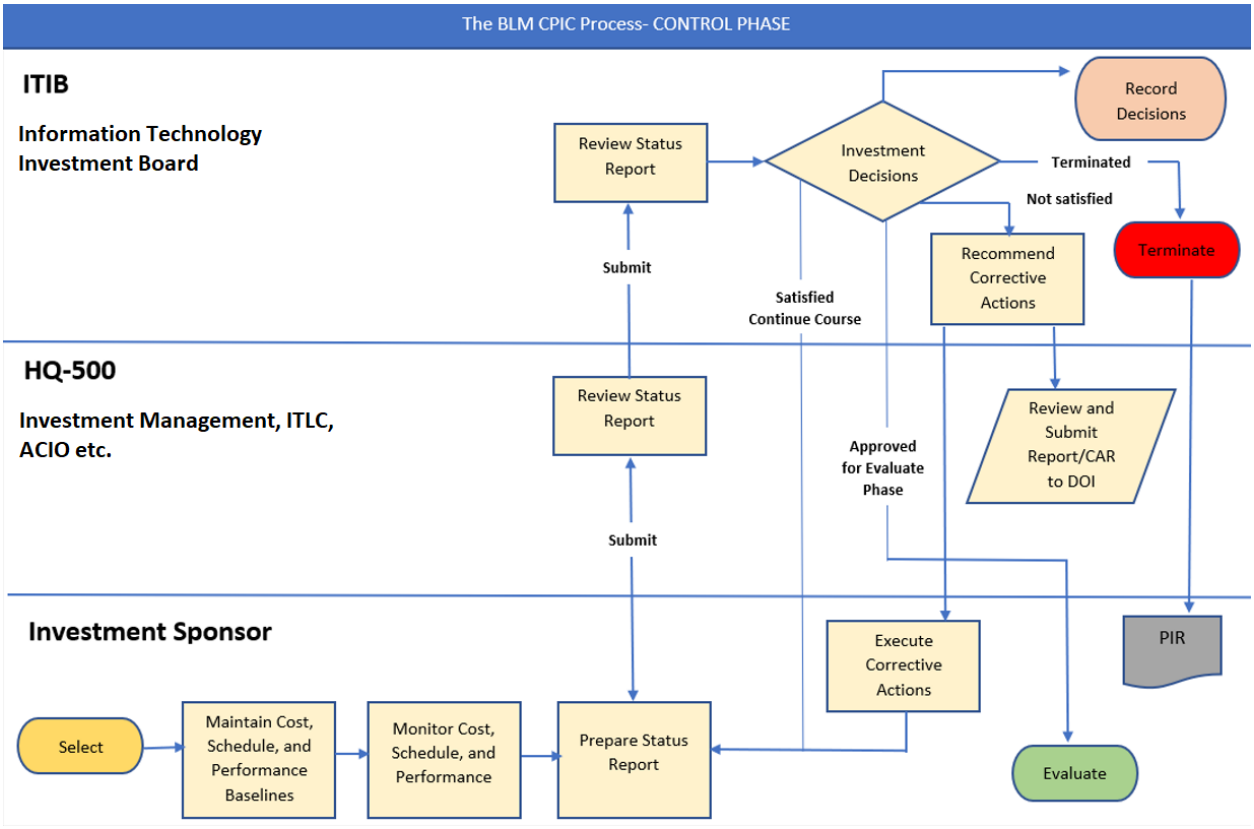


Figure 4-1: Control Phase Process Steps

4.3.1 Maintain Project Costs, Schedule, and Technical Baselines

In accordance with U.S. code 44, Chapter 35 Coordination of Federal Information Policy, Section 3506, Federal Agency Responsibilities, agencies must have the means to effectively and efficiently manage IT. Office of Management and Budget (OMB) M-10-27 also requires agencies to have baseline management policy in place that addresses establishment, management, and change to investment baselines.

Investment baselines for major IT investments require DOI CIO approval. Bureaus and offices must continue to maintain and update major IT investment baselines in accordance with DOI, OMB, and other relevant federal laws and requirements.

4.3.2 Monitor Current Project Cost, Schedule, and Technical Information

The PM collects actual information on the resources allocated and expended throughout the Control Phase. The project sponsor ensures that the investment still aligns with the mission and strategic plan. The PM compares the actual information collected to the estimated baselines developed during the Select Phase and identifies root causes for any differences. The PM reviews the security and infrastructure analyses for accuracy. The PM maintains a record of changes to the initiative's technical components including hardware, software, security, and communications equipment.

4.3.3 Investment Artifact Requirements

All Part-1 IT investments must develop the following artifacts or update existing artifacts as necessary. The PM must upload their artifacts to the appropriate folders on the InvM website. The PM is responsible for providing updated versions (including date of last update) as changes are made or as available throughout the IT investment's lifecycle. The InvM will submit the required artifacts to the DOI and the OMB.

Artifact	Submission Frequency
Investment Charter, including the IPT (if/when projects are added to the investment, Investment charter should be updated).	Submit once, update as needed.
Investment-Level Alternative Analysis and Benefit-Cost Analysis	Every 3 years.
Risk Management Plan and Risk Register	Annually.
Operational Analyses (for operational or mixed life cycle systems).	Annually.
Post Implementation Review (PIR) Results (investment level or project specific).	As necessary within 6 months after implementation.
Documentation of Investment Rebaseline and Management	As applicable.
Acquisition Plan	Annually.

Table 4-1: IT investments artifacts

4.3.4 Prepare Status Report

On a monthly basis the PM prepares a status report that provides project status on costs, schedule, and risks. Ongoing performance reporting enables the InvM to conduct investment and portfolio-level analysis in accordance with the OMB's reporting requirements.

Once complete, this status report is submitted to the InvM for review.

4.3.5 Review Status Report

The InvM evaluates the Status Reports for project performance and prepares findings and recommendations for the ITIB.

4.3.6 ITIB Review of Status Report

Achieving maximum benefits from an investment, while minimizing risks, requires that the investment be consistently monitored and managed for successful results. The ITIB continues to monitor investments making decisions and taking actions to change the course of a particular investment when necessary. The ITIB determines whether to continue, modify, or terminate the project and if the PM is managing investment cost and SV, mitigating risks, and providing projections for future performance based upon work accomplished to date. The ITIB verifies if the current cost and schedule projections align with the investment.

4.3.7 Investment Decision

The ITIB reviews the Status Reports along with the InvM findings and recommendations and issues one of the four decisions listed below:

1. Continue the investment "as is"

2. Recommend corrective actions – the ITIB may recommend corrective action if:

   - The Project performance variance exceeds ten (10) percent from the project's established baseline;
   - There are constant changes in the requirements and work scope;
   - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;
   - The investment's outcome does not adequately support the mission, business, or security function; and/or
   - Major problems hinder the planned investment development.

   These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.

3. Rebaseline the investment. PMs, with sponsor concurrence and approval, must request ACIO/ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ACIO/ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.

4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment. If an investment is terminated, the PM prepares and confirms the PIR schedule (section 5.3).

4.3.8 Investment Re-baseline

Re-baselining is required in response to changed requirements, funding changes, or realization that the operative implementation plan is not achievable. This includes the addition, removal, and adjustment of projects and activities to the investments currently approved baseline (cost and/or schedule). A re-baseline constitutes a revised implementation plan with a new milestone schedule.

All re-baselines require ACIO/ITIB review and approval, and the respective budget officer must be aware of the change. Re-baselines exceeding a +/-10% change to the performance measurement baseline, or a major change to the technical approach will need the investment teams to provide more detail regarding the rationale and impact of the change, and a meeting between the ACIO/ITIB and the investment team may be required for approval.

4.4 Exit Criteria

Prior to exiting the Control Phase, investments must complete the following activities:

- Complete investment development, production deployment, and/or implementation;
- Confirm the PIR schedule;
- Obtain ITIB approval to enter the Evaluate Phase.

Table 4-2 provides a summary of the documents generated during the Control Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
Status Reports	**X**	**X**
PIR Schedule (For investments terminated or approved for Evaluate Phase)	**X**	
Updated Business Case	**X**	**X**

Table 4-2: Summary of documents generated during the Control Phase

5 Evaluate Phase

5.1 Purpose

The purpose of the Evaluate Phase is to compare actual to expected results after an investment is fully implemented. This is done to assess the investment's impact on mission performance, identify any investment changes or modifications that may be needed, and revise the investment management process based on lessons learned. The Evaluation Phase closes the loop of the IT investment management process by comparing actual against estimates to assess the performance and identify areas where decision-making can be improved.

The Evaluate Phase focuses on three outcomes:

- Determines whether the IT investment met its performance, cost, and schedule objectives;
- Provides the means to assess mature investments, determine their continued effectiveness in supporting mission requirements, evaluate the cost of continued maintenance support, assess technology opportunities, and consider potential retirement or replacement of the investment; and
- Determines the extent to which the CPIC process improved the outcome of the IT investment.

The outcomes are measured by collecting performance data, comparing actual to projected performance and conducting a PIR and OA (Operational Analysis) to determine the system's efficiency and effectiveness in meeting performance and financial objectives.

5.2 Entry Criteria

The Evaluate Phase begins once a system has been implemented and becomes operational or goes into production. Prior to entering the Evaluate Phase, investments must have executed the following activities:

- Complete investment development and production deployment;
- Confirm the PIR schedule; and
- Obtain BLM ITIB approval to enter the Evaluate Phase.

5.3 Process

Investments enter the Evaluate Phase based on the ITIB's decision to either continue the investment, with or without modifications, or to terminate the investment. Investments move to the PIR stage and after a successful PIR to the OA stage. During the PIR, actual performance measures are compared to performance projections made during the Select Phase. Then, "lessons learned" for both the investment and the CPIC process are collected and applied to prior CPIC phases.

PIR STAGE:

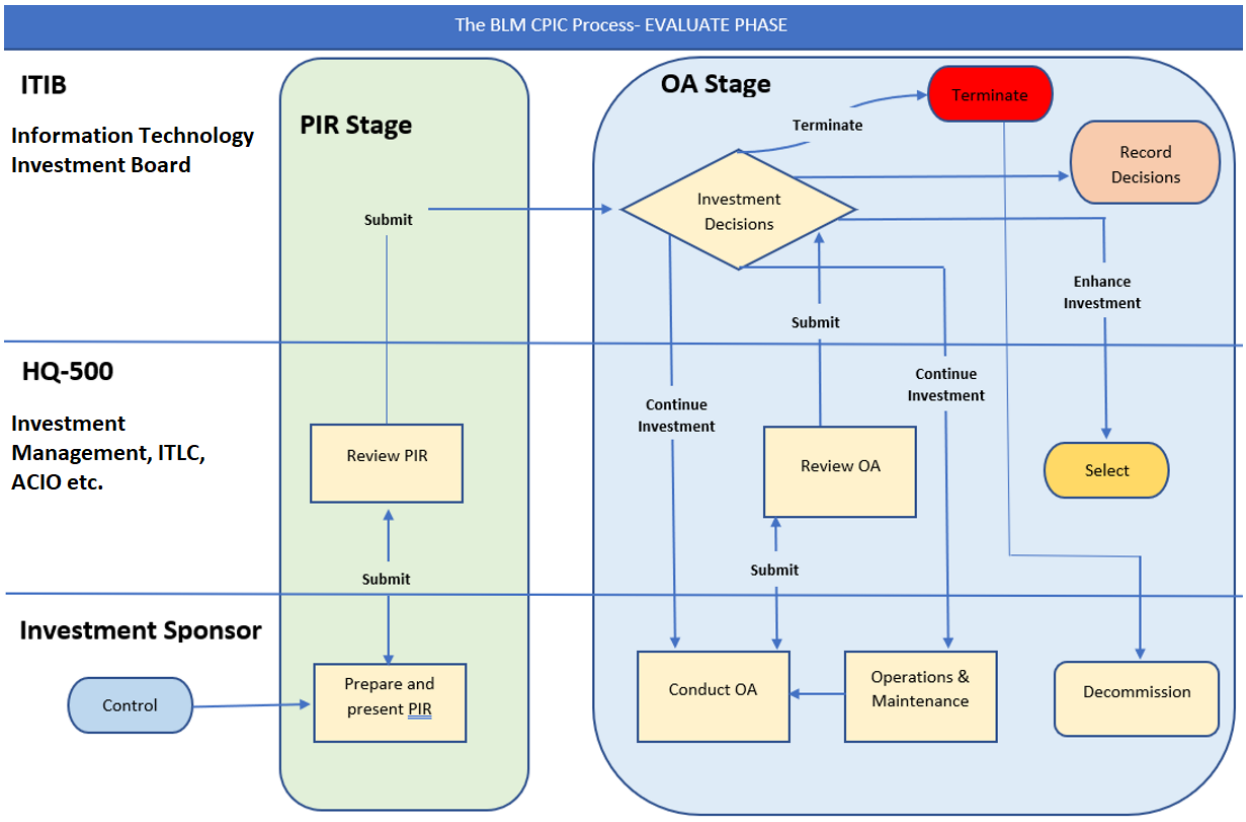
From the time of implementation, the system is continually monitored for performance, maintenance activities, costs, resource allocation, defects, problems, and system changes. System stability is also periodically evaluated. The PIR (template is available on the BLM CPIC website[12]) includes a methodical assessment of the investment's costs, performance, benefits, documentation, mission, and level of stakeholder and customer satisfaction.

The PIR process involves reviewing mission needs and project goals, collecting and analyzing cost, schedule, performance, and customer satisfaction data, and providing major findings and issues to the InvM. It also provides feedback and incorporates lessons learned.

The PIR is conducted by the project sponsor and PM and results are reported to the InvM and ITIB to provide a better understanding of initiative performance and to assist the project sponsor in directing any necessary initiative adjustments.

OA STAGE:
During this stage, an OA (template and guidance on the BLM CPIC website[12]) is performed annually for operational or mixed lifecycle systems to determine.

Figure 5-1 provides a summary of the Evaluate Phase process, both in the PIR and OA stages, as well individual(s) and/or group(s) responsible for completing each process step.



[12] Appendix-D

Figure 5-1: Evaluate Phase Process Steps

5.3.1 Prepare and Present PIR

The PIR schedule is determined during the Control Phase. The PIR for a newly deployed initiative should take place six to twelve months after the system is operational. In the case of a terminated system, it should take place within six months because the review will help to define any "lessons learned" that can be factored into future IT investment decisions and activities. In either case, before starting the PIR, the project sponsor develops a PIR plan that details the roles, responsibilities, and schedule for all PIR tasks.

The project sponsor also prepares and makes a formal PIR presentation to the InvM. The presentation should summarize the investment evaluation and provide a summary of recommendations for presentation to the ITIB.

5.3.2 Review PIR

InvM reviews the PIR results, prepares findings and recommendations, and forwards the package to the ITIB for review

5.3.3 Approve PIR

The ITIB reviews the PIR results of the investment and issues one of the four decisions listed below:

1. Continue the investment "as is" and approve to move to the OA stage;

2. Recommend corrective actions – the ITIB may recommend corrective actions for the following:

   - Project performance variance exceeds ten (10) percent from the project's established baseline;
   - There are constant changes in the requirements and work scope;
   - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;
   - The investment's outcome does not adequately support the mission, business, or security function; and
   - Major problems hinder the planned investment development.

   These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.

3. Re-baseline the investment. PMs, with sponsor concurrence and approval, must request ACIO/ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ACIO/ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.

4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment.

If the investment is approved to remain operational, an OA is prepared. Investments that are not operational are removed from the BLM's portfolio. The ITIB's decision is recorded and appropriate parties are notified.

5.3.4 Conduct OA

The project sponsor and the PM conduct an OA (template is available on the BLM CPIC website[13]) to assess the cost and extent of continued maintenance and upgrades. The OA should include a trend analysis of O&M costs and a quantification of maintenance releases. Costs for Government employees as well as any customer cost should be included in all cost estimates and analysis. OA is conducted annually for operational and mixed lifecycle systems.

The project sponsor and PM also conduct an analysis to determine if the system is continuing to meet mission requirements and supports the BLM's evolving strategic direction. The mission analysis process identified in the Pre-Select Phase and the MNS provide a framework to assist in the mission analysis for the OA Stage. This includes an analysis of the performance measurements accomplished.

The PM assesses the technology and determines potential opportunities to improve performance, reduce costs, meet Security, Data, Privacy, Records, and GIS requirements, and to ensure alignment with BLM's strategic direction.

Alternatively, the ITIB may decide to enhance an investment and return it to the Select Phase. The ITIB also reviews InvM recommendations to rate and rank the investment as a part of the ITIB's function of annual reselection of BLM's IT portfolio. Systems that are not annually reselected will be terminated and removed from the portfolio. InvM then informs the project sponsors of the ITIB decisions and recommendations.

5.3.5 Review OA

InvM reviews the OA results and prepares findings and recommendations. The updated package is then submitted to the ITIB.

5.3.6 Investment Decisions

The ITIB, after reviewing the OA and the recommendations of InvM, makes one of the following decisions:

1. Continue the investment "as is" and approve to move to the OA stage;

2. Recommend corrective actions – the ITIB may recommend corrective actions for the following:

    - Project performance variance exceeds ten (10) percent from the project's established baseline;
    - There are constant changes in the requirements and work scope;
    - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;
    - The investment's outcome does not adequately support the mission, business, or security function; and
    - Major problems hinder the planned investment development.

[13] Appendix-D

These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.

3. Re-baseline the investment. PMs, with sponsor concurrence and approval, must request ACIO/ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.

4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment.

5.3.7 Operation

The project is operational and is in the OA stage.

The formal monitoring of investment progress, and the determination of risks and returns, continues throughout the life of the investment or until the investment is enhanced. The investment is considered to be in O&M or Steady State (SS). The following activities may be performed without requiring a re-baseline or completion of an MNS.

- Technical Refresh (swapping out old software or hardware with newer software or hardware to perform the same function but improve performance);
- Upgrading/adding bandwidth capacity;
- Patch Management;
- Release Management (installing new releases of the same software);
- Cleanup of existing directories performance;
- Monitoring and Management of existing network;
- Replacing or moving an existing office circuit from one location to another;
- IT service and support to end users; and
- Replacing defective HW with a new unit that is fundamentally the same but without defect.

5.3.8 Capture Lessons Learned

The Evaluate Phase also provides the project sponsor and the PM with an opportunity to assess and share lessons learned about the CPIC management processes. The InvM uses these assessments to recommend CPIC process improvements to the ITIB

To capture "lessons learned," the project sponsor develops an investment management report and submits it to InvM. All failures and successes are collected and shared to ensure that future initiatives benefit from past experiences. A high-level assessment of management techniques, including organizational approaches, budgeting and acquisition, contracting strategies, tools and techniques, and testing methodologies is essential to establish realistic baselines and to ensure the future success of other IT initiatives.

5.4 Exit Criteria

Prior to exiting the Evaluate Phase, investments must have completed the following activities:

- Conducted a PIR;
- Established an OA review schedule.

Table 5-1 provides a summary of the documents generated during the Evaluate Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
PIR Presentation	**X**	**X**
Updated Business Case	**X**	
Operational Analysis Schedule	**X**	
Operational Analysis	**X**	**X**

Table 5-1: Summary of documents generated during the Evaluate Phase

The investment remains in the OA stage until a decision is made by the BLM ITIB to modify, replace, or retire the system.

New development, modernization or major enhancements (DME) to OA systems are required to complete an MNS and start at the Pre-Select Phase. Per OMB IT Budget - Capital Planning Guidance, "DME refers to projects and activities leading to new IT assets/systems, as well as projects and activities that change or modify existing IT assets to substantively improve capability or performance, implement legislative or regulatory requirements, or meet an Agency leadership request. DME activity may occur at any time during a program's life cycle. As part of DME capital costs can include hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs for planning, development, acquisition, system integration, and direct project management and overhead support."

6 Waiver

6.1 Purpose

The waiver process provides a standardized guideline for requesting an exception to the process, procedure, and/or regulation, specifically as it relates to IT investments and associated funding. For example, a natural disaster may necessitate that the Pre-Select Phase or Select Phase be waived to expedite the IT Investment Management Process, or an appeal made to exceed approved funding levels. A mandated or unforeseen IT expenditure may result in the submission of a waiver request which would require modifications to the IT Spend Plan. However, based on the nature of the investment, IT Security, Privacy, and EA screening procedures may have to be implemented as an out-of-cycle process. Upon approval, this change will be incorporated into the BLM's IT portfolio.

6.2 Entry Criteria

Prior to submitting a waiver, the request must meet one of the following criteria:

- A BLM mission-critical system, infrastructure, or replacement resulting from an emergency condition;
- A mandated or unforeseen expenditure;
- The result of a Congressional directive that must be in place within a very short period of time; or
- The result of a DOI directive that must be in place within a very short period of time.

6.3 Process

Figure 6-1 provides a summary of the waiver process as well as the individual(s) and/or group(s) responsible for completing each process step.

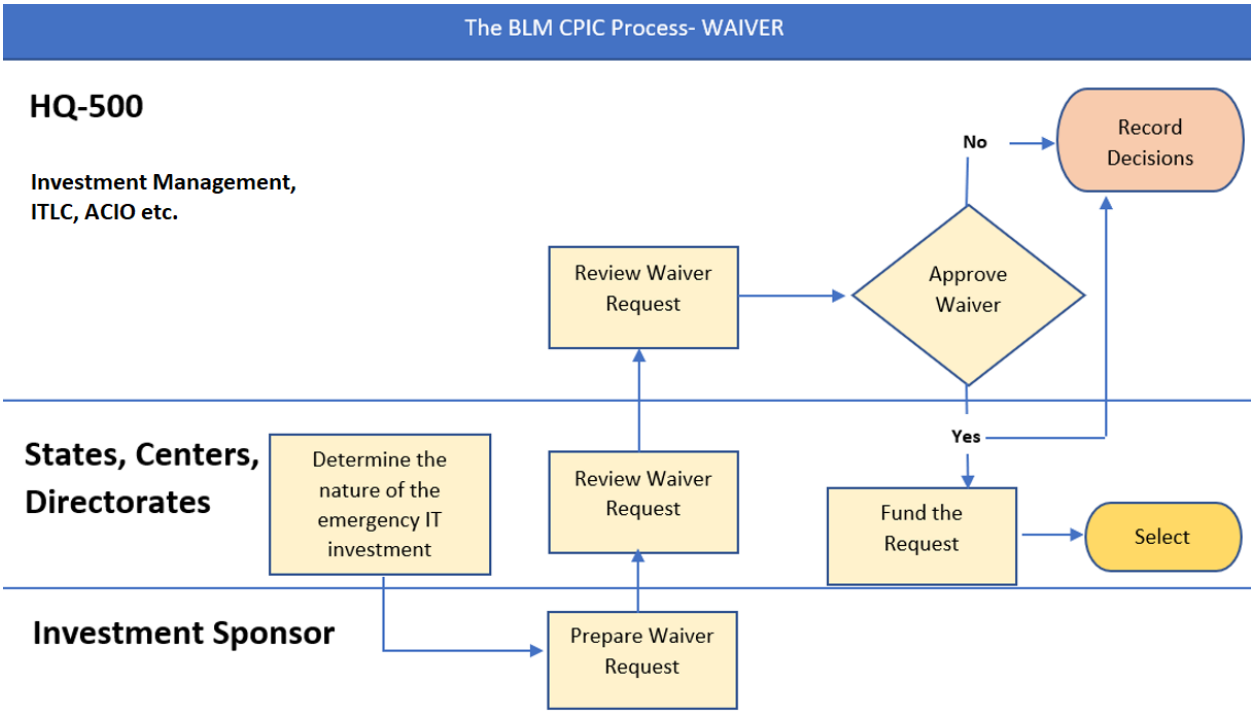


Figure 6-1: Waiver Process

6.3.1 Determine the Nature of the Emergency IT Investment

The criteria defined in Section 6.2 may necessitate that the investment sponsor determines if an emergency waiver is appropriate.

The investment sponsor will work with IMT to determine if an existing application/system may be able to meet the immediate requirements of the investment for which the emergency waiver is being developed. The investment sponsor will also work with IMT to determine new or proposed hardware, software, or service contract acquisition to meet the requirements of the waiver.

6.3.2 Prepare Waiver Request

The investment sponsor and the PM prepare a waiver request. The waiver request provides supporting justification as to why the waiver is being requested. The following are addressed:

- Nature and circumstances of the need;
- The scope of the new or proposed investment or new or proposed acquisition ;
- A proposed budget or spending plan; and
- Description of risk and impact.

6.3.3 Submit Waiver Request

All completed waiver requests must be submitted to the InvM who will facilitate the expedited ACIO approval process. For details see latest InvM guidance.

6.3.4 Review Waiver Request

The waiver request is reviewed by the InvM to determine potential funding issues and conflicts, as well as describing the impacts to the total IT Portfolio. The InvM will also develop IT portfolio adjustment alternatives or strategy should the ACIO approve the exemption.

6.3.5 Decision for submitting Waiver Request

The InvM recommends the waiver to the ITLC. If it is concurred by the ITLC, it is forwarded to the BLM ACIO for approval. If it is rejected, it is returned to the investment sponsor.

6.3.6 Decision for Waiver Request

ITLC members analyze the information with findings and recommendations provided. From this information, they will make their decision to exempt the investment from the specified process or not.

6.3.7 Fund the Request

Based on the nature and the alternatives presented, the ACIO decides to approve the investment or acquisition by adjusting the IT Portfolio. Approving the investment or acquisition will have an impact on the IT portfolio which will be documented by the InvM.

The Record of Decision is documented by the InvM and the investment re-enters the CPIC process.

6.4 Exit Criteria

The exception investment must obtain ACIO approval.

Table 6-1 provides a summary of the documents generated during the waiver process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
Waiver Request	**X**	**X**
Supporting Documents	**X**	

Table 6-1: Summary of documents generated during the waiver process

7 Portfolio Management

7.1 Purpose

The purpose of IT Portfolio Management is to ensure that an optimal mix of IT investments with manageable risk and returns is defined, selected, and funded. Portfolio Management comprises the following:

- Defining portfolio goals and objectives;
- Understanding, accepting, and balancing trade-offs;
- Identifying, eliminating, and minimizing risks;
- Monitoring and measuring portfolio performance;
- Assessing whether desired goals and objectives have been obtained; and
- Determining how each portfolio fits into the BLM's overarching architecture including IT Modernization Blueprints for key lines of business.

IT Portfolio Management delivers the following benefits:

- Contributes to investment management decision-making by providing pertinent information;
- Provides key information for monitoring cost and performance; and
- Provides information for investment decisions throughout the life of the investment.

7.2 Prerequisites

In order to perform the activities associated with selecting, funding, and managing an optimal IT investment portfolio, adequate resources must be provided for executing the process.

- ITIB members must exhibit core competencies in portfolio management.
- All investments within the portfolio must be analyzed and prioritized based on each investment's CSBR throughout the investment's lifecycle.
- BLM must have defined its common portfolio categories.

7.3 Process

The portfolio management process ensures that the ACIO/ITIB collectively analyzes all investments and proposals to select those that best fit with BLM's strategic business direction, needs, and strategic vision. In addition, BLM has fiscal and workforce constraints that must be weighed against the risks and the long

term return on investments within the portfolio. When making portfolio decisions, executives must consider use of IT resources along with work force and contracting options available to meet mission objectives.

7.3.1 Portfolio Formulation

Throughout the FY, investments must complete the OMB and the DOI requirements as part of the budget cycle. The requirements and processes outlined in this section are to assess the costs and benefits of all proposed IT investments and to formulate the optimal portfolio of IT investments for the upcoming BY. Through this process, the BLM funds and prepares IT investments that best support the BLM's mission and strategic priorities for success.

7.3.2 IT Spend Plan

To formulate the BLM's IT Portfolio accurately and collaboratively, IMT issues the IT Spend Plan template annually for all investments and offices via instruction memorandum for completion and submission.

The IT Spend Plans serve as the source documents for IT budgetary requests and the totals are transmitted to DOI and OMB through the initial budget and President's budget submission process. For more details, please contact InvM team or view the annual IT Spend Plan guidance.

7.3.3 IT Acquisitions

The Deputy Assistant Secretary for Budget, Finance, Grants and Acquisition (DAS-BFGA) releases an annual memorandum that requires each DOI bureau and office to submit their Forecast for the upcoming fiscal year, as required by section 8(a)(12)(C) of the Small Business Act, 15 U.S.C. 637(a)(12)(C). In alignment with the DOI Federal Information Technology Acquisition Reform Act (FITARA) Implementation Plan and the DOI Acquisition, Arts, and Asset Policy (DOI-AAAP-0147, v02), acquisition and IT leadership must plan, review, and evaluate collaboratively all IT-related acquisitions, at the bureau, office, and Departmental level. The Forecast process addresses this requirement. Bureaus and offices should refer to the most recent Forecast memorandum for details on the submission process.

7.3.4 Joint Certification Statement (JCS)

In response to the OMB requirements outlined in FITARA, the DOI initiated a joint certification process where the DOI certifies the IT Portfolio prior to any submission to the OMB. First, the BLM BO and the BLM ACIO must jointly sign the JCS to certify prioritization and allocation of IT investment costs. Once signed at the BLM level, the DOI CIO and the Director of Budget will certify the entire request and submit a JCS Budget Exhibit to the OMB. The DOI will distribute the JCS to the BLM during a FY, during BY Passback (President's Budget) and during BY Official submission. Please see DOI JCS latest guidance for details.

7.3.5 IT Portfolio/Investment Updates

All Major and Non-Major Mission IT investments must update the IT Portfolio Summary information prior to the BY official IT budget submission. The BLM ITIB and the BLM ACIO must review the BY budget requests. Prior to the submission the BLM BOs should validate the submission to ensure each IT investment's life cycle costs table, funding sources, and more match bureau or office funding for PY, CY, and BY.

Additionally, all Major IT investments should update both the Major IT Business Case and the Major IT Business Case Detail processes in the system of record. The Major Investment Business Cases provide the budgetary and management information necessary for sound planning, management, and governance of IT investments. These documents help the BLM explicitly align IT investments with strategic and performance goals, and ultimately provide value to the public by making IT investment and management information more transparent.

7.4 Portfolio Evaluation

Portfolio evaluation focuses on the assessment of the overall health and performance of the IT Portfolio. Portfolio and project reviews are conducted to provide for the assessment and to make necessary adjustments to the IT Portfolio.

After examining all IT assets considering the BLM's business objectives and assumptions, the ITIB prioritizes business objectives and then evaluates proposed IT Investments against those objectives using enterprise portfolio analysis software tools. Upon approval of the outcome, the ITIB conducts portfolio optimization to determine the best mix of investments, thus helping to align resources behind the most effective means of achieving Agency objectives.

7.4.1 IT Portfolio Reviews

The performance of BLM's entire IT Portfolio is reviewed throughout the year by InvM and the ACIO. Formal portfolio reviews may include but are not limited to discussing strategic topics, open action items, and facilitate open discussion and review etc. In practice, the BLM IT Portfolio evaluation process provides the basis to re-affirm or "re-select" funded projects based on continuing to meet a business/mission need and meeting project performance objectives, such as cost, schedule, and technical performance. To create an optimized portfolio, it is vital that all IT investments have been uniformly judged on both their merits and liabilities.

At their discretion, the ITIB and/or ACIO may direct the review of an individual investment or portfolio when deemed necessary and to make recommendations for further improvement subject to ACIO and ITIB approval. An output of the portfolio review process is to accomplish an optimal IT portfolio that meets business and mission needs.

Appendix A - Definitions

Accessibility

Information technology products or services that are in full compliance with the standards of section 508 of the Rehabilitation Act of 1973.

Acquisition Plan

Description of the acquisition approach including:

- Contract strategy (definition of government and contractor roles and responsibilities);
- Use of enterprise solutions and strategic contracts;
- Major milestones (such as software releases, hardware delivery, installation, and testing).

Adequate security

Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Agency

Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.

Agency Strategic Plan

A plan that provides general and long-term goals that the agency aims to achieve, the actions the agency will take to realize those goals, the strategies planned, how the agency will deal with challenges and risks that may hinder achieving results, and the approaches it will use to monitor its progress.

Agile Development

A development methodology that uses an iterative approach to deliver solutions incrementally through close collaboration and frequent reassessment.

Appropriations

An appropriation provides budget authority that permits Government officials to incur obligations that result in immediate or future outlays of Government funds. Regular annual appropriations. These appropriations are:

- Enacted normally in the current year;
- Scored entirely in the budget year; and
- Available for obligation in the budget year and subsequent years if specified in the language (see "Availability," below).

Architectural Alignment

Degree to which the IT initiative is compliant with the DOI's and BLM's IT architecture.

Architecture

An integrated framework for evolving or maintaining existing technologies and acquiring new technologies to support the mission(s).

Assets

Tangible or intangible items owned by the Federal Government which would have probable economic benefits that can be obtained or controlled by a Federal entity.

Authorization to Operate (ATO)

The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

Authorization boundary

All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

Authorization package

The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

Authorizing official

A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

Availability

Appropriations made in appropriations acts are available for obligation only in the budget year unless the language specifies that an appropriation is available for a longer period. If the language specifies that the funds are to remain available until the end of a certain year beyond the budget year, the availability is said to be "multi-year." If the language specifies that the funds are to remain available until expended, the availability is said to be "no-year." Appropriations for major procurements and construction projects are typically made available for multiple years or until expended.

Baseline Goals

Baseline cost, schedule, and performance goals will be the standard against which actual work is measured. They will be the basis for the annual report to the Congress required by FASA Title V on variances of 10 percent or more from cost and schedule goals and any deviation from performance goals. The goals, and any changes to the goals, must be approved by the OMB.

- Cost and schedule goals. The baseline cost and schedule goals should be realistic projections of total cost, total time to complete the project, and interim cost and schedule goals. The interim cost and schedule goals should be based on the value of work performed or a comparable concept.
- Performance goals. A target level of performance against which actual achievement or progress can be compared, preferably expressed as a tangible, measurable objective or as a quantitative standard, value, or rate. This can include goals containing key milestones or goals framed as a position relative to the past or relative to peers.
- Illustrative major milestones in establishing goals. Illustrative major milestones in establishing or proposing revised baseline goals could be:
    - Agency mission analysis, process design, and requirements development;
    - Agency submission and justification to the OMB;
    - Approval for inclusion in the Administration's budget proposal to the Congress;
    - Enactment of appropriations;
    - Before and after the contract or contracts are signed; and
    - Other times after the contracts are signed, depending on circumstances.

Benefit

Quantifiable or non-quantifiable advantage, profit, or gain.

Binding Operational Directive

A compulsory direction from the Department of Homeland Security to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

Budget Authority

The authority provided by law to incur financial obligations that will result in outlays. The specific forms of budget authority are appropriations, borrowing authority, contract authority, and spending authority from offsetting collections. This definition is the same as the one contained in section 3(2) of the Congressional Budget and Impoundment Control Act of 1974, which the Congress uses in the congressional budget process.

Budget Classification Categories

The Life Cycle Costs table in eCPIC, which feeds the Department IT Portfolio and Major IT Business Cases, collects funding at a detailed level of categories listed below:

- Government full time equivalents (FTE);
- Contract Services;

- Hardware Costs (HW);
- Software Costs (SW);
- Travel Costs;
- Rent, Communications, Utilities; and
- Other costs.

Budget Cycle

The overall estimated cost for one fiscal year including direct and indirect costs.

Budget Resources

Budget resources refer to the mean amounts available to incur obligations in a given year. Budgetary resources consist of new budget authority and unobligated balances of budget authority provided in previous years.

Business Case

Structured proposal for business improvement that functions as a decision package for organizational decision-makers. A business case includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints, and risk-adjusted CBA. The business case is this document is for the DOI purposes.

Business Continuity Plan

A plan that focuses on sustaining an organization's mission or business processes during and after a disruption, and may be written for mission or business processes within a single business unit or may address the entire organization's processes.

Business Process

A collection of related, structured activities or chain of events that produce a specific service or product for a particular customer or group of customers.

Business Process Reengineering

A systematic, disciplined approach to improving business processes that critically examines, rethinks, and redesigns mission delivery processes.

Business Requirements Analysis

Identifies how personnel conduct business activities to fulfill mission requirements, meet objectives, and perform tactical plans.

Capital Asset

Tangible property including durable goods, equipment, buildings, installations, and land.

Certification and Accreditation

The official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations, Agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

Chief Information Officer

The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.

Chief Information Officers Council

The Council codified in the E-Government Act of 2002.

Commercially Available Off-The-Shelf (COTS) Item

Any item, other than real property, that is of a type customarily used by the general public for nongovernmental purposes, and that has been sold, leased, or licensed to the general public; is sold, leased, or licensed in substantial quantities in the commercial marketplace; and is offered to the Government, without modification, in the same form in which it is sold, leased, or licensed in the commercial marketplace.

Common control

A security or privacy control that is inherited by multiple information systems or programs.

Control Phase

Capital planning phase that requires ongoing monitoring of IT investments against schedules, budgets, and performance measures.

Controlled Unclassified Information

Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

Cost

Defined in Statements of Federal Financial Accounting Concepts (SFFAC) No. 1, Objectives of Federal Financial Reporting, as the monetary value of resources used. Defined more specifically in Statements of Federal Financial Accounting Standards (SFFAS) No. 4, Managerial Cost Accounting Concepts and Standards for the Federal Government, as the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, such as to acquire or produce a good or to perform an activity or service. Depending on the nature of the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period) or to an asset account for recognition as an expense of subsequent

periods. In most contexts within SFFAS No. 7, Accounting for Revenue and Other Financing Sources, "cost" is used synonymously with expense.

Critical infrastructure

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters.

Customer

Groups or individuals who have a business relationship with the organization; those who receive or use or are directly affected by the products and services of the organization.

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Development Modernization and Enhancement (DME)

Per OMB IT Budget – Capital Planning Guidance, "DME refers to projects and activities leading to new IT assets/systems, as well as projects and activities that change or modify existing IT assets to substantively improve capability or performance, implement legislative or regulatory requirements, or meet an Agency leadership request. DME activity may occur at any time during a program's life cycle. As part of DME capital costs can include hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs for planning, development, acquisition, system integration, and direct project management and overhead support."

Discount Rate

The interest rate used in calculating the present value of expected yearly benefits and costs.

Dissemination

The government-initiated distribution of information to a nongovernment entity, including the public. The term 'dissemination,' as used within this Circular, does not include distribution limited to Federal Government employees, intra- or interagency use or sharing of Federal information, and responses to requests for agency records under the Freedom of Information Act or the Privacy Act.

Earned Value Analysis

A structured approach to project management and forecasting including comparisons of actual and planned costs, work performed, and schedule.

Efficiency measures

While outcome measures provide valuable insight into program achievement, more of an outcome can be achieved with the same resources if an effective program increases its efficiency.

Agencies are encouraged to develop efficiency measures. Efficiency gains may be described as maintaining a level of performance at a lower cost, improving performance levels at a lower cost, improving performance levels at the same cost, or improving performance levels to a much greater degree than costs are increased. Simply put, efficiency is the ratio of the outcome or output to the input of any program.

Enterprise architecture

- Means:
    - A strategic information asset base, which defines the mission;
    - The information necessary to perform the mission;
    - The technologies necessary to perform the mission; and
    - The transitional processes for implementing new technologies in response to changing mission needs.
- And includes :
    - A baseline architecture;
    - A target architecture; and
    - A sequencing plan.

Environment of operation

The physical surroundings in which an information system processes, stores, and transmits information.

Evaluate Phase

Capital planning phase that requires IT investments to be reviewed once they are operational to determine whether the investments meet expectations.

Executive agency

Has the meaning defined in Title 41, Public Contracts section 133.

Expected Outcome

Projected end result of the initiative (e.g., system(s) being replaced or improved customer service) that is directly linked with performance measures.

Feasibility Study

Preliminary research performed to determine the viability of the proposed initiative by performing an alternatives analysis including market research and extensive interviews with SMEs. Also includes a proposed technical approach and preliminary cost, scope, and schedule data.

Federal information

Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system

An information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

Federal Privacy Council

The Council established by Executive Order 13719.

Full Cost

All direct and indirect costs to any part of the Federal Government of providing goods, resources, and services (OMB Circular A–25: User Charges (July 8, 1993). The total amount of resources used to produce the output. More specifically, the full cost of an output produced by a responsibility segment is the sum of:

- The costs of resources consumed by the responsibility segment that directly or indirectly contribute to the output; and
- The costs of identifiable supporting services provided by other responsibility segments within the reporting entity and by other reporting entities.

Functional Requirements

A description of system capabilities or functions required to execute a required process such as a communication link between several locations and generating specific reports.

Funding

There are two types of funding for projects:

- Full funding means that appropriations are enacted that are sufficient in total to complete a useful segment of a capital project (investment) before any obligations may be incurred for that segment. When capital projects (investments) or useful segments are incrementally funded, without certainty if or when future funding will be available, it can result in poor planning, acquisition of assets not fully justified, higher acquisition costs, projects (investments) delays, cancellation of major projects (investments), the loss of sunk costs, or inadequate funding to maintain and operate the assets. Budget requests for full acquisition propose for full funding.
- Incremental (annual) funding means that appropriations are enacted that only fund an annual or other part of a useful segment of a capital project (investment). The OMB or the Congress may change the agency's request for full finding to incremental funding in order to accommodate more projects in a year than would be allowed with full funding.

Funding Source

Funding Source (or Fund Account Title, as defined in the OMB Circular A-11) refers to the direct appropriation or other budgetary resources an agency receives. Bureaus and offices need to identify the budget account and the budget authority provided. Report those budget accounts providing the financing for a particular IT investment. Where IT investment funding is provided in a manner such that "original paying accounts" within agencies are transferring resources to a different agency account which ultimately supports the IT investment (for example, when bureau accounts are paying into a central CIO office account or a WCF), the funding source provided in the Department IT Portfolio should be that of the account which ultimately pays contracts and other costs directly, for the IT investment, rather than the original paying accounts.

Government publication

Information that is published as an individual document at Government expense, or as required by law, in any medium or form.

Hardware or Equipment

Includes any equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information (e.g., computers and modems); capital and non-capital purchases or leases.

Hybrid control

A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control.

Incident

An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Independent Verification and Validation

An independent review conducted by persons separate from the management and operation of the investment or system.

Inflation

The proportionate rate of change in the general price level as opposed to the proportionate increase in a specific price. Inflation is usually measured by a broad-based price index such as the implicit deflator for Gross Domestic Product or the Consumer Price Index.

Information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

Information dissemination product

Any recorded information, regardless of physical form or characteristics, disseminated by an agency, or contractor thereof, to the public.

Information life cycle

The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

Information management

The planning, budgeting, manipulating, and controlling of information throughout its' life cycle. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

Information resources

Information and related resources, such as personnel, equipment, funds, and information technology.

Information resources management

The process of managing information resources to accomplish agency missions. The term encompasses an agency's information and the related resources, such as personnel, equipment, funds, and information technology.

Information Resource Management Strategy

A strategy that demonstrates how information resources management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Information security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information.

Information security architecture

An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, information security systems, personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

Information security continuous monitoring

Maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.

Information security continuous monitoring program

The compendium of methods, tools, and techniques necessary to implement the agency information continuous monitoring strategy in a way that is sufficient to inform risk-based decisions and maintain operations within established risk tolerances. The program includes determining monitoring metrics, establishing monitoring frequencies, and developing a monitoring architecture.

Information security continuous monitoring strategy

A comprehensive plan to address monitoring requirements and activities at each organizational tier (organization, mission or business process, and information system).

Information system security plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Information security program plan

A formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information system

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information system life cycle

All phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing.

Information system resilience

The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

Information technology

Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

Information technology investment

An expenditure of information technology resources to address mission delivery and management support. This may include a project or projects for the development, modernization, enhancement, or maintenance of a single information technology asset or group of information technology assets with related functionality, and the subsequent operation of those assets in a production environment. These investments shall have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment’s most current alternatives analysis if applicable.

Information Technology Investment Management

A decision-making process that, in support of agency missions and business needs, provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of all major investments made by an agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the investments.

Information technology resources

All agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants that establish or support information technology not operated directly by the Federal Government.

Information Technology Systems for National Security

Section 5142 of ITMRA defines a national security system as follows:

- DEFINITION - In this subtitle, the term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which:
    - Involves intelligence activities;
    - Involves cryptologic activities related to national security;
    - Involves command and control of military forces;
    - Involves equipment that is an integral part of a weapon or weapons system; or
    - Subject to subsection is critical to the direct fulfillment of military or intelligence missions.
    -
- LIMITATION – Subsection:
    - Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Infrastructure

The IT operating environment (e.g., hardware, software, and communications).

Initial authorization

The initial risk determination and risk acceptance decision based on a zero-base review of the information system conducted prior to its entering the operations or maintenance phase of the system development life cycle. The zero-base review includes an assessment of all security and privacy controls (i.e., system-specific, hybrid, and common controls) contained in an information system security plan or in a privacy plan and implemented within an information system or the environment in which the system operates.

Interagency agreement

For the purposes of this document, a written agreement entered into between two or more Federal agencies that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other(s) (the requesting agency), including assisted acquisitions as described in

the OMB Memorandum: Improving the Management and Use of Interagency Acquisitions and other cases described in FAR Part 17.

Integrated Project Teams (IPT)

The OMB and the Department require that any bureau and office IT investment planning to perform any DME must establish an IPT. An IPT refers to a cross-functional or multidisciplinary group of individuals organized and collectively responsible for the specific purpose of delivering a project, product, or process to an external or internal customer. An IPT must include at a minimum: a qualified, fully dedicated IT program manager; a contracting specialist, if applicable; an IT specialist; an IT security specialist; and a business process owner or SME.

IT Portfolio

Combination of all IT assets, resources, and investments that an organization owns. The IT Portfolio considers new proposals along with previously funded investments to identify the appropriate mix and synergies of IT investments that best meet organizational, mission, and technological needs.

Lifecycle

The duration of the system life typically organized into four phases: initiation, development, operation, and disposal.

Lifecycle Benefits

The overall estimated benefits for a particular program alternative over the time period corresponding to the life of the program including:

- Cost or expense reduction (productivity and headcount);
- Other expense reductions (operational);
- Cost or expense avoidance; and
- Revenue-related savings.

Lifecycle Cost

The overall estimated cost for a particular program alternative over the time period corresponding to the life of the program including direct and indirect initial costs plus any periodic or continuing costs of operation and maintenance.

Major Investment

Per the OMB Circular A-11 Section 55, a Major IT investment refers to an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or defined as major by the agency's capital planning and IT investment control process. Agency CIO's can use their discretion to classify any investment as a major investment. The DOI's Major IT investment criteria include at least one of the following:

Financial Thresholds:

- $30M Total Lifecycle Funding (3-year total; PY through BY) or

Qualitative Criteria:

- Importance to the mission or significant role in administration of programs, finances, property, or other resources
- Identified by executive leadership as critical
- High risk as determined by departmental or bureau enterprise risk management processes, OMB, GAO, Congress and/or the CIO
- Classified as a High Value Asset (HVA) and,
- E-Government initiatives and enterprise-wide (involves multiple bureaus and offices)

Mission Analysis

Analysis of current and forecasted mission capabilities in relationship to projected demand for services.

Modular Development Approach

The OMB and the Department require that any bureau and office IT investment planning to perform any DME must leverage a modular development approach to focus on on-time delivery. Incremental development is required with deliverables not to exceed 90-120 day increments. More information and guidance can be found within the OMB's Contracting Guidance for Modular Development.

Nation's Integrated Industrial Base

The Nation's integrated industrial base includes those companies with facilities, design and manufacturing processes, and technologies capable of servicing both commercial and Government needs.

National security system

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities:

- Involves cryptologic activities related to national security;
- Involves command and control of military forces;
- Involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications);
- Or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-Developmental Item (NDI)

Any previously developed item of supply used exclusively for governmental purposes by a Federal agency, a State, or local government that requires only minor modifications or modifications of a type customarily available in the commercial marketplace.

Non-Major Investments

Per OMB Circular A-11 Section 55, Non-Major IT Investments are "those that are not designated major by the agency or OMB, or are designated as a "Standard IT Investment", "IT Migration Investment", or "Funding Transfer Investment".

Ongoing authorization

The risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.

Operations and Maintenance (O&M) and Steady State (SS)

Per OMB IT Budget – Capital Planning Guidance, "Operations & Maintenance Costs refers to the expenses required to operate and maintain an IT asset that is operating in a production environment. O&M costs include costs associated with operations, maintenance activities, and maintenance projects needed to sustain the IT asset at the current capability and performance levels. IT includes Federal and contracted labor costs, corrective hardware and software maintenance, voice and data communications maintenance and service, replacement of broken or obsolete IT equipment, overhead costs, business operations and commercial services costs, and costs for the disposal of an asset. Also commonly referred to as steady state."

Open data

Publicly available data that are made available consistent with relevant privacy, confidentiality, security, and other valid access, use, and dissemination restrictions, and are structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are consistent with principles, explained in the OMB guidance, of such data being public, accessible, machine-readable, described, reusable, complete, timely, and managed post-release.

Opportunity Costs

Cost of not investing in the initiative or cost of a forgone option.

Outcome Measure

Outcomes describe the intended result of carrying out a program or activity. Outcome measure indicates progress against achieving the intended result of a program. Indicates changes in conditions that the Government is trying to influence.

Outlay

The issuance of checks, disbursement of cash, or electronic transfer of funds made to liquidate a federal obligation. Outlays also occur when interest on the Treasury debt held by the public accrues and when the Government issues bonds, notes, debentures, monetary credits, or other cash-equivalent instruments in order to liquidate obligations. Also, under credit reform, the credit subsidy cost is recorded as an outlay when a direct or guaranteed loan is disbursed.

Output Measure

A type of measure, specifically the tabulation, calculation, or recording of activity or effort usually expressed quantitatively. Outputs describe the level of activity that will be provided over a period of time. Outputs refer to the activities or products of a program. While output measures can be useful, there must be a reasonable connection between outputs used as performance indicators and outcomes. Agencies should select output measures based on evidence supporting the relationship between outputs and outcomes, or in the absence of available evidence, based on a clearly established argument for the logic of the relationship.

Overlay

A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

Payback Period

The number of years it takes for the cumulative dollar value of the benefits to exceed the cumulative costs of an investment.

Performance budget

A budget presentation that clearly links performance goals with costs for achieving a target level of performance. In general, a performance budget links strategic goals with related long-term and annual performance goals (outcomes) with the costs of specific activities to influence these outcomes about which budget decisions are made. The Performance Budget/Annual Performance Plan is either used to structure or is a part of the agency's budget submission to the OMB and the agency's Congressional Budget Justification.

Personally identifiable information

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Performance Indicator

What is to be measured including the metric to be used (e.g., conformance, efficiency, effectiveness, costs, reaction, or customer satisfaction), scale (e.g., dollars, hours, etc.), formula to be applied (e.g., percent of "a" compared to "b," mean time between failures), or conditions under which the measurement will be taken (e.g., taken after system is operational for more than 12 hours, adjusted for constant dollars, etc.).

Performance Measures

Method used to determine the success of an initiative by assessing the investment contribution to predetermined strategic goals. Measures are quantitative (e.g., staff-hours saved, dollars saved, reduction in errors, etc.) or qualitative (e.g., quality of life, customer satisfaction, etc.).

Performance Measurement

Means of evaluating efficiency, effectiveness, and results. A particular value or characteristic used to measure progress toward goals, and also used to find ways to improve progress, reduce risks, or improve cost-effectiveness.

Portfolio

A set of programs, projects or other work grouped together to meet strategic goals and objectives.

Pre-Select Phase

Capital planning phase that provides a process to assess whether IT investments support strategic and mission needs.

Privacy continuous monitoring

Maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

Privacy continuous monitoring program

An agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.

Privacy continuous monitoring strategy

A formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

Privacy control

The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

Privacy control assessment

The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.

Privacy impact assessment

An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

Privacy program plan

A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

Privacy plan

A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.

Program

An ongoing initiative composed of a group of projects and other work managed in a coordinated way to obtain benefits not obtained from managing them individually.

Program management control

In the context of information security and privacy, a control that is generally implemented at the agency level, independent of any particular information system, and essential for managing information security or privacy programs.

Program Risk-Adjusted Budget (PRB)

The total budget that represents the amount of resources and schedule expected to be needed to cover the risk of cost and schedule overruns to meet a 90 percent probability of project/program success. It is an amount held at a level above the program level to be released to the program when needed to cover risk that was not identifiable through an IBR, but that history indicates will cause cost and schedule overruns from the Performance Measurement Baseline through no fault of the program management process.

Project

A temporary endeavor to create a unique product or service with a start date, a completion date, and a defined scope.

Project Charter

A document issued by senior management that provides the PM with the authority to apply organizational resources to project activities.

Project Plan

A document that describes the technical and management approach to carrying out a defined scope of work including the project organization, resources, methods, and procedures and the project schedule.

Project Sponsor

Defines business needs and associated capabilities, risks, benefits, and costs of an investment.

Provisioned IT Service

An information technology service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency.

Public information

Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.

Reauthorization

The risk determination and risk acceptance decision that occurs after an initial authorization. In general, reauthorization actions may be time-driven or event-driven; however, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that drives risk above the previously agreed-upon agency risk tolerance.

Records

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

Records management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Return

The difference between the value of the benefits and the costs of an investment. In a CBA, it is computed by subtracting the Total Discounted Costs from the Total Discounted Benefits; and it is called the Total NPV.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of:

- The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
- The likelihood of occurrence.

Risk management

The program and supporting processes to manage risk to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other organizations, and the Nation, and includes:

- Establishing the context for risk-related activities;
- Assessing risk;
- Responding to risk once determined; and
- Monitoring risk over time.

Risk Management Plan

A description of potential cost, schedule, and performance risks and impact of the proposed system to the infrastructure. Includes a sensitivity analysis to articulate the effect different outcomes might have on diminishing or exacerbating risk. Provides an approach to managing all potential risks.

Risk management strategy

The description of how an agency intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.

Risk response

Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.

Security

Measures and controls that ensure the confidentiality, integrity, availability, and accountability of the information processes stored by a computer.

Security category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.

Security control

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Security control assessment

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

Security control baseline

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Plan

Description of system security considerations such as access, physical or architectural modifications, and adherence to Federal and the DOI security requirements.

Select Phase

Capital planning phase used to identify all new, ongoing, and operational investments for inclusion into the IT portfolio.

Sensitivity Analysis

An analysis of how sensitive outcomes are to changes in assumptions. Assumptions about the dominant cost or benefits elements and the areas of greatest uncertainty deserve the most attention.

Software

Any software, including firmware, specifically designed to make use of and extend the capabilities of hardware or equipment.

Steady State Phase

Capital planning phase that provides the means to assess mature IT investments to ensure they continue to support mission, cost, and technology requirements.

Strategic Goal

A statement of aim or purpose that is included in a strategic plan. Strategic goals articulate clear statements of what the agency wants to achieve to advance its mission, and address relevant national problems, needs, and challenges. Each performance goal should relate to the strategic goals of the agency.

Sunk Cost

A cost incurred in the past that cannot be recovered which may or may not affect present or future decisions.

Supply chain

A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

Supply chain risk

Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Supply chain risk management

The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

Support Costs

Costs of activities not directly associated with production. Typical examples are the costs of automation support, communications, postage, process engineering, and purchasing.

System-specific control

A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.

Systems security engineering

A specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that satisfies stakeholder requirements; is seamlessly integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to stakeholders.

Tailoring

The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls.

Target

Quantifiable or otherwise measurable characteristic that tells how well or at what level a program aspires to perform.

Technical Requirements

Description of hardware, software, and communications requirements associated with the initiative.

TechStat

A face-to-face, evidence-based accountability review of an IT investment that enables the Federal Government to intervene to turn around, halt, or terminate IT projects that are failing or are not producing results for the American people.

Trustworthy information system

An information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

Appendix B - Acronyms

AA	Alternative Analysis
ACIO	Assistant Chief Information Officer
AD	Assistant Directors
AP	Acquisition Plan
BFIRM	Business Fiscal and Information Resources Management
BC	Business Case
BLM	Bureau of Land Management
BMC	Business Management Council
BO	Budget Office
BPR	Business Process Reengineering
bStat	BLM Status
BY	Budget Year
CAR	Corrective Action Report
CBA	Cost-Benefit Analysis
CCA	Clinger Cohen Act of 1996
CD	Center Director
CFO	Chief Financial Officer
CIO	Chief Information Officer
COTS	Commercial-Off-The-Shelf
CPIC	Capital Planning and Investment Control
CSBR	Cost, Schedule, Benefit, and Risk
CSAM	Cyber Security Assessment & Management
CV	Cost Variance
CV%	Cost Variance Percentage
CY	Current Year
DAC	Data Advisory Committee
DME	Development, Modernization and Enhancement
DOG	Deputies Operation Group
DOI	Department of the Interior
DSD	Deputy State Directors
EA	Enterprise Architecture
eCPIC	Electronic Capital Planning Investment Control
ELT	Executive Leadership Team
EOC	Explanation of Change
EVM	Earned Value Management
EVMS	Earned Value Management System
FAC-P/PM	Federal Acquisition Certification for Program and Project Managers
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition Streamlining Act
FC	Field Committee
FDCCI	Federal Data Center Consolidation Initiative

FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GAO	Government Accountability Office
GPEA	Government Paperwork Elimination Act of 1998
GPRA	Government Performance and Results Act of 1993
GSC	Geospatial Steering Committee
HW	Hardware
IDC	Integrated Data Collection
IPT	Integrated Project Team
InvM	Division of Investment Management
IT	Information Technology
ITMRA	Information Technology Management Reform Act
JCS	Joint Certification Statement
MAR	More Accurate Reporting
MNS	Mission Needs Statement
NOC	National Operations Center
O&M	Operations and Maintenance
OA	Operational Analysis
OMB	Office of Management and Budget
PBCR	Performance Baseline Change Request
PIA	Privacy Impact Assessment
PIR	Post-Implementation Review
PM	Project Manager
POG	Principles Operating Group
PRA	Paperwork Reduction Act
RMP	Risk Management Plan
ROI	Return on Investment
RRC	Rating and Ranking Committee
SD	State Director
SFFAC	Statements of Federal Financial Accounting Concepts
SFFAS	Statements of Federal Financial Accounting Standards
SME	Subject Matter Expert
SS	Steady State
SV	Schedule Variance
SV%	Schedule Variance Percentage
SW	Software
WBS	Work Breakdown Structure
WCF	Working Capital Fund
WO	Washington Office

Appendix C - References

1. ***ITIB Charter****:* Charter of the IT Investment Board, Bureau of Land Management, November 2013.

2. ***Field Committee Charter****:* Charter of the Field Committee, Bureau of Land Management, May 2014.

3. ***Business Management Council Charter****:* Charter of the Business Management Council, Bureau of Land Management.

4. ***Geospatial Steering Committee Charter****:* Charter of the Geospatial Steering Committee, Bureau of Land Management, January 2016.

5. ***Data Advisory Committee Charter****:* Charter of the Data Advisory Committee, Bureau of Land Management, 2015.

6. ***FAC-P/PM****:* Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM), Office of Management and Budget, December 2013.

7. ***Contracting Guidance to Support Modular Development****:* Office of Management and Budget, June 2012.

8. ***Handbook for Procuring Digital Services Using Agile Processes****:* TechFAR, Office of Management and Budget, August 2014.

9. ***Assessing Risks and Returns****:* A Guide for Evaluating Federal Agencies' IT Investment Decision-Making, U.S. General Accounting Office, Accounting and Information Management Division, February 1997.

10. ***Bureau of Land Management's IT Security Plan***, Bureau of Land Management, April 2002.

11. ***Circular A-11****:* Preparation, Submission and Execution of the Budget, Office of Management and Budget, July 2016.
    a. ***Capital Programming Guide***, Office of Management and Budget, June 2006.
    b. ***Section 55 - Information Technology Investments***, Office of Management and Budget, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s55.pdf

12. ***Circular A-76****:* Performance of Commercial Activities, Office of Management and Budget, May 29th 2003.

13. ***Circular A-94****:* Discount Rates for Cost-Effectiveness, Lease Purchase, and Related Analyses, Office of Management and Budget, January 2015.

14. ***Circular A-127****:* Financial Management Systems, Office of Management and Budget, January 2009.

15. ***Circular A-130****:* Management of Federal Information Resources, Office of Management and Budget, July 28, 2016.

16. ***Citizen-Centered Governance****: Customer Value Through Accountability, Modernization, and Integration, Second Edition;* A Progress Report, DOI, October 9, 2002.

17. ***Clinger-Cohen Act of 1996*** (formerly the Information Technology Management Reform Act [ITMRA]).

18. ***Earned Value Management Systems*** *(EVMS) Basic Concepts*, Project Management Institute, Project Management Institute (PMI) Home Page

19. ***Executive Guide: Leading Practices in Capital Decision-Making***, U.S. General Accounting Office, Accounting and Information Management Division, December 1998.

20. ***Earned Value, Project Management,*** Fleming, Quentin W., Joel M. Koppelman**,** Second Edition, Project Management Institute, Inc., 2000.

21. ***Federal Information Technology Acquisition Reform Act (FITARA),*** Title VIII, Subtitle D of the National Defense Authorization Act (NOAA) for Fiscal Year 2015, Pub. L. No. 11 3-29, December 2014.

22. ***NIST SP 800-65 Integrating IT Security into the Capital Planning and Investment Control Process,*** *January 2005*

23. ***Principles of Engineering Economy,*** Grant, Eugene L., W. Grant Ireson**,** Fifth Edition, The Ronald Press Company, 1970.

24. ***Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*** (Exposure Draft), U.S. General Accounting Office, Accounting and Information Management Division, March 2004. http://www.gao.gov/new.items/d04394g.pdf

25. ***Smart Practices in Capital Planning***, The Federal CIO Council, Capital Planning and IT Management Committee, Industry Advisory Council (IAC), October 2000.