

Information Technology Governance Guide




August 2020

Version 8.0

U.S. Department of Justice
Information Technology Governance Guide

Signatures / Approvals

ROBERT
HOUSER

 Digitally signed by ROBERT
HOUSER
Date: 2020.09.17 09:04:55
-04'00'

Robert Houser
Assistant Director, Policy & Planning Staff
Office of the Chief Information Officer

September 17, 2020
Date

Action Log

Version Number	Date Approved	Approved By	Description of Changes
5.0	5/2008		Initial release of version 5.0
6.0	10/2014		<p>Added new sections:</p> <ul style="list-style-type: none"> • IT Performance Measurement section added • Added discussion and graphic on CPIC phases • Project Cost Estimating section added <p>Updated Existing Sections:</p> <ul style="list-style-type: none"> • Retitled Governance Framework section to Portfolio Management • Updated SDLC process and minimum mandatory artifacts list • Updated role and processes of DIRB and DIRC • Updated EA sections and processes • Stakeholder Model and Stakeholder Integration Matrix • Updated IT Oversight Model • Investment Lifecycle Model • System Development Lifecycle • Compliance Reviews • Executive Review Process • IT Planning and Budget Phases
7.0	9/16/2016		<p>Added new sections:</p> <ul style="list-style-type: none"> • OCIO Services Catalog section added • ITIL section added • Acquisition Compliance Review section expanded • Operational Analysis Review section added • Improved Portfolio Rationalization added to Investment Classification Model section • Appendix A – Acronyms • Appendix D – Workforce Management <p>Updated Existing Sections:</p> <ul style="list-style-type: none"> • Updated CIO role for consistency with FITARA requirements • Reorganization of DOJ oversight groups and roles; DPRB is now DIRC • Lifecycle Model • Stakeholder Model • SDLC Framework

U.S. Department of Justice
Information Technology Governance Guide

Version Number	Date Approved	Approved By	Description of Changes
			<ul style="list-style-type: none"> • Cost-Estimating Model • IT Oversight Model • Component Self-Governance Model • Updated Governance Phases • Privacy Compliance Review • Updated Cost/Schedule/Risk Review • Enterprise Architecture Review • Acquisition Compliance Review • Appendix C – Legislation & Regulatory Requirements
8.0	06/2020		<p>Removed references to inactive policy documents and updated language to incorporate more recent policy guidance</p> <p>Removed “Appendix C – Legislation & Regulatory Requirements”</p> <p>Removed references to eCPIC and replaced with FOLIO</p> <p>Added new Major IT Investment criteria</p> <p>Added language: EA team being part of PPS, the “Exhibit 53” becoming the IT Portfolio, and CISO participates in the DIRC Executive Review</p>

Table of Contents

1.	Introduction.....	11
1.1	Purpose.....	11
1.2	Goals	11
1.3	Background	12
1.4	Drivers.....	13
2.	Portfolio Management	14
2.1	Introduction to the Framework	14
2.2	Investment Life Cycle Model	15
2.2.1	Phases.....	16
2.2.2	Processes	18
2.2.3	Products.....	20
2.2.4	Value Chain	20
2.3	Stakeholder Model	21
2.3.1	Federal Oversight Groups	23
2.3.2	DOJ Oversight Groups.....	24
2.3.3	DOJ Office of the Chief Information Officer (OCIO).....	26
2.3.4	DOJ Partners	27
2.3.5	Component Partners.....	28
2.3.6	Integration Matrix	28
2.4	System Development Life Cycle (SDLC) Framework	30
2.5	Cost Estimating.....	35
2.5.1	Types of Government Cost Estimates.....	35
2.5.2	Cost Estimation Techniques	36
2.5.3	Cost Estimation Methodology	37
2.5.4	Cost Estimation Tools.....	38
2.6	Enterprise Performance Management (EPM)	38
2.7	Investment Classification Model	41
2.8	IT Oversight Model.....	44
2.9	Component Self-Governance Model	48
3.	Governance Phases and Processes	51
3.1	IT Planning Phase	51
3.1.1	IT Strategic Planning Process	53
3.1.2	Enterprise Roadmap Planning Process	53
3.1.3	IT Investment Planning Process.....	56
3.2	IT Budgeting Phase.....	59
3.2.1	Spring IT Budget Planning Process	60
3.2.2	Fall IT Budget Planning Process.....	63
3.2.3	OMB Passback IT Budget Review Process	69
3.2.4	Congressional Budget Review Process.....	73
3.2.5	Information Technology Infrastructure Library.....	77
3.3	IT Oversight Phase.....	78
3.3.1	Executive Review Process	79
3.3.2	Compliance Review Process.....	85
3.3.3	IT Performance Measurement.....	99

U.S. Department of Justice
Information Technology Governance Guide

Appendix A – Acronyms	104
Appendix B – Definition of IT for DOJ.....	107
Mission Delivery and Business Solutions	107
Core Functions	107
Support Functions	108
IT Infrastructure	109
IT Practices and Management.....	110
Appendix C – Workforce Management.....	112
Component CIOs	112
Workforce Knowledge & Skills	112

List of Figures

Figure 2-1: DOJ Investment Life Cycle Model Layered Over the CPIC Life Cycle	16
Figure 2-2: IT Governance - Investment Life Cycle Model.....	18
Figure 2-3: IT Governance Stakeholder Model.....	23
Figure 2-4: IT Governance Stakeholder Model - DOJ Oversight Groups.....	24
Figure 2-5: Federal Oversight - IT Governance Integration Matrix.....	29
Figure 2-6: Departmental and Domain Oversight - IT Governance Integration Matrix.....	29
Figure 2-7: Service/Program/Project Execution - IT Governance Integration Matrix	30
Figure 2-8: SDLC Minimum Deliverables	32
Figure 2-9: Enterprise Performance Management.....	39
Figure 2-10: Investment Classification Model	43
Figure 2-11: IT Oversight Model	46
Figure 2-12: Component Self-Governance Model	49
Figure 3-1: IT Planning Phase	52
Figure 3-2: DOJ EA Structured Approach	54
Figure 3-3: Enterprise Roadmap Timeline	55
Figure 3-4: IT Investment Planning Process Summary.....	56
Figure 3-5: IT Investment Planning Process Diagram	57
Figure 3-6: IT Budget Phase.....	59
Figure 3-7: Spring IT Budget Planning Process Summary.....	60
Figure 3-8: Spring IT Budget Planning Process Diagram	61
Figure 3-9: Fall IT Budget Planning Process Summary	64
Figure 3-10: Fall IT Budget Planning Process Diagram	65
Figure 3-11: OMB Passback IT Budget Review Process Summary	70
Figure 3-12: OMB Passback IT Planning Process Diagram	71
Figure 3-13: Congressional Budget Review Process Summary	74
Figure 3-14: Congressional Budget Planning Process Diagram.....	75
Figure 3-15: IT Oversight Phase	79
Figure 3-16: IT Governance - Executive Review Process.....	81
Figure 3-17: Executive Review Process Diagram	82
Figure 3-18: Compliance Reviews	85
Figure 3-19: Example Data Calls	101

U.S. Department of Justice
Information Technology Governance Guide

1. Introduction

1.1 Purpose

The purpose of this guide is to communicate the procedures to stakeholders involved in the execution and oversight of the Department's Information Technology (IT) investments, programs, and initiatives. This guide is a companion document to the Department of Justice (DOJ) *Order 0903 Information Technology Management*, and its underlying Policy Statements, that authorize the governance procedures described herein.

As specified in the Clinger Cohen Act of 1996, and further emphasized in the Federal Information Technology Acquisition Reform Act (FITARA) of 2014¹, responsibility for the governance of the Department's IT investments resides primarily with the Department's Chief Information Officer (CIO), working in concert with the Department's Chief Financial Officer (CFO) and with the Department's Senior Procurement Executive (SPE). Key stakeholders include the Office of the Chief Information Officer (OCIO), the Department's Budget and Procurement Services Staffs, component CIOs, the component business leaders who invest and oversee IT at component and Offices, Boards, and Divisions (OBDs) levels, and the component's respective budget and procurement offices. Section 2.3 provides a more extensive list of stakeholders.

Governance of IT investments is a multi-layer framework. In addition to governance at the CIO level, this guide also communicates the Departmental component/OBD self-governance and reporting requirements of the Department entities that directly manage IT services or investments. This guide communicates Departmental IT governance practices to external oversight organizations, such as the Office of Management and Budget (OMB), the Government Accountability Office (GAO), Congress, and the Department's Office of the Inspector General (OIG).

1.2 Goals

IT has an important and powerful role to advance, protect, and serve the Department of Justice's core objective, protecting the American people.² IT at the Department supports wide and diverse missions and goals and is composed of three broad categories: mission-delivery and business solutions; IT infrastructure; and IT practices and management. This IT Governance Guide supports the achievement of the Department's IT governance program goals:

- Inform and influence Department and component IT investment decisions to ensure that allocated IT resources are efficiently used to support the Department's missions and goals, and continuously deliver and improve upon expected performance results.
- Satisfy statutory and regulatory IT management requirements.

¹ Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, further referenced in this text as FITARA (Pub. L. 113-291)

² Department of Justice Strategic Plan for Information Services and Technology, Fiscal Years 2015-2018

1.3 Background

Federal legislative mandates have steadily increased the oversight and reporting requirements for acquisition and management of IT resources at the department level, most recently with FITARA. FITARA requires that the agency CIO have a significant role in managing IT investments and it expands the definition of IT resources to include all agency budgetary resources, personnel, equipment, facilities, services, acquisitions, and interagency agreements that include IT services and equipment.³

Subsequent to the passage of FITARA, OMB issued memorandum M-15-14, which provides implementation guidance, including specific investment review, oversight and reporting requirements agencies must incorporate into governance and management processes.

OMB Memorandum M-15-14 defines information technology as follows:

- IT includes 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.
- Services and equipment are “used” if used directly by the agency itself, or if used by a vendor under a contract with the agency.
- The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.
- The term “information technology” does not include any equipment that is acquired by a vendor/contractor incidental to delivering goods/services under the terms and conditions of a contract.

The Clinger-Cohen Act, FITARA, and other legislation and policy identify the Department CIO as the incumbent responsible for monitoring and managing the performance of Department IT investments and for advising the Attorney General (AG) when ongoing investments should be modified, replaced, or terminated. To comply with legislation and policy, the Department’s OCIO has developed and implemented an integrated IT governance process that maximizes value and assesses and manages risks associated with acquisition and management of IT investments. The Department’s governance efforts concentrate on improving IT portfolio planning, investment selection, and investment oversight throughout the investment’s life cycle.

Three of the four OCIO staffs administer the CIO’s IT governance responsibilities. The Policy and

³ OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology

Planning Staff (PPS) is responsible for facilitating and coordinating IT portfolio planning and investment selection, reporting on the overall health and compliance of investments, and performing program oversight reviews. The Service Delivery Staff (SDS) and Cybersecurity Services Staff (CSS) are responsible for communicating IT-related guidance, as well as identifying, planning, and designing common enterprise-wide solutions. CSS is also responsible for establishing and administering cybersecurity policy, guidance, and compliance across the Department. SDS is also responsible for providing a wide range of customer-facing IT services, including common desktop, remote and mobility services, telecommunications, and IT infrastructure-related services, among others.

1.4 Drivers

There are four main drivers for the Department's IT governance program: legislative requirements and oversight, DOJ mission needs, audit findings and recommendations, and the use of shared services and commodity IT across the DOJ enterprise. A comprehensive list of authorities can be found in *DOJ Order 0903 Information Technology Management*.

- **Legislative Requirements and Oversight:** Four oversight bodies monitor the Department's implementation of legislative and regulatory requirements and provide guidance based on best practices. These agencies are OMB, GAO, Congress, and the DOJ OIG.
- **DOJ Mission Needs:** Internal drivers primarily come from two sources: the Offices of the Attorney General and Deputy Attorney General in the form of strategic mission and business priorities aligned with the Department's strategic plan, and the Department CIO in the form of strategic IT goals and priorities aligned with the Department's IT strategic plan. These goals and priorities set forth in these strategic plans serve as criteria for investment selection and budget decisions in the planning and budget phases of the IT investment life cycle.
- **Audit Findings and Recommendations:** Audits of the Department's IT programs and investments by GAO and OIG may identify weaknesses in management practices and with policies that require revisions. Improvements to IT policies, practices, and management processes implemented to address recommendations from an audit must be officially documented. This guide serves as a resource to implement or otherwise revise Department policies for IT governance processes and procedures.
- **Shared Services and Commodity IT:** The growth in the use of shared services and commodity IT across the Department, and in government as a whole, has driven many changes to IT governance. With the implementation of IT PortfolioStat in 2012, the Department is required to monitor and report spending on commodity IT to OMB on a regular basis. Establishing shared services and contracts throughout the Department is an important goal for reducing cost and increasing efficiency in the enterprise environment.

2. Portfolio Management

IT portfolio management is the application of systematic management practices applied to the Department's enterprise IT investments, projects, and activities in order to better analyze, select, and manage project investments and ensure they remain aligned with the Agency's mission, goals, and objectives. The goal is to increase the value proposition of the Department's IT portfolio in its support of mission and business priorities by selecting the best initiatives serving the broadest community for investment. Key benefits include improved return on investment (ROI), reduced development costs, improved customer satisfaction, and increased compliance. IT portfolio management allows the Department to provide continuous oversight and decision-making support about which initiatives to undertake, which to continue, and which to discontinue or otherwise not approve.

In order to ensure that the proper results are achieved from the use of IT portfolio management, the Department CIO has delegated authority, created entities/functions, developed and implemented policies and practices, defined and filled roles and responsibilities, and identified decision-making rules and powers. The Department has organized its IT portfolio according to an investment classification model, described in detail in Section 2.7, Investment Classification Model. All of these IT business management elements collectively make up the Department's portfolio-management governance framework.

2.1 Introduction to the Framework

IT governance is the practice of planning and managing the Department's IT resources through a related set of managed processes. The governance framework provides the context and structure for binding together the cogs of the various governance processes so that they operate as a well-oiled machine. The framework consists of eight models that together provide the structure linking the moving parts of the entire governance process.

- **Investment Life Cycle Model** integrates the investment life cycle processes through the movement of standard products from one process to the next. The sequence of governance processes along which investments progress must begin at strategic inception, through reviewed operations, to delivery and final disposition.
- **Stakeholder Model** identifies the stakeholders (persons, groups, committees, and organizations) that play significant roles in the Department's IT governance processes and demonstrates how these stakeholders participate in the life cycle by relating each to processes and products.
- **System Development Life Cycle (SDLC) Framework** provides a standard approach for completing key planning processes necessary for the orderly and effective development and implementation of information technology systems, and identifies a minimum set of required artifacts to provide visibility and rigor into the development process.

- **Cost Estimation Framework** provides methods and standards to predict future capital expenditures even if not all factors and conditions of the investment are fully defined. The framework is useful for preparing the annual budget, determining return on investment estimates, informing the analysis of alternatives discussion, and improving the life cycle management of investments.
- **Enterprise Performance Management (EPM) Framework** describes a standard approach for measuring investment performance in meeting mission / business needs across the IT portfolio.
- **Investment Classification Model** provides a standard structure for categorizing investments for analysis and oversight.
- **IT Oversight Model** provides a structure for integrating DOJ tiered oversight reviews under a unified governance structure.
- **Component Self-Governance Model** identifies the self-governance actions components must perform to manage their agency-specific IT assets.

These eight models provide the structure for integrating the various aspects of IT governance throughout the Department. Later in this chapter, two example investments will illustrate how these models relate to one another, as well as how each model applies to the management of individual IT investments. The examples are Investment A, addressing a common business need for several components, and Investment B, which addresses a unique business need for a single component.

2.2 Investment Life Cycle Model

The Investment Life Cycle Model is the backbone of the governance framework of IT investment portfolio management, and is built on the foundation of the Capital Planning and Investment Control (CPIC) Life Cycle. It provides an end-to-end iterative sequence of processes for managing IT investments. The life cycle processes in the model are integrated via the logical and repeatable progression of IT management products from one process to the next, while providing for periodic feedback to support the iterative cycle of planning, budgeting, and oversight that recurs each fiscal year.

Different stakeholders are involved in directing, producing, reviewing, and using the products developed by each process, so the success of the model relies on its ability to define the products produced in one process and passed onto another for further processing. Example Investments A and B, as well as all other investments in the Department's IT portfolio, are managed through these processes.

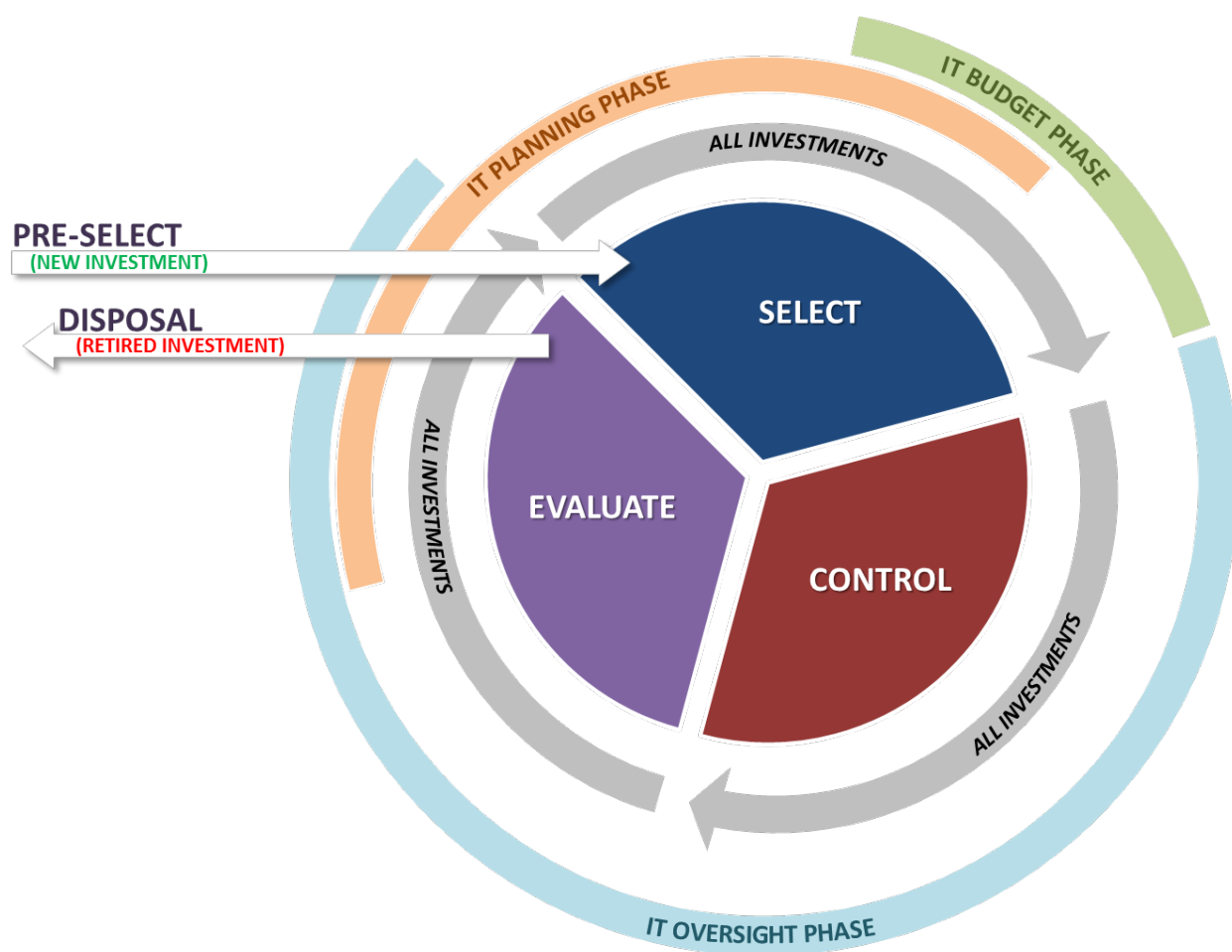


Figure 2-1: DOJ Investment Life Cycle Model Layered Over the CPIC Life Cycle⁴

Figure 2-1 depicts the full DOJ Investment Life Cycle Model layered over the CPIC Life Cycle. To explain the model, its components have been broken down and individually described below.

2.2.1 Phases

The CPIC Life Cycle consists of three phases: Select, Control, and Evaluate. These phases are grounded in the Investment Life Cycle Model developed by GAO.

- **Select Phase** is used to determine priorities and make decisions about which investments (new and ongoing) should be funded and included in the IT portfolio.

⁴ The DOJ Investment Life Cycle Model and phases were developed based on the model in the [GAO Information Technology Investment Management Assessment Framework](http://www.gao.gov) (www.gao.gov)

- **Control Phase** is used for ongoing management and monitoring of investments against projected cost, schedule, performance, and expected mission benefits.
- **Evaluate Phase** is used to measure actual versus expected results in order to (1) assess the investments' impact on strategic performance; (2) identify any necessary corrective actions that must be taken for investments; and (3) revise investment management processes based on lessons learned, self-assessments, and benchmarking.

As DOJ evolved the CPIC Life Cycle into its own Investment Life Cycle Model, two additional phases were added to the life cycle: Pre-Select and Disposal.

- **Pre-Select Phase** covers new initiatives that are pre-screened for investment. Once they are approved through pre-selection, they are then added to the pool of investments that go through the Select phase in order to be considered for inclusion in the DOJ IT portfolio.
- **Disposal Phase** covers existing investments that have been evaluated and selected for elimination and go through the process of being removed from the IT portfolio.

To complete the DOJ Investment Life Cycle Model, the investment life cycle phases – IT Planning Phase, IT Budget Phase, and IT Oversight Phase – were arrayed in alignment with the CPIC life cycle phases – Select, Control, and Evaluate (see Figure 2-1). Each are supported by the models and frameworks previously described in Section 2.1, Introduction to the Framework.

- In the **IT Planning Phase**, the Department CIO defines the Department's strategic IT direction, the transition strategies for moving forward, and the investment priorities for the future.
- In the **IT Budget Phase**, the Department CIO defines the Department's IT investments needed to achieve the Department's IT strategic goals and supports those both internal and submitted by components for approval and funding via the budget formulation process.
- In the **IT Oversight Phase**, the Department monitors the development and on-going operations of the Department's investments to ensure that performance objectives are and continue to be achieved.

Each IT investment life cycle phase consists of three elements: processes, products, and the resulting value chain. Figure 2-2 depicts the linear breakout of each IT investment life cycle phase.

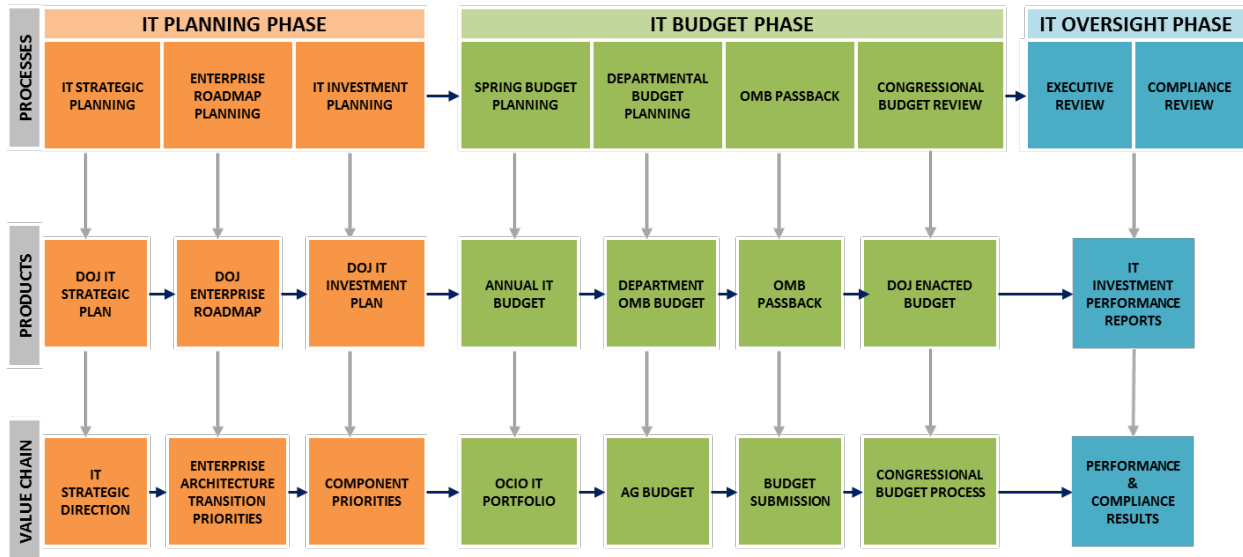


Figure 2-2: IT Governance - Investment Life Cycle Model

2.2.2 Processes

The processes associated with each governance phase are shown in the top row of Figure 2-2. More detailed information on these processes can be found in Section 3.

- IT Strategic Planning Process:** The DOJ OCIO examines the current state of the Department's IT enterprise and its support of Department missions, goals, and objectives; determines and defines IT strategic goals and programs; assigns priorities, performance goals, indicators and metrics; and produces the Department's IT Strategic Plan.
- Enterprise Roadmap Planning Process:** The DOJ OCIO creates a mid-term plan to drive current IT investment decisions for the Department. The Department's Enterprise Roadmap is developed during this process based on the following: mission and business goals outlined in the DOJ Strategic Plan; the goals, priorities, and actions identified in the IT Strategic Plan; and input from DOJ components, including the CIO Council, and from OCIO Staffs.
- IT Investment Planning Process:** Prior to the formal Spring Call budget guidance, the OCIO issues its IT budget planning guidance wherein component CIOs are asked to identify their IT investment plans for the coming budget cycle, including identifying and prioritizing IT investments based on mission and business priorities from their component operational and business leaders, and based on the Department's Strategic Plan and the IT Strategic Plan.
- Spring Budget Planning Process:** Based on the CIO's IT investment priorities for the coming budget cycle, components use internal IT Investment Management (ITIM) selection processes and the Department's Spring Call and IT investment planning guidance to prepare budget requests. Requests for IT enhancements are evaluated and the CIO can make informed

decisions and recommendations on IT-related requests in direct support of the Department's internal budget formulation activities.

- **Departmental Budget Planning Process:** DOJ senior leadership reviews the IT-related funding recommendations forwarded by the CIO and selects IT investments that are to be included in the Department's budget request to OMB.
- **OMB Passback:** OMB reviews the Department's budget request for incorporation into the President's Budget. OMB makes its prioritized decisions passes it back to the Department providing opportunity for the Department to submit its appeal on any of OMB's initial decisions. For any IT-related matter, the CIO fully participates in all discussions relative to the Department's appeal response to OMB. With final decisions issued by OMB, the Department budget is packaged for inclusion in the President's Budget transmittal.
- **Congressional Budget Review Process:** Congress reviews the President's Budget request, during which the CIO may be required to answer IT-related questions on programs and IT priorities. The Congress enacts budget legislation to fund federal government operations for the coming fiscal year.
- **Executive Review Process:** The Department Investment Review Board (DIRB) serves as the Department's top-level IT Review/Oversight Board, chaired by the Deputy Attorney General, and which is responsible for setting the strategic direction of the Department's IT program, prioritizing enterprise investment initiatives, and monitoring the largest IT programs exceeding \$100 million or more on new capabilities. Complementing this body, the Department Investment Review Council (DIRC), chaired by the Department's CIO, conducts periodic executive level reviews for the Department's most critical IT programs. These programs require executive level oversight due to their high cost, high risk, or high visibility, or they require specific review to comply with legislative requirements. Components perform equivalent reviews for their programs, projects, and resulting services at more in- depth levels and the CIO continuously engages component CIOs on these activities.
- **Compliance Review Process:** The compliance review process determines how well investments conform to Department and federal IT policies and standards. All IT investments are subject to review, most of which occur at the component level but may be conducted at the Department level, as well. Compliance reviews may occur in both the development and the operations and maintenance phases (O&M) of an investment's life cycle. Compliance managers conduct reviews for each compliance area throughout the fiscal year ensuring specific reporting requirements are being achieved.

2.2.3 Products

The second element of the Investment Life Cycle Model is the set of products that are the outputs of the governance processes. The products, in the middle row of Figure 2-2 (P.9), contain the information output from each process, which are also used as informational input into other processes.

- **DOJ IT Strategic Plan** defines the Department's three to five year strategic goals and objectives for how IT resources will support the Department's missions.
- **DOJ Enterprise Roadmap** describes the tactical approach for moving the Department's IT enterprise from its current architecture to the targeted architecture to support the IT strategic goals and priorities described in the IT Strategic Plan.
- **Annual IT Budget planning** represents component-identified IT investment priorities. This information is submitted to the OCIO and reviewed for strategic alignment with Department-level IT investment priorities. This process supports the Annual Spring Call budget formulation process as it provides a list of all IT investments formally requested by components for the upcoming budget cycle for review by the Department CIO and the JMD Budget Staff.
- **Department OMB Budget** submission is an update of the Spring Call budget reflecting the AG's final budget and program priorities.
- **OMB Passback** represents the Administration's budget and policy priorities. OMB reviews the Department budget request and renders its decision in late fall. The Department is given opportunity to appeal. The outcome of these negotiations represents what will be transmitted as part of the President's Budget Request to Congress.
- **DOJ Enacted Budget** is the budget enacted by the Congress, which results in appropriated funding for any IT investments requested or otherwise deemed a priority of various key stakeholders.
- **IT Investment Performance Reports** are the various reports prepared by project managers (PMs), components, and oversight groups that describe the progress and performance of the investments, as well as the investments' compliance with Department IT policy and federal regulation and law.

2.2.4 Value Chain

The final element of the Investment Life Cycle Model is the value chain, represented at the bottom of Figure 2-2 (P.9). The value chain represents the business outcomes that result from each process.

- **IT Strategic Direction:** The IT Strategic Direction is driven by the mission, vision, goals, and objectives of the Department and is defined in the DOJ IT Strategic Plan.
- **Enterprise Architecture (EA) Transition Priorities:** The EA Transition Priorities are

defined in the DOJ Enterprise Roadmap. They describe the approach the Department is taking to move its enterprise IT from the current state to a future state that aligns with the IT strategic direction of the organization.

- **Component Priorities:** The component CIOs identify their IT priorities for the coming budget cycle, including defining current IT investment needs, based on mission and business priorities from their component business leaders and from the Department's Strategic Plan, IT Strategic Plan, and IT budget planning guidance. This document should note both critical existing investments as well as new investments for the component. The components submit their IT investment plans to the Department CIO via the winter IT Budget Guidance planning call to provide situational awareness on IT-related investments/prospective enhancement requests that may be part of the components Spring Call submission. The IT portfolio summary serves as the component's IT investment plan.
- **OCIO Proposed IT Portfolio:** Once the component IT investment plans are received, they are reviewed by OCIO staff for adherence to the strategic direction the Department CIO is leading. This also serves an educational purpose, as the CIO is better able to support/defend component IT requests submitted to JMD Budget Staff as part of the Spring Call.
- **AG Proposed Budget:** As part of the budget planning process, DOJ senior leadership reviews the recommendations forwarded by JMD Budget Staff that may include IT budget enhancement recommendations.
- **Budget Submission:** Any approved IT investments selected for inclusion in the Department's OMB budget request are included in the official Department transmittal. OMB makes its decisions on the overall request and provides the passback package returning its decisions to the Department. This package details the changes/updates that must be made to the Department's budget prior to its inclusion in the President's Budget. Any changes/updates to IT investment funding requests may be appealed and negotiated for final disposition.
- **Congressional Budget Process:** The Congress reviews the Department's budget request and works with the Department on prioritizing enhancement requests, including IT enhancements. Enhancements selected and approved by Congress become part of the enacted Departmental appropriation.
- **Performance and Compliance Results:** After appropriated funds are received by the Department, they are allotted for the specified investment. These new/continuing program investments are monitored through a variety of reporting and review processes to ensure that planned performance is achieved.

2.3 Stakeholder Model

The IT Governance Stakeholder Model identifies key stakeholders (persons, groups, committees, organization), that play a role in the Department's IT governance processes. These stakeholders participate at various stages of the Department's IT Governance Framework, including in the

Investment Life Cycle. As with each investment in the Department's IT Portfolio, Investments A and B (previously explained) will interact both directly and indirectly with many of these stakeholders throughout their life cycles.

Six key stakeholder groups:

- **Federal Oversight Groups** include external organizations who oversee the Department's IT investments and its governance activities.
- **DOJ Oversight Groups** include the review boards, councils and committees who govern the Department's IT investment activities.
- **DOJ Office of the CIO (OCIO)** includes staff organizations under the Department CIO that are responsible for managing the Department's IT investment management programs.
- **DOJ Partners** are the Department-level persons and organizations outside the DOJ OCIO who participate in or influence IT investment planning and management.
- **Component Partners** are the people and organizations within components responsible for performing or participating in IT investment management processes.
- **DOJ End Users** are the customers for which OCIO services are made available. They are the final or ultimate users of the technology after it has been fully developed/deployed.

The stakeholder groups shown in Figure 2-3 are described in subsequent sections.

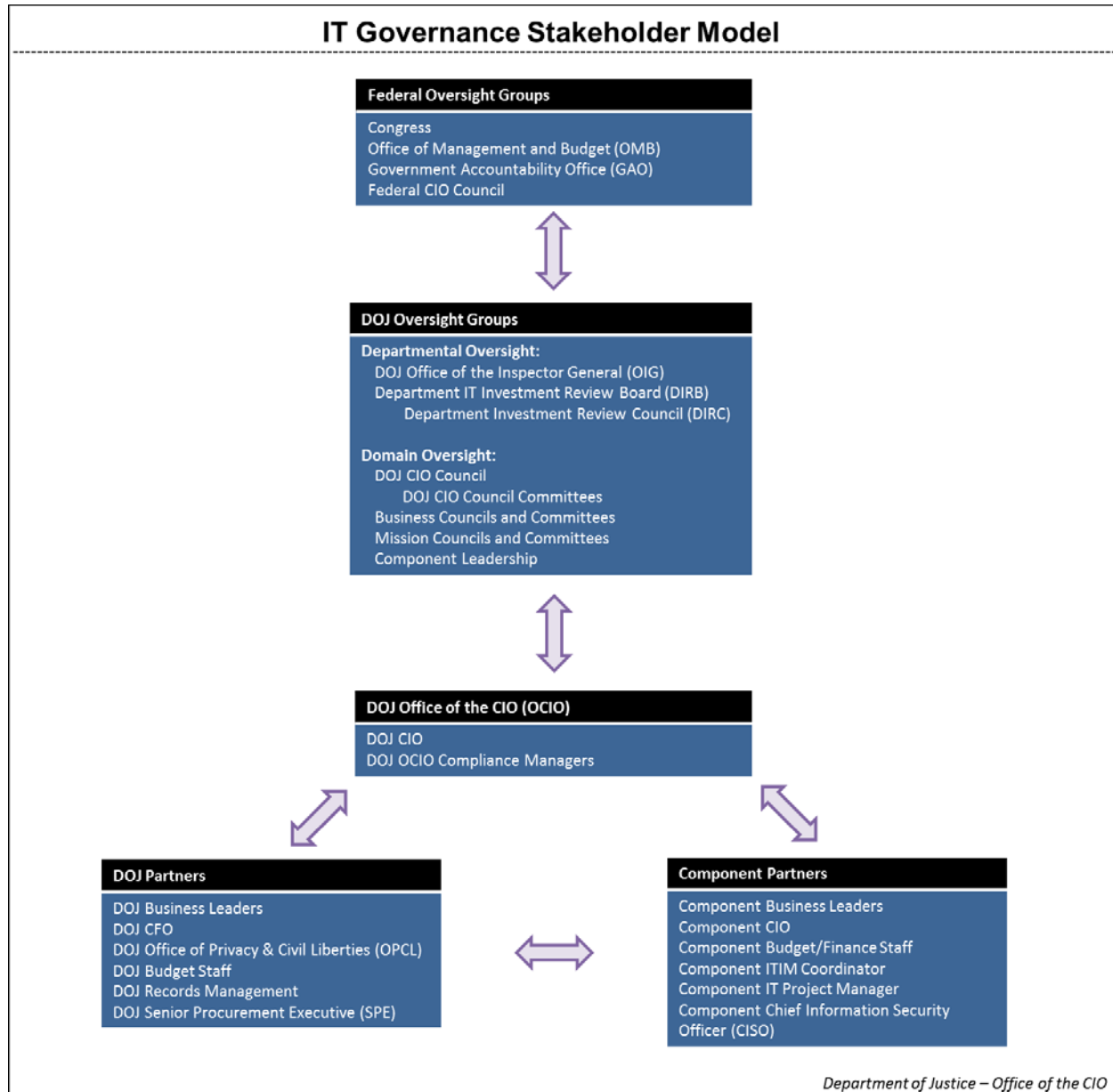


Figure 2-3: IT Governance Stakeholder Model

2.3.1 Federal Oversight Groups

- **Congress:** The legislative branch defines, authorizes, and oversees the Department's operations through authorization (Judiciary Committees of the House and Senate) and the appropriations process. Congress may also periodically review the Department's IT program or the development and performance of selected high profile IT investments.

- **Office of Management and Budget (OMB):** As part of the Executive Office of the President, OMB performs oversight of executive branch IT investments to ensure compliance with federal laws and administration policy. OMB prepares the President's budget for presentation to the Congress with its recommendations on funding levels for IT investments.
- **Government Accountability Office (GAO)** audits executive branch agencies and programs for compliance with Federal laws, policies, and best practices on behalf and at the request of the Congress. IT governance practices and IT investment selection and management are subject to GAO audit.
- **Federal CIO Council** serves as the principal interagency forum on federal agency practices for IT management. The Council's mission is to improve practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal government information resources. The Council's role includes developing strategies to support IT innovation; developing recommendations for information technology management policies, procedures and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the federal government's IT workforce.

2.3.2 DOJ Oversight Groups

Within DOJ there are departmental and domain oversight groups. Service/program/project execution includes varied participation from all Department stakeholders.

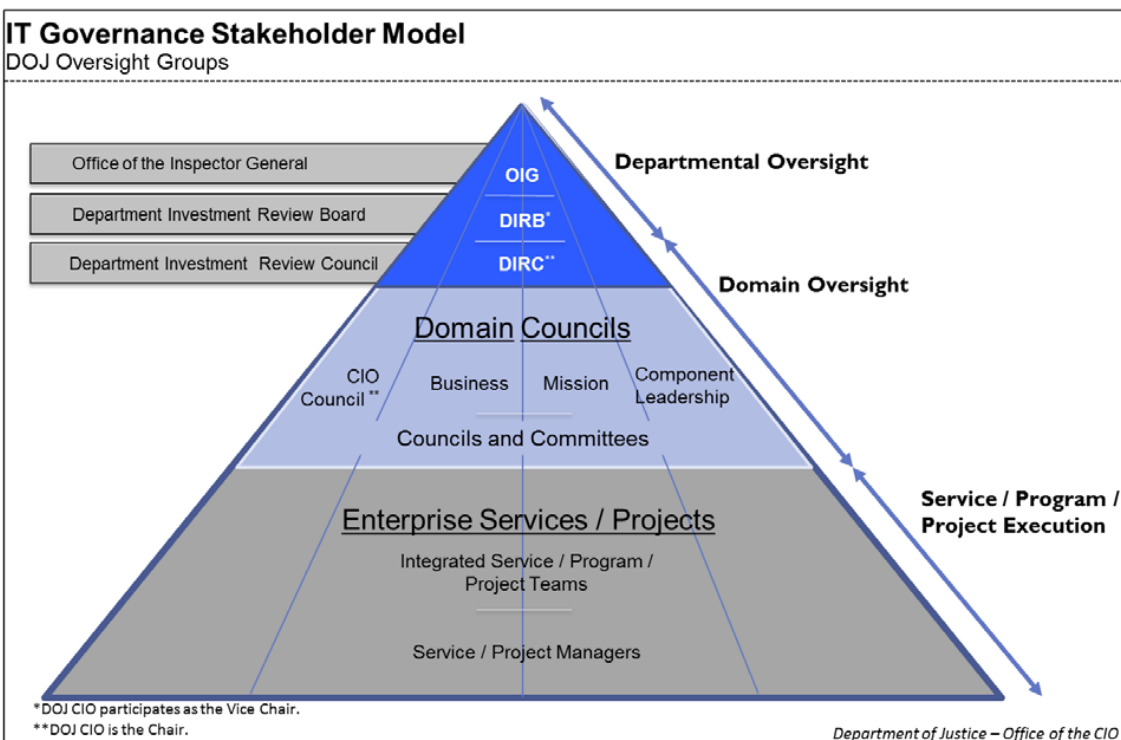


Figure 2-4: IT Governance Stakeholder Model - DOJ Oversight Groups

Departmental Oversight Groups

Governance bodies composed of senior executives with oversight and advisory responsibilities of IT investments.

- **DOJ Office of the Inspector General (OIG)** is the Department's internal audit organization and is responsible for reviewing IT processes and investments to ensure compliance with best practices, federal regulations and Department policies.
- **Department IT Investment Review Board (DIRB)** is the executive body responsible for setting strategic direction of the Department's IT portfolio, prioritizing enterprise investment initiatives, and monitoring the largest IT programs that exceed \$100 million or more on new capabilities. The DIRB oversees the development, implementation, and operation of the DOJ-wide CPIC function. The DIRB is chaired by the Deputy Attorney General (DAG) and the membership includes the Deputy Assistant Attorney General/Chief Information Officer (CIO) – who serves as Vice Chair, the Chief Financial Officer (CFO) (Assistant Attorney General for Administration), Deputy Assistant Attorney General/Controller, and on a rotating basis designated by the Chair, component CIOs and three other senior executives.
- **Department Investment Review Council (DIRC)** is a committee of the DIRB that provides direct monitoring, oversight, and facilitation for the success of the Department's major IT program investments. Major IT investments include any project with CY DME spend greater than or equal to \$10M (or 15% of total component budget for OBD components) with DME spend spanning 2 or more future years, or greater than or equal to \$50M over 5 years. The DIRC is chaired by the Department CIO and membership includes the DOJ Controller – who serves as the Vice Chair, the Senior Procurement Executive, Chief Human Capital Officer (CHCO), Chief Technology Officer (CTO), Chief Information Security Officer (CISO), an Offices, Boards, and Divisions (OBDs) representative, and three component CIOs.

Domain Oversight Groups

These committees and individuals are comprised of executive stakeholders responsible for providing strategic direction and oversight of large common solution IT investments.

- **DOJ CIO Council** is a Department-wide governance body chartered and chaired by the DOJ CIO and composed of the CIOs from the Department's components. The CIO Council is the principal internal Department forum for addressing DOJ information resource management priorities, policies, and practices. The CIO Council provides oversight and serves as a mechanism for coordinating and facilitating implementation of Department-wide processes and standards, and for addressing common issues affecting component IT programs and resources. The Council meets monthly to review progress on strategic goals and to advise the DOJ CIO on IT management issues: identifying strategic goals and defining strategies for achieving goals; improving Department practices related to design, acquisition, development, modernization, use, sharing, and performance of agency information resources; promoting efficient and effective use of information resources; and supporting proven methodologies to achieve measurable increases in productivity and performance.

- **DOJ CIO Council Standing Committees** are in place to provide guidance and oversight on all major technology domains and major initiatives. Committees provide recommendations on governance practices and processes for initiatives and priorities within their respective domains and ensure alignment among components. The Council committees provide regular updates to the DOJ CIO Council. Committees are chaired by a component CIO; membership includes representation from the DOJ CIO Council, DOJ OCIO, and technical and business subject matter experts (SMEs).
- **Business Councils and Committees** are comprised of executive stakeholders responsible for providing strategic direction and oversight of large, common-solution enterprise business services (e.g. human resources (HR), acquisition, finance, property/facilities, grant management, and IT investments). Supporting committees include, but are not limited to, the Unified Financial Management System (UFMS) executive committee.
- **Mission Councils and Committees** are comprised of executive stakeholders, appointed by department and component leadership, responsible for providing strategic direction and oversight of large common solution mission IT investments. Supporting committees include, but are not limited to, the Law Enforcement Information Sharing Program (LEISP) Steering Committee, the Joint Automated Booking System (JABS) Steering Committee, the Wireless Communications Board, and the Law Enforcement Coordinating Council (LECC).
- **Component Leadership** actively participates or are represented within other DOJ oversight groups. Component CIOs are members of the DOJ CIO Council and appoint the members for the DOJ CIO Council standing committees, business councils and committees, and mission council's and committees.

2.3.3 DOJ Office of the Chief Information Officer (OCIO)

- **Department of Justice Chief Information Officer (DOJ CIO)** concurs with the component head in the appointment of component CIOs, sits on component investment review boards, and is responsible for the acquisition and management of the Department's IT resources. This includes reviewing IT investments and acquisition plans as part of CPIC and program oversight processes required by FITARA. FITARA also mandates CIO review of the annual DOJ IT budget request, including the proposed allocation of all Department resources that may be devoted to IT, contracts or other arrangements for acquiring IT or IT services, and requests for reprogramming funds to be allocated to IT programs. The incumbent provides advice to the Deputy Attorney General and the Attorney General on all matters pertaining to IT.
- **DOJ OCIO Compliance Managers** are staff members from each of the OCIO staffs responsible for one or more IT compliance review processes, such as project management, enterprise architecture, security, privacy, etc. Compliance managers supervise the review processes and guarantee their integration into the IT investment life cycle.

- **DOJ Chief Information Security Officer (CISO)** is responsible for setting the Department's IT Security policy and monitoring programs and projects for compliance. The CISO oversees the activities of the Cybersecurity Services Staff, which is responsible for daily IT Security operations within the Department.

2.3.4 DOJ Partners

- **DOJ Business Leaders** are the non-IT Department and component executives and mission program managers who define mission and business priorities and rely on IT systems and services for the successful accomplishment of those missions and programs. The business leaders drive IT planning for the Department through the goals and objectives of the DOJ strategic plan and annual performance plan.
- **DOJ Chief Financial Officer (CFO)** participates in IT governance as a voting member of the DIRB and as the principal Department executive responsible to the Attorney General for overseeing the formulation and execution of the Department's budget.
- **DOJ Office of Privacy and Civil Liberties (OPCL)** is part of the Office of the Deputy Attorney General. The OPCL mission is to protect the privacy and civil liberties of the American people by reviewing and overseeing the Department's privacy operations, and ensuring that the Department complies with federal privacy statutes, including the Privacy Act of 1974. The primary role of the OPCL in IT governance is the review and approval of IT systems Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).
- **JMD Budget Staff** is part of the Chief Financial Officer's (CFO) organization, and oversees the budget formulation process for submission to OMB and subsequently the Congress. IT investments represent a subset of the overall Department budget and it is through the annual Spring budget data calls that IT investment requests are collected and reviewed by the CIO, representing a key partnership with the JMD Budget Staff.
- **DOJ Office of Records Management Policy (ORMP)** assures the fair and impartial administration of justice through records management that preserves the essential evidence of DOJ functions, policies, and actions. Federal records include all books, papers, maps, photographs, machine-readable materials, or other documentation such as email records. The ORMP also oversees the review of Records Information Management (RIMCert) applications and ensures all programs and projects comply with records management policies.
- **DOJ Senior Procurement Executive (SPE)** is responsible for establishing policies and procedures relating to all Departmental procurement and acquisition activities.

2.3.5 Component Partners

- **Component Business Leaders** define the business priorities for each component, collaborate with the component CIO to select and prioritize IT investments during the component's annual budget process, and participate in the oversight of key component investments to ensure that results are achieved.
- **Component Chief Information Officer (CIO)** is the senior IT leader within each component responsible for overseeing the application and improvement of IT to support the component's mission(s) and for verifying the accuracy of investment cost information. Though primarily responsible for the successful management of IT programs within their respective components, component CIOs also serve as members of the DOJ CIO Council, acting as advisors to the DOJ CIO on cross-component issues ranging from IT policy and strategic planning to technology and acquisition coordination. Component CIOs are appointed by the component head with the concurrence of the Department CIO, and are identified in organization charts regularly provided to Department HR staff and posted on component internal webpages.
- **Component Budget/Finance Staff** prepares and manages the component's budget working closely with the component ITIM coordinator to ensure that IT budget information is accurately reflected within the component's overall budget.
- **Component ITIM Coordinator** acts as the liaison between the DOJ OCIO and the component IT project managers to ensure completion of all component ITIM activities and delivery of required component ITIM products.
- **Component IT Project Manager** provides reports and other information on their IT projects in response to Department data calls.
- **Component Chief Information Security Officer (CISO)** is the senior information security manager within each component with responsibility for establishing, overseeing, and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are secured and remain protected.

2.3.6 Integration Matrix

The Integration Matrix on the following page aligns the IT governance stakeholders described on the preceding pages with the phases and processes of the IT Investment Life Cycle. Using the matrix, stakeholders can quickly determine in what part of the process they are involved over the course of the IT Investment Life Cycle.

The matrix is divided into three separate parts associated with the different stakeholder groups: federal oversight, departmental and domain oversight, and service/program/project execution. The stakeholders are listed down the left-most column. The IT Investment Life Cycle phases and processes are shown sequentially across the top. In the body of the matrix, check marks are used to show in which phases and processes each stakeholder participates. Figure 2-5 shows the participation of federal oversight stakeholders in DOJ's governance phases and processes.

IT Governance Integration Matrix									
Federal Oversight: Processes, Stakeholders, & Products									
IT Governance		IT PLANNING PHASE			IT BUDGET PHASE			IT OVERSIGHT PHASE	
Phases		IT Strategic Planning Process	EA Roadmap Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Review Process	Congressional Budget Review Process	
Processes									
STAKEHOLDERS									
Federal Oversight	Congress							✓	
	OMB		✓		✓	✓	✓	✓	✓
	GAO*								✓
	*Federal Oversight is situational								

Figure 2-5: Federal Oversight - IT Governance Integration Matrix

Figure 2-6 shows the participation of departmental and domain oversight stakeholders in DOJ's governance phases and processes.

IT Governance Integration Matrix									
Departmental and Domain Oversight: Processes, Stakeholders, & Products									
IT Governance		IT PLANNING PHASE			IT BUDGET PHASE			IT OVERSIGHT PHASE	
Phases		IT Strategic Planning Process	EA Roadmap Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Review Process	Congressional Budget Review Process	
Processes									
STAKEHOLDERS									
DOJ Partners	DOJ Business Leaders	✓		✓				✓	
	DOJ Budget			✓	✓	✓	✓		
	DOJ OPCL			✓					✓
	DOJ Records Management			✓					✓
	DOJ SPE			✓					✓
DOJ Oversight	OIG								✓
	DIRB							✓	
	DIRC							✓	✓
	CIO Council	✓	✓						✓
	Business Committees	✓	✓						✓
	Mission Committees	✓	✓						✓
	CIO Council Committees		✓						

Figure 2-6: Departmental and Domain Oversight - IT Governance Integration Matrix

Figure 2-7 shows the participation of service/program/project stakeholders in DOJ's governance phases and processes.

IT Governance Integration Matrix										
Service/Program/Project Execution: Processes, Stakeholders, & Products										
IT Governance		IT PLANNING PHASE			IT BUDGET PHASE			IT OVERSIGHT PHASE		
Phases										
Processes		IT Strategic Planning Process	EA Roadmap Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Review Process	Congressional Budget Review Process	Executive Review Process	Compliance Review Process
STAKEHOLDERS										
DOJ CIO Office	DOJ CIO	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OCIO DIRC Exec Sec								✓	✓
	OCIO PPS	✓		✓	✓	✓	✓		✓	✓
	OCIO PPS EA		✓	✓	✓	✓				✓
	OCIO CSS				✓	✓			✓	✓
	OCIO CISO	✓	✓	✓	✓	✓			✓	✓
Component Partners	Component Business Leaders	✓								
	Component CIO	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Component Budget/ Finance Staff				✓	✓	✓	✓		
	Component ITIM Coordinator			✓	✓	✓	✓	✓		✓
	Component IT Project Manager			✓	✓	✓	✓	✓	✓	✓
	Component CISO			✓	✓	✓				✓

Figure 2-7: Service/Program/Project Execution - IT Governance Integration Matrix

While the three stakeholder matrices show individual stakeholder groups, they collectively show the overall integration of the different stakeholders across DOJ's governance phases and processes.

2.4 System Development Life Cycle (SDLC) Framework

The Department's System Development Life Cycle (SDLC) is a set of established procedures, practices, and guidelines governing how DOJ information systems shall be planned, developed, implemented, and managed. *DOJ Order 0903* on IT Management establishes the DOJ CIO's authority to develop and implement department-wide program management guidelines, including

a standardized [SDLC methodology](#).⁵ For those components that have received authorization from the OCIO to use an alternative SDLC, refer to specific guidance from component IT governance leadership. Department guidance on “modular” Agile software development is also available and referenced later in this section. OCIO is advocating use of an agile methodology and will be updating its SDLC to reflect agile as the preferred methodology.

The Department’s SDLC guidance establishes standard processes and artifacts that allow for the orderly and effective planning, development, implementation, operation, and retirement of IT systems. The guidance also provides visibility into the development process to permit independent assessment of program efforts and to support investment management decisions.

The SDLC is used for guidance and planning of each project or program. The SDLC consists of ten development life cycle phases that are described in detail in the Department’s SDLC Guidance Document. The development life cycle phases are

1. Initiation
2. Concept Development
3. Planning
4. Requirements Analysis
5. Design
6. Development
7. Integration and Test
8. Implementation
9. Operations and Maintenance
10. Disposition

During each of these phases, program teams may need to prepare a plan, perform a study, or complete a program evaluation or review before the program can proceed to the next phase. The plans, studies and evaluations prepared during system development help ensure that program teams perform the appropriate analysis and planning necessary to deliver the benefits expected from investments, both on time and within budget. These documents also serve as records of the decisions made during project planning, execution, or evaluation for later reference.

Because of the wide variation in IT solutions, program scope, investment cost, risks, development approaches, and implementation strategies that may be associated with an IT development project, program managers are given discretion in tailoring the SDLC activities and artifacts for their assigned project. Depending upon the size, complexity, and development approach of the program, life cycle phases may be combined or may overlap. However, to ensure that the essential planning and evaluation actions necessary for program success are performed and documented, the Department has identified a set of standard artifacts that should be prepared for all programs.

All programs and projects managed under the DOJ SDLC must prepare the applicable artifacts listed in Figure 2-8. The list categorizes projects into three types: non-system projects; projects less than \$1M; and projects \$1M and above. The list is grouped into four sections: artifacts

⁵ <http://www.justice.gov/archive/jmd/irm/lifecycle/table.htm>

required before the project starts (e.g. a business case); mandatory artifacts; mandatory compliance requirements; and key SDLC deliverables for IT projects. Comprehensive guidance on required SDLC documents, processes, and artifacts may be found in the *DOJ IT Project Manager Guide* on the [DOJ Project Management Center of Excellence](#)⁶ Website.

ARTIFACTS LIST		REQUIREMENTS		
		Non-System Project/or Important Initiative (ex. IT Flash Mentoring Event)	Project Life-cycle Cost of Less than \$1M	Project Life-cycle Cost of \$1M or greater
Before the Project Starts				
1	Business Case	N/A	✓	✓
	a) Analysis of Alternatives	N/A		✓
	b) Budget or Lifecycle Cost Estimate	N/A		✓
2	Project Charter	N/A	✓	✓
Mandatory				
3	Project Status Report	Tailored	✓	✓
4	IT Acquisition Review	N/A	✓	✓
5	Project Management Plan	Tailored	✓	✓
6	Reviews - pre, during, and post implementation reviews with customer(s)/IV&V/Lessons Learned	Tailored	✓	✓
Mandatory Compliance Items - may be tailored based on project scope				
7	Section 508 Compliance	Tailored	Tailored	✓
8	Records and Information Management Certification (RIMCert)	N/A	Tailored	✓
9	Security Assessment and Authorization Compliance	N/A	Tailored	✓
10	Supply Chain Risk Review	N/A	Tailored	✓
11	Initial Privacy Assessment (IPA)/Privacy Impact Assessment (PIA)	N/A	Tailored	✓
Key SDLC Deliverables for IT Projects				
12	Concept of Operations (CONOPs)	N/A	Tailored	✓
13	System Design Document (SDD)	N/A	Tailored	✓
14	Information System Contingency Plan (ISCP)	N/A	Tailored	✓
15	Target Architecture	N/A	Tailored	✓
16	Service Transition Plan/Checklist	N/A	Tailored	✓

Figure 2-8: SDLC Minimum Deliverables

The Business Case, Analysis of Alternatives (AoA), Target Architecture, and Information System Contingency Plan (ISCP) artifacts are relatively new, and are not yet embedded in the DOJ SDLC. Descriptions and templates for all the artifacts in Figure 2-8 are available in the [Project Management Checklist](#).⁷

The artifacts listed in Figure 2-8 are intended to: (a) provide visibility into the decision making

⁶ <https://itim.doj.gov/projectmanagement/SitePages/PMGuide.aspx>

⁷ <https://itim.doj.gov/projectmanagement/SitePages/PMChecklist.aspx>

process for oversight and investment management assessments; (b) establish a minimum level of formal treatment of programmatic decisions; and (c) provide value to the programs by documenting requirements, management activities, and acceptance criteria related to finished system capabilities. Programs may tailor these artifacts from the forms specified in the template appendices so long as the tailored products serve the basic artifact purpose described in the SDLC guidance. For each tailored artifact, the program should document, via memorandum for the record, (a) the reason why tailoring occurred and (b) any foreseen impact of using a tailored template. These artifacts, when tailored, may be prepared as stand-alone documents or combined, if appropriate, so long as each SDLC artifact is clearly identified for future reference and location.

The SDLC deliverables and compliance requirements identified in Figure 2-8 serve as a minimum compliance standard for DOJ programs. Project managers are highly encouraged to prepare other relevant deliverables defined in the SDLC. Over time, the DOJ OCIO may expand the list of mandatory and recommended SDLC deliverables in response to observed Departmental program development performance and to increase the use of best practices in program development activities.

Recent FITARA legislation requires “adequate incremental development” approaches consistent with the “modular” approach previously mandated by the Federal CIO in its *25-Point Implementation Plan to Reform Federal Information Technology Management*⁸. Direction on Agile and other iterative approaches to meet these requirements is being incorporated into SDLC guidance as described in the *DOJ Agile Guidance Document* stored on the Agile Project Management page of the [DOJ Project Management Center of Excellence](#).

There are three major stakeholders involved in applying and administering the Department’s SDLC framework: the Department CIO, the component CIO, and the Program Manager. Their roles are as follows:

- **Department CIO**
 - Establish an extensible SDLC framework with standard high-level processes that promotes an agile methodology
 - Promote the creation of standard artifacts, develop minimum criteria for gate reviews, and employ agile and incremental development principles
 - Work with IT Oversight Managers to insert appropriate gate reviews into the SDLC, including each review’s specific standards and templates for artifacts
 - Review component processes for compliance with the framework
 - Review SDLC artifacts, when appropriate, through the Executive Review and Compliance Review processes (Section 3.3.1 and 3.3.2) to monitor the performance of selected programs and systems
- **Component CIO**
 - Implement the enterprise SDLC in the component, expanding it to meet component needs

⁸ Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington: White House, December 2010).

- Submit component SDLC to the DOJ IT Investment Oversight Manager for review and approval prior to implementation
 - Ensure component programs comply with Department and component SDLC requirements by reviewing artifacts, as necessary, during regular component program oversight reviews
 - Advocate for the transition to agile and incremental development practices
- **Program Manager**
 - Identify all SDLC activities appropriate for the orderly and effective development and implementation of the IT system and/or service being developed and incorporate the activities into the program or project work plan
 - Ensure all required and necessary SDLC artifacts are prepared and maintained
 - Submit SDLC artifacts, when required, for component and Department Executive oversight reviews (Section 3.3.1)
 - Participate in training on the agile methodology

To illustrate application of the SDLC guidance, consider how the guidance applies to two example investments.

Investment A is an operational system/service undergoing a major enhancement of capabilities budgeted over \$1 million. The existing system/service is in an O&M phase, therefore an initial set of SDLC artifacts is assumed to be in existence. The enhancement project is currently in the SDLC Design phase. Based on the mandatory artifacts listed in Figure 2-8, the program team must prepare or update the following mandatory artifacts for the enhancement effort before completing the Design phase:

- Business Case, LCCE, and Analysis of Alternatives (update for the enhancements)
- Project Charter (update to address purpose, authority, and scope of the new work)
- Project Management Plan (update to address management of the new work)
- Risk Management Plan (update risk register to address the risks for the new work)
- Reviews (regular lifecycle reviews are expected, including adherence to a governance process)

Additionally, based on tailoring of the SDLC to this specific IT project, it might be determined that the Concept of Operations (CONOPS) is also required, since it incorporates new capabilities.

Investment B is a new development program. Per Figure 2-8, the program team must prepare the following mandatory artifacts before beginning development:

- Business Case, LCCE, and Analysis of Alternatives
- Project Charter
- Project Management Plan
- Risk Management Plan
- Reviews

Additionally, based on tailoring of the SDLC to this specific IT project, it might be determined that the following key IT deliverables are also required:

- Concept of Operations (CONOPS)
- System Design Document
- Target Architecture
- Information Systems Contingency Plan (ISCP)
- Service Transition Plan/Checklist

In both scenarios above, other recommended or needed artifacts should also be developed depending on the nature and scale of the solution, and the compliance requirements in Figure 2-8 should be met.

2.5 Cost Estimating

As stated in the [*OMB Capital Programming Guide*](#) (Supplement to OMB Circular A-11), credible cost estimates are vital for sound management decision making and for any program/project to succeed. Early emphasis on cost estimating during the planning phase is critical to successful life cycle management of a program/project. As such, the Department has developed requirements and an approach with respect to collecting, managing, and sharing cost data that will aid in providing greater information management support, more accurate and timely cost estimates, and improved risk assessments that will help to increase the credibility and reliability of investment cost estimates.

Following the Department's cost estimation approach and meeting cost estimation requirements will produce sound cost estimates. This information can be used in preparing the annual budget, determining return on investment estimates, and improving the life cycle management of investments with more reliable performance baselines and earned value management (EVM). Additionally, evaluating alternatives through cost-benefit analysis and assessing and managing risk becomes more effectively performed.

2.5.1 Types of Government Cost Estimates

Cost estimating attempts to predict future capital expenditures even if not all factors and conditions of the investment are fully defined. There are many different types of cost estimates that can be developed for various purposes and at different phases of the investment life cycle. For each type of estimate, bases (ground rules) and assumptions are spelled out. OMB has identified the following as types of cost estimates, which can be used throughout the investment life cycle.

- **Conceptual Cost Estimate** is used early in the planning phase of the acquisition life cycle and is often based on a one-to-one comparison with an existing system similar to the system being proposed.
- **Preliminary Cost Estimates** are used as more details become available and for preparing the general outlines to budgetary requirements.

- **Detailed or Engineering Cost Estimates** represent a bottom-up estimate using the detailed work-breakdown structure (WBS) to price out discrete project elements, such as material, design hours, labor, off the shelf software, etc.
- **Definitive Cost Estimate** is used late in the acquisition life cycle during the project control phase, based on actual cost data available from the same system at an earlier time in the project's history. The EVM concept is used to arrive at the estimate at completion (EAC).
- **Life Cycle Cost Estimate (LCCE)** provides the total cost to the Federal Government of acquiring and owning the system over its full lifetime. It includes the cost of development, acquisition, support, O&M, and (where applicable) disposal.
- **Independent Cost Estimate (ICE)** is based on the same scope as the LCCE, except that an independent review team using independent data sources and cost estimating approaches prepares it.
- **Independent Government Cost Estimate (IGCE)** is prepared for evaluating and validating vendor proposals presented during the acquisition phase. It is prepared from the Government's point of view and is based on the scope of work and estimated level of effort as outlined in the solicitation.

DOJ requires that all major IT investments develop a LCCE in order to meet cost estimation requirements. The LCCE is used as an aid in preparing the DOJ Spring Call and the Departmental budget submission to OMB. Cost estimates should be developed following Department policy⁹ and procedure guidance governing the preparation and review of cost estimates for projects/programs (or their increments) as they proceed through their life cycle stages.

2.5.2 Cost Estimation Techniques

Many techniques can be used for cost estimating, from simple calculations to complex mathematical models with numerous variables. Some of the techniques identified by OMB are:

- **Analogy:** Used early in the acquisition life cycle based on a one-to-one comparison with an existing system similar to the system being designed.
- **Parametric:** Uses statistical analysis from a number of similar systems and their relationship to your system.
- **Engineering:** A bottom-up estimate using the detailed WBS to price out discrete program components, such as material, design hours, labor, etc.
- **Extrapolation from Actual Costs:** Method used late in the acquisition life cycle after actual cost data are available from the same system from an earlier time.

⁹ Project Management Policy Statement, DOJ Policy Memorandum #2016-03

2.5.3 Cost Estimation Methodology

To keep the estimate current, accurate, and valid, the cost estimating process is continuously updated, based on the latest information available. As the project matures the availability of valid data increases. The following are the major steps in the cost estimating process and should be applied, as applicable. For more information on cost estimating, please reference the [*GAO Cost Guide*](#).¹⁰

- **Prepare a WBS or Similar Project Work Structure:** Based on preliminary project scope, prepare a high-level WBS, generally three levels deep.
- **Define the Ground Rules and Assumptions:** Define the technical, economic, schedule, business, and other factors. The assumptions need to be realistic and continuously reviewed and updated as the scope of the project becomes better defined with the passage of time.
- **Develop Data:** Collect, identify, and analyze data for the cost estimate. Data (accurate, relevant, and correct confidence level) is the most important piece of the cost estimate, is time consuming to prepare properly, and includes cost drivers for the cost estimate and risks. Most data are in raw form and must be normalized using learning curves and other methods so that they are comparable and consistent. The normalized data must be adjusted to make it useable for the specific project. All data, including any adjustments made, should be thoroughly documented so an audit trail is established for verification purposes.
- **Select/Construct Cost Model:** Select the most appropriate tool/model or create a model to estimate the cost. Document factors that influence the selection process such as data and resource availability, schedule, and cost.
- **Develop the Estimate:** Based on the ground rules and assumptions, and using the normalized/adjusted data, develop the cost estimate and the level of confidence applying various risk factors.
- **Perform the Sensitivity Analysis:** Once the estimate is developed, decision makers want and need to know how sensitive the total cost estimate is to changes in the data input. Therefore, a sensitivity analysis is performed to identify the major cost drivers of the estimate. Cost drivers are those variables that, when changed in value, create the greatest changes in cost. Generally, many initial assumptions made in the early phases of a project's definition may be found to be inaccurate requiring updating.
- **Develop Contingency Reserve:** Based on the confidence level of the estimate, a contingency allowance, often called a management reserve, should be incorporated into the cost estimate to cover the cost of items that are not known at the time the estimate is prepared. A preliminary estimate generally has a confidence level of 70 percent while a definitive estimate will have a confidence level of 90 percent. Contingency allowances of 30 percent and 10 percent, respectively, should be added to the preliminary estimate and definitive estimate within those

¹⁰ <http://www.gao.gov/new.items/d093sp.pdf>

phases of the project, and adjusted accordingly.

- **Document Cost Estimate:** Explain the cost estimating process used and document how the cost estimates were prepared so that the quality of the estimate can be determined. Proper documentation will increase credibility, facilitate information sharing, and make these estimates usable in the future.
- **Update Cost Estimate:** On a regular basis, keep the cost estimates current. Such quality data are needed for decision-making, "what if" models, and estimating the costs of alternatives.

2.5.4 Cost Estimation Tools

The Automated Cost Estimating Integrated Tools (ACEIT) suite is one recommended tool for project managers to use for cost estimation. Similar to how Microsoft Office provides a suite of applications to automate office functions, ACEIT provides a suite of applications to automate cost analysis. More information on cost estimating is available at [DOJ Project Management Center of Excellence](#), under "Cost-Estimating Tools."

2.6 Enterprise Performance Management (EPM)

The purpose of EPM is to provide a standard method for measuring the Department's progress toward its target state using a set of performance metrics consistent with an investment's purpose and its position in the SDLC. EPM is results-oriented and shows a causal relationship between the performance of individual IT investments and the success of the Department as a whole. This approach helps provide rigor and due diligence to the IT Governance Framework and the IT Investment Life Cycle, and it helps to ensure that investments such as the example Investments A and B deliver the strategic and business needs that each are intended to provide.

Performance measurement is a cyclical process that begins with defining strategic needs and envisioning desired outcomes. The process is continued by assessing current performance and performance gaps, establishing target improvements and measures of success, measuring results and comparing results to targets. If the targets are no longer valid, the process is repeated by establishing new targets and identifying actions necessary to achieve those targets. This cycle is illustrated by the Enterprise Performance Management Model shown in Figure 2-9. The model provides a methodology for continually improving an investment's performance through periodic review and analysis of investment results. This approach enables DOJ and component leadership to take into account how IT investments contribute to the success of the Department's priorities when making budget decisions and to take corrective action when necessary.

Enterprise Performance Management

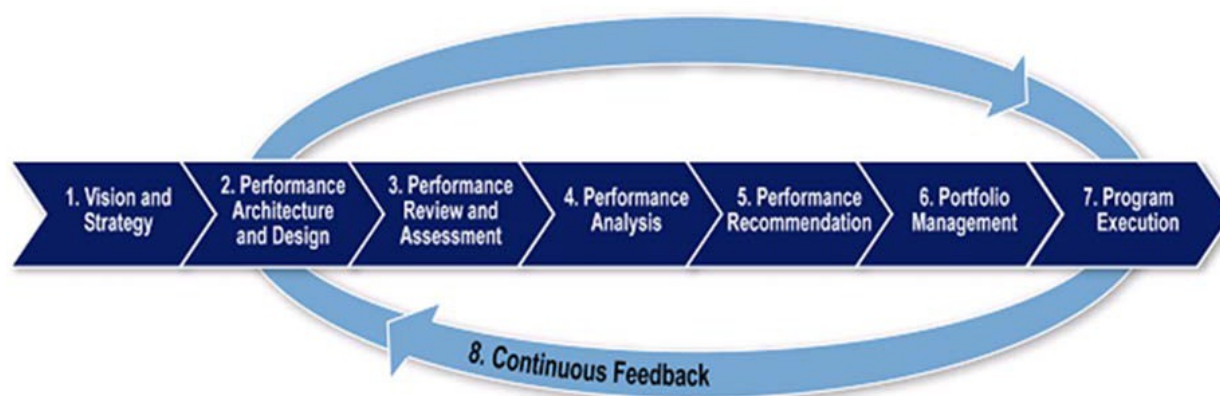


Figure 2-9: Enterprise Performance Management

The eight EPM stages link to the activities of the IT Investment Life Cycle and are described below.

1. **Vision and Strategy:** Department's strategic goals and priorities from the *DOJ Strategic Plan* and *IT Strategic Plan* provide direction for designing, developing and aligning the Enterprise Performance Architecture.
2. **Performance Architecture and Design:** DOJ OCIO identifies program and mission performance goals and metrics, and collaborates with investment owners in selecting key IT performance metrics to measure achievement of strategic goals.
3. **Performance Review and Assessment:** Individual investment performance results are compared to performance goals and aggregated to produce performance results reporting.
4. **Performance Analysis:** DOJ OCIO and component leadership review the Department's performance metrics in relation to investment specific performance results and identify performance gaps and/or issues.
5. **Performance Recommendations:** Developed to address performance gaps discovered during performance analysis and help shape investment priorities for the IT investment-planning process.
6. **Portfolio Management:** performance recommendations are used to inform investment selection decisions in the IT budget phase to shape the Department's priorities and its IT portfolio.
7. **Program Execution:** Investment managers monitor investment performance results

during the IT oversight phase.

8. **Continuous Feedback:** Performance results collected for oversight reviews are compared with the performance targets to start the next IT planning cycle.

The Department's EPM process is integrated into the Department's annual ITIM process in order to gather investment performance information on a regular basis. The process includes key investments monitored by the DIRC, reported on the DOJ Majors and [Federal IT Dashboard](#)¹¹ (FITDB), and included in the *DOJ Transition Strategy and Sequencing Plan*. Performance reporting also is a key process within the ISO 20000 framework employed by the OCIO.

- **Department-Level Responsibilities**

- Develop guidance on types of metrics that should be developed and reported for programs/investments (e.g. operational metrics for Major IT Business Cases), including a catalogue of the different types of metrics and measures being gathered across the Department
- Normalize the individual program/investment metrics so similar metrics are used across the Department

- **Component-Level Responsibilities**

- Ensure development and tracking of performance metrics for component programs/investments
- Periodically report metrics to the Department

- **Program-Level Responsibilities**

- Program managers must develop performance metrics and track performance results for the program/investment under management.

The DOJ OCIO groups investments and activities into manageable pieces for performance analysis. The results of the analyses are used to help the Department manage its IT resources and to focus those resources on the continued development and employment of enterprise solutions. Performance metrics from the various components and programs are grouped to provide a broader picture of the Department's success in delivering the strategic outcomes for particular mission areas. Analyzing performance helps to relate the successful delivery of IT investments to success in meeting the Department's strategic goals and missions.

In terms of our examples, both Investment A and B's annual outcomes are measured against their roles in fulfilling mission and business needs against targets established by the program. Outcomes indicate the degree to which program objectives are being met and whether or not the expected value is being delivered as represented in the business case. Metrics are applied based on investment status including investment classification, current position in its SDLC, and other criteria. After performance results are reviewed and analyzed, recommendations can be made, at both the component and Department level, for improving each investment to better meet the

¹¹ <http://itdashboard.gov>

strategic business need it was created to address.

2.7 Investment Classification Model

The Investment Classification Model provides a structure for classifying investments to support portfolio analysis and to determine the oversight reviews required for each investment at any point in its life cycle. Investments are classified in three tiers: scope of the investment, the type of technology investment, and the life cycle stage of the investment.

The first tier of investment classification supports the Department's strategic goal of unifying and standardizing solutions across the IT enterprise by identifying the planned scope of an investment and the users the investment is intended to help. All investments are classified as either enterprise investments or component investments. Investments intended to fill a single component's business needs are classified as component investments, whereas investments intended to fill the needs of multiple components are classified as enterprise investments. Each enterprise investment is assigned to a lead component that is responsible for ensuring that the appropriate compliance reviews are completed. For the purpose of classification, the following definitions are used:

- **Enterprise Investment:** An investment that supports the functional needs of two or more components
- **Component Investment:** An investment that supports the functional needs of a single component

The second tier of investment classification supports the Department's strategic goal of reducing redundant infrastructure by identifying the type of business need an investment is meant to fulfill. Using the categories in the Department's definition of IT (See Section 1.2 and Appendix B – Definition of IT for DOJ), each investment is classified as a mission-delivery and business solution, infrastructure, or IT practices and management investment. Investments that are a mix of two or more of these types are apportioned to each category based on the percentage of funding applied toward each area. For the purposes of classification, apportionment, and IT cost reporting, the following definitions are used:

- **Mission-Delivery and Business Solutions:** The software applications, systems, services and the people, processes, commercial contracts, overhead occupancy, and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department. Mission-delivery and business solutions provide support for the missions of the Department, as stated in the DOJ Strategic Plan.
- **Infrastructure:** The people, processes, commercial contracts, overhead occupancy, and technology used to interconnect computers and users and automate business processes. Infrastructure is also used to acquire process, store, send, receive, interchange, manage, switch, and transmit electronic data and information. Infrastructure is further classified into end-user, mainframe & server, and telecommunications systems & support.
 - **End User Systems & Support** includes the people, processes, commercial contracts, overhead occupancy, and technology necessary to enable and support an end user in their

interaction with information technology services.

- **Mainframe & Server Systems & Support** includes the people, processes, commercial contracts, overhead occupancy, and technology to provide physical or logical, centralized or aggregated computer systems and related services to one or more parts of the enterprise.
- **Telecommunications Systems & Support** includes the people, processes, commercial contracts, overhead occupancy, and technology to provide any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.
- **IT Practices and Management:** The programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology, and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support all the IT investments of the component or enterprise.

The third tier of investment classification identifies the investment's life cycle stage and is used to determine the appropriate oversight review. IT investments are classified as development projects, O&M systems/services, or mixed life cycle investments. Investments that are classified as mixed life cycle investments are apportioned to development and O&M based on the amount of funding applied in each area. For the purposes of classification and apportionment, the following definitions are used:

- **Development Projects** are investments that apply substantial resources to development, modernization, or enhancement (DME) of IT business solutions or infrastructure services¹². Projects have start and end dates, and deliver an IT asset or service when completed. Development project investments fund the activities for planning, developing, testing, or implementing new infrastructure or business solutions, expanding existing solutions to serve new users and uses, or implementing significant enhancements to existing infrastructure or business solutions to update or improve existing capabilities.
- **Operations and Maintenance (O&M) Systems / Services** are assets that are in service and are being supported for ongoing operations¹³. While there is often some low level of ongoing system enhancement, such as software and/or hardware upgrades, the new work is usually to maintain system performance or operational availability. There may also be service delivery activities funded by O&M.
- **Mixed Life Cycle Investments** are investments that apply resources for significant modernization or enhancement of existing IT assets, as well as for the ongoing operations and maintenance of those assets.

¹² Investments for technical refresh of systems are considered development projects that may require project reviews.

¹³ Operations and maintenance investments may contain nominal funds for development, as long as the development activity does not rise to the level of requiring a component or Department-level project review. When the development activity is significant enough to require project review, the investment will typically be classified as a project for the purpose of review.

The relationship of these three classification tiers is illustrated in the Investment Classification Model in Figure 2-10. Using these three classification tiers, the Department's IT portfolio's costs can be grouped and analyzed for strategic investment and budget planning.

Tier	Category	Purpose	Classification	Definition
I	Investment Scope	Support IT Strategy 1.0: Share Business Solutions	Enterprise Investment	An investment that supports functional needs across two or more components.
II	Investment Type	Support IT Strategy 3.0: Share Infrastructure	IT Infrastructure	The people, processes, commercial contracts, overhead occupancy, and technology used to interconnect computers and users and automate business processes. Infrastructure is also used to acquire process, store, send, receive, interchange, manage, switch, transmit, and receive electronic data and information.
II	Investment Type	Support IT Strategy 3.0: Share Infrastructure	Mission-Delivery & Business Solutions	The software applications, systems, services and the people, processes, commercial contracts, overhead occupancy, and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department.
II	Investment Type	Support IT Strategy 3.0: Share Infrastructure	IT Practices & Management	The programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology, and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support all the IT investments of the component.
III	Life Cycle Stage	Assign Appropriate Oversight Reviews	Development Project	An investment that applies resources primarily to development, modernization or enhancement (DME) of IT business solutions or infrastructure services
III	Life Cycle Stage	Assign Appropriate Oversight Reviews	O & M System	An investment for IT assets that are in service and are being supported for ongoing, steady state operations & maintenance (O&M)
III	Life Cycle Stage	Assign Appropriate Oversight Reviews	Mixed Life Cycle Investment	An investment that applies substantial resources for modernization or enhancement of existing IT assets, as well as for operations and maintenance of those assets

Figure 2-10: Investment Classification Model

To illustrate how the Investment Classification Model is used, the three classification tiers are applied to two example investments.

Investment A is classified as an enterprise investment, a business-solution, and a mixed life-cycle investment.

- Enterprise – It fulfills a business need for two or more components.
- Business Solution – It is an application that directly supports a business function.
- Mixed Life Cycle – It is in O&M, but is undergoing a major enhancement.

Because Investment A is an enterprise business solution, it will likely receive a high priority ranking in the Department IT portfolio during investment and budget planning. Investment A will also receive different types of reviews as an enterprise, mixed-lifecycle investment, than it would as, for example, a component development life-cycle stage investment, as discussed further in the IT Oversight Model (Section 2.8).

Investment B is classified as a component investment, a business-solution, and a development project.

- Component – It fulfills the mission or business needs of a single component.
- Business Solution – It is an application that supports a specific business function.
- Development Project – It is under development and is not yet operational.

Because Investment B is a component-specific business solution, the managing component must justify the investment's priority during investment and budget planning.

2.8 IT Oversight Model

The IT Oversight Model communicates the Department's vision for integrating the processes and outcomes of the oversight phase of the investment life cycle based on the investment's position in the SDLC and its classification. The model provides a structure for describing the levels of oversight that occur at the Department level and in the component CIO offices.

Oversight of IT investments serves two main purposes:

- Monitor the progress and performance of projects and other investments to ensure each are managed well and each delivers expected results
- Provide feedback to influence resource planning decisions for the future

Oversight reviews occur at the Department and the component level:

- **Department Reviews:** Monitor the summary level performance of the DOJ portfolio with individual focus on investments that are high cost, high risk, or high visibility and are important to Department-wide missions or cross-government integration, or ensure uniform compliance with federal and Department policies and procedures.
- **Component Reviews:** Monitor the progress of development projects and O&M systems/services important for component success, and assess investment performance and

compliance with component business practices, processes, and procedures.

There are two primary types of Department and component oversight reviews – executive review and compliance reviews:

- **Executive Reviews:** These reviews are performed by executive oversight groups to ensure that investments are aligned with the Department and/or component strategic priorities (respectively) such that key investments are delivering the business value and return on investment (ROI) commensurate with investment costs.
- **Compliance Reviews:** These reviews are typically performed by functional oversight groups to ensure that projects and other investments proceed according to approved plans, deliver expected service, and comply with established policies, procedures, and standards.

Executive and compliance reviews are divided into project and operational reviews, based on the life cycle stage of the investments under review:

- **Development-Project Reviews:** Regular or event-driven reviews that monitor the progress of development projects against cost targets, schedule milestones, and completion of compliance requirements associated with design, development, or implementation. Project reviews typically occur on a frequent basis, such as monthly or quarterly, to monitor progress. Project reviews may also occur at key milestones in the project life cycle when decisions are required to move the project from one SDLC stage to another.
- **Operations and Maintenance (O&M) Reviews:** Periodic reviews that assess operational systems/services for effectiveness, cost management, customer satisfaction, and compliance with established operating procedures and management standards. O&M reviews are typically performed on a periodic basis, often quarterly, and at least annually.

The IT Oversight Model in Figure 2-11 illustrates the interaction between the oversight processes and stakeholder engagement to achieve the specified purposes of oversight. The model illustrates coordinated actions for

- Progress, performance, and compliance reporting, including reporting up to OMB
- Resource planning decisions, based on strategic direction, and resulting in investment prioritization

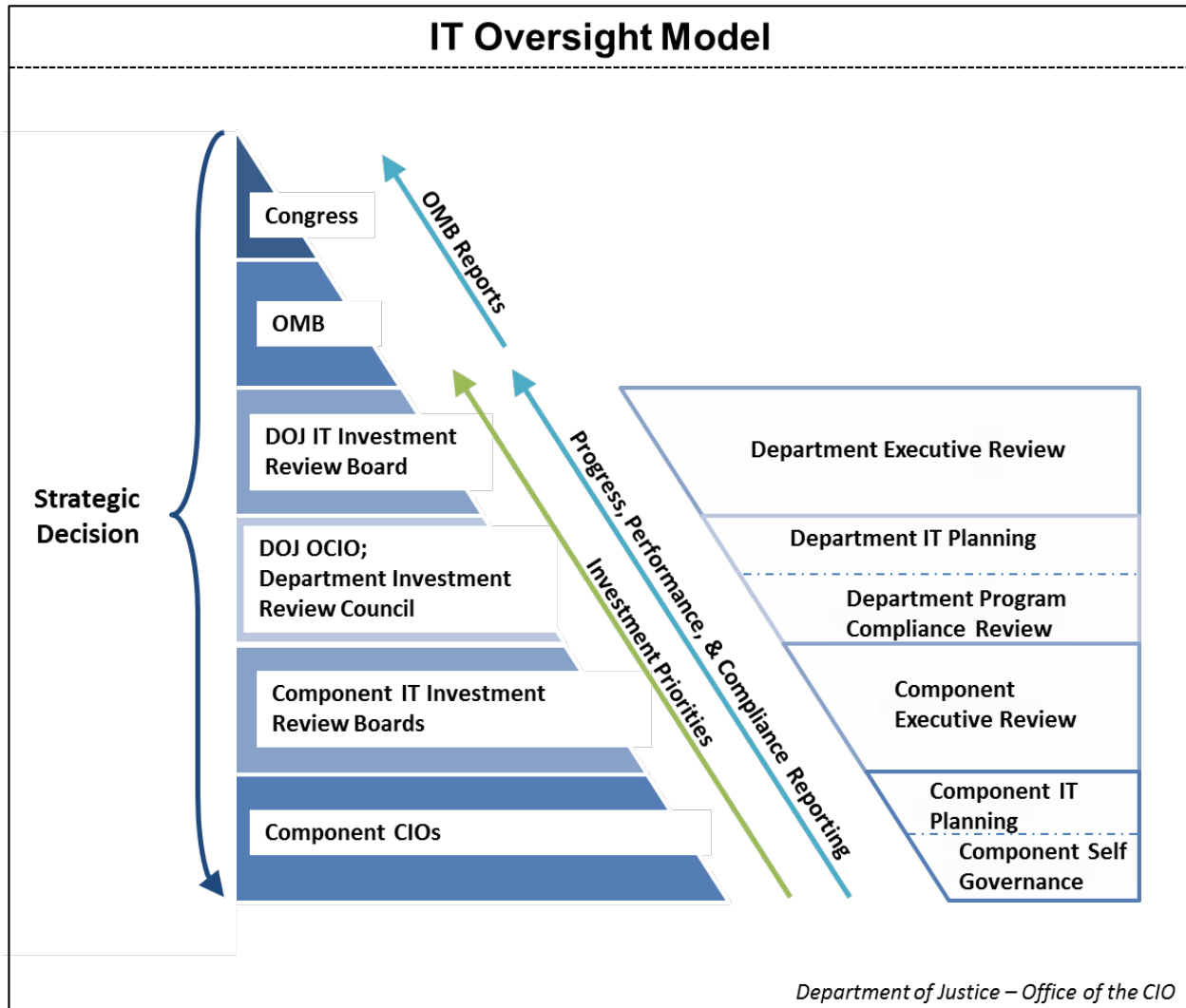


Figure 2-11: IT Oversight Model

The DOJ Investment Review Board (DIRB) serves as the Department's top-level board responsible for Department executive review and IT planning. The DIRB sets the strategic direction of the Department's IT program, prioritizes enterprise investment initiatives, and monitors the largest IT programs exceeding \$100 million or more on new capabilities.

The Department Investment Review Council (DIRC) directly supports the DIRB. It serves three purposes:

- Oversees the progress and management of select major investment programs in the control/evaluate phase
- Monitors that appropriate program oversight mechanisms are in place at the component-level for specified investments

- Monitors IT programs and projects for compliance with departmental and federal standards and regulations

The DIRC oversees executive and compliance reviews that are largely conducted at the component level and reported to the DIRC and other Department oversight offices (e.g. Cost/Schedule/Risk, Privacy, Security, and RIMCert). The DIRC reviews these component oversight processes, and monitors component self-governance to ensure programs and projects comply with departmental and federal standards and regulations, including performance expectations (e.g. value delivery). If necessary, the DIRC holds in-person Deep Dive and TechStat Sessions to assist with turning around underperforming investments.

For investments categorized as development projects or mixed life cycle, there are nine potential compliance reviews or activities, as described and defined in Section 3.3.2:

1. Program/Project Manager Qualification (PMQ)
2. Cost/Schedule/Risk and Earned Value Management Surveillance
3. Enterprise Architecture
4. Security
5. Privacy
6. Records and Information Management Certification
7. Section 508 Compliance
8. Acquisition (ACQ)
9. Operational Analysis

Investments categorized as mixed life-cycle and/or O&M system/service investments are subject to operational analysis reviews, as described and defined in section 3.3.2.9.

The component portion of the oversight model looks very similar to the Department portion, with one key difference: component compliance review responsibilities are divided between Department compliance review support and component compliance review. Components not only provide information needed for compliance reviews performed at the Department-level, they also perform compliance reviews at the component-level and use the results of those reviews internally to satisfy component IT planning and oversight needs. In order to ensure early matching of IT with program objectives, the DOJ CIO shall be a member of all governance boards that include IT resources, including internal bureau investment review boards (IRB). The component executive review serves three purposes:

- Prioritizes component investments for component and Department IT planning
- Monitors the progress of selected component-level investments in the control and evaluate phases, through metrics-based measurements
- Ensures that component IT programs and projects are complying with all departmental and federal standards and regulations

Information produced from component compliance reviews is used as input to component IT strategic planning and IT budget planning processes, and is provided to the DIRC for Department-level monitoring. Additional guidance for component oversight is provided in the component self-governance model, as described and defined in Section 2.9.

To illustrate how the IT oversight model is used, the model is applied to two example investments. Investment A is classified as an enterprise business-solution, mixed life-cycle investment. Consequently, the investment is subject to the following reviews or monitoring:

- DIRC monitoring because it is an enterprise investment undergoing a major enhancement
- DIRC compliance monitoring for projects and O&M systems/services as specified by the DIRC's pre-defined selection criteria
- Component program and compliance reviews as specified by component oversight processes and selection criteria

Investment B is classified as a component business-solution, development project and is therefore subject to the following reviews:

- Department compliance reviews that apply to all component and Department projects and O&M systems/services
- Component project reviews as specified by component oversight processes and selection criteria

2.9 Component Self-Governance Model

One of the purposes of this guide is to communicate to component CIOs the Department's expectations for component self-governance. The OCIO developed the Component Self-Governance Model to help components identify the requirements for self-governance actions in the budget and oversight phases and to help implement the specific requirements for internal component IT governance.

By applying the investment classifications defined in the Investment Classification Model, components can discern the specific actions they must plan to perform throughout the investment life cycle for both component investments and Enterprise investments for which they are the managing component.

The Component Self-Governance Model in Figure 2-12 applies the categories from the Investment Classification Model described in Section 2.7 to show when component self-governance actions must occur during the investment life cycle for each investment type¹⁴.

¹⁴ Components that do not directly manage IT services or investments have no obligation to implement IT self-governance processes and are not included in the process discussions in Section 3.

Self-Governance Actions by Investment Category and Life-Cycle Phase

	IT Planning Phase	IT Budget Phase		IT Oversight Phase		
Investment Category	Define Component Investment Priorities	Report Investments in Agency IT Portfolio Summary	Verify Investment Costs	Perform Component Executive Reviews ¹⁵	Perform Component Compliance Reviews	Define Component Review Criteria
Enterprise Investments						
Development Projects	X	X	X	X	X	
O&M Systems/ Services	X	X	X	X	X	
Mixed Life Cycle	X	X	X	X	X	
Component Investments						
Development Projects	X	X	X	X	X	X
O&M Systems/ Services		X	X	X	X	
Mixed Life Cycle		X	X	X	X	

Figure 2-12: Component Self-Governance Model

Six primary component self-governance actions are required to support Department-level processes during the three IT governance life cycle phases.

- **IT Planning Phase**
 - Define component investment priorities
- **IT Budget Phase**
 - Report investments on the Agency IT Portfolio Summary
 - Verify accuracy of investment costs
- **IT Oversight Phase**
 - Perform component executive reviews
 - Perform component compliance reviews
 - Define component review criteria

To illustrate how the Component Self-Governance Model is used, consider the two example investments described earlier. Investment A is an enterprise mixed life-cycle investment, required to undergo Department-level monitoring. Per the model, the managing component responsibilities

¹⁵ Each component will work with the DIRC to establish and mature component-level program oversight processes

are to:

- Report the investment in its investment priorities during the IT planning phase
- Report the investment on Agency IT Portfolio Summary and verify the investment cost during the IT budget phase
- Perform appropriate component-level executive reviews to ensure that the investment will be delivered on time, on budget, and to specification(s)
- Ensure all other Department and federally required compliance reviews are completed

Investment B is a component development investment and is primarily reviewed at the component level. Per the model, the component responsibilities for this investment are to

- Report the investment in its investment priorities during the IT planning phase
- Report the investment on the Agency IT Portfolio Summary and verify the investment cost during the IT budget phase
- Perform appropriate component-level compliance reviews to ensure that the investment will be delivered on time, on budget, and to specification(s)
- Ensure all Department-level (e.g. security and privacy) and component-level compliance reviews are completed in the IT oversight phase
- Pre-define review criteria for this and other development projects within the component

Section 3, Governance Phases and Processes, describes specific component self-governance actions required to support the Department's governance processes embedded in text boxes under the title 'Component Self-Governance' found at the end of each process description sub-section.

3. Governance Phases and Processes

The IT Governance Investment Life Cycle Model, introduced in Section 2.2 of this guide, provides the framework for the processes that are discussed in this section. The model portrays the end-to-end processing needs for the Department's IT governance. It contains three sequential life cycle phases for IT planning, budgeting, and oversight, and each phase contains two or more governance processes. In this section, each phase is briefly reintroduced to provide context, followed by a detailed discussion of each process in the phase.

Each process is discussed in three parts. The first part contains a brief discussion of the high-level activities within the process, a summary diagram depicting the sequence of the high-level activities, and a definition of the resulting product(s).

The second part provides expanded detail on the workings of the process. It contains a process diagram that depicts the flow of lower-level sub processes and shows stakeholder involvement using swim lanes. For each lower-level sub process, a brief description is provided.

The third part describes the Department's requirements for component self-governance. For some processes, the Department requires components to perform like or similar processes.

3.1 IT Planning Phase

The first phase of the governance life cycle is the IT planning phase. It begins with strategic planning, which defines the Department's strategic goals and priorities, and culminates with IT investment planning, which produces the IT investment plan and guides IT budget decisions.

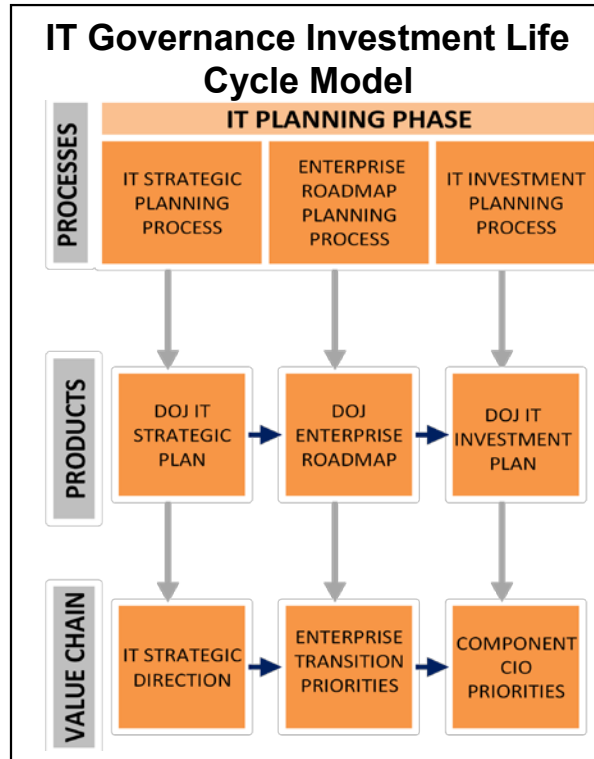


Figure 3-1: IT Planning Phase

The IT planning phase consists of three major planning processes, each generating one key Department-level planning document.

- The DOJ IT strategic planning process generates the Department's IT Strategic Plan.
- The DOJ enterprise roadmap planning process generates the Department's enterprise roadmap.
- The DOJ IT investment planning process produces the Department's IT investment plan.

The IT planning phase is designed to transform the mission and business drivers from the Department's strategic plan into a prioritized investment plan to guide the formulation of the Department's IT budget. The following sections describe the IT planning phase processes that produce the Department's IT plans, summarizes the contents of the process outputs, identifies the responsibilities of the process stakeholders, and specifies the associated requirements for component self-governance.

3.1.1 IT Strategic Planning Process

The DOJ IT Strategic Plan provides the Department CIO's vision and strategic goals and objectives for evolving the IT program in support of the Department missions. The plan identifies business and mission challenges that face the Department, key mission and technology support drivers, and ultimately the key strategies, programs, and actions that the Department will undertake to respond to these challenges.

The OCIO activities in the Department IT strategic planning process include the following: examine the current state of the Department's IT enterprise and its support of the Departmental mission and objectives; determine and define IT strategic goals and programs; assign priorities, performance goals, indicators and metrics; and produce the Department's IT Strategic Plan.

The plan covers a three to five-year period and drives the Department's enterprise architecture and IT capital planning. Since the plan covers a multi-year period, a new plan is not developed every year; however, the plan is reviewed annually to determine if updates are needed to keep the plan current. While minor updates to the plan may be made every year, major plan revisions are expected to occur roughly in conjunction with the induction of each new administration.

- Members of the DOJ CIO Council help craft the strategies in the IT Strategic Plan, and play essential roles in its execution to meet the Department's IT goals.
- The goals of the strategic plan serve the Department's customers, which include DOJ employees, private industry and citizens, federal agencies, foreign governments, state, local and tribal organizations, and non-government organizations.

Component Self-Governance

Component responsibilities in the IT Strategic Planning Process:

- Component CIOs should help craft, endorse and execute the IT Strategic Plan with the input and support of their component's IT community
- Components should align their IT Strategic Plans with the Department's plan

3.1.2 Enterprise Roadmap Planning Process

The Enterprise Roadmap planning process is the second major process of the IT planning phase. This process satisfies the requirements for IT architecture planning contained in the OMB Enterprise Architecture (EA) Assessment Framework and the EA Practice Guidance.

In alignment with the IT strategic plan, PortfolioStat and the ITIM strategy, the enterprise roadmap is the authoritative reference that details the Department's current and future views of its business and technology environment from an architecture perspective. It does so by reflecting the implementation of new or updated business capabilities and enabling technologies that support the Department's strategic goals and initiatives. Moreover, the Enterprise Roadmap focuses on increasing and leveraging shared approaches to IT service delivery across mission, support, and commodity areas.

The DOJ Enterprise Roadmap provides the necessary organizational self-awareness for strategic self-assessment adaptation and transformation, and fulfills the DOJ business and strategic drivers to achieve business services excellence. The Roadmap is a reference to how EA is managed and governed within the Department and provides the transparency and business value that EA provides. The Roadmap provides a high-level view of the current and future state of the DOJ enterprise and the key IT modernization activities and governance structures/processes to enable the successful organizational transformation from the current to the future state.

The Roadmap consists of IT investments, commodity IT, and IT initiatives, and is based on the common approach to federal enterprise architecture that provides guidance on how EA will be developed and used throughout the executive branch of the Federal Government. The Department uses a structured approach, illustrated in Figure 3-2, to document the Roadmap and its alignment to the IT Strategic Plan.

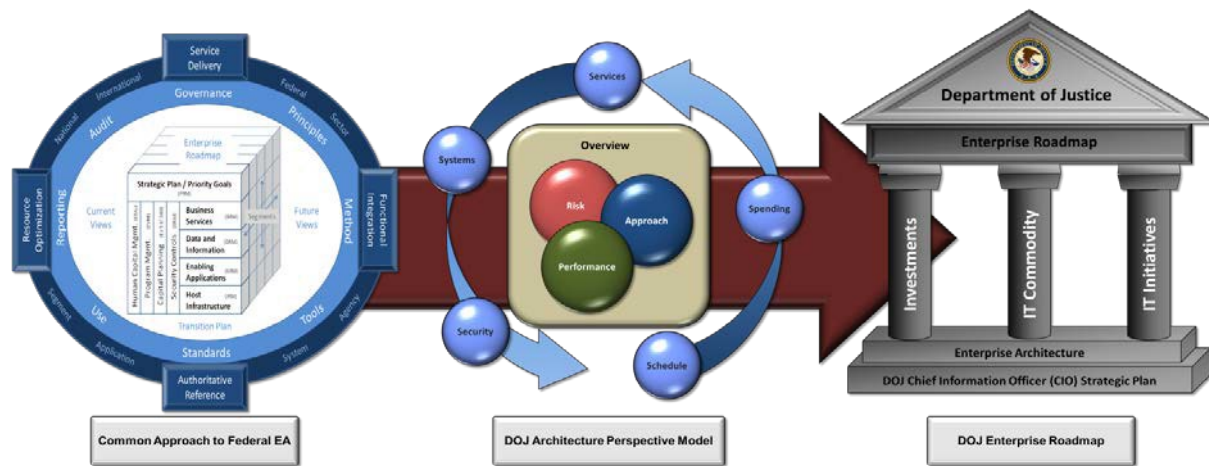


Figure 3-2: DOJ EA Structured Approach

When developing the roadmap and assessing IT alignment to the mission, the DOJ EA leverages federal best practices from the Federal Enterprise Architecture (FEA), Common Approach to federal EA, and the collaboration and planning methodology. The Enterprise Architecture Program Management Office (EAPMO) regularly interacts with all DOJ Components and collects specific information about the IT Portfolio based on the four outcomes of the common approach to EA: service delivery, functional integration, resource optimization, and authoritative reference. Information collected from this process is used to update the EA database and is reflected in EA documentation.

Incorporating the common approach, including the four federal outcomes, with the DOJ architecture description produces a roadmap that provides a broad overview of IT activities occurring across the enterprise. These IT activities are grouped into three different categories: investments, commodities, and initiatives. Each section of the roadmap identifies the critical IT investments, commodity areas, and initiatives that support its services and mission needs. The summary process diagram below illustrates the high-level tasks within the process, the process outputs, and the connection to other processes in the IT governance lifecycle.



Figure 3-3: Enterprise Roadmap Timeline

The Enterprise Roadmap timeline is illustrated in Figure 3-3, which shows the sequence of the processes and the stakeholders involved in the progression. The following processes are completed by DOJ EAPMO:

- **Identify Business Needs**
 - Incorporate the IT priorities described in the IT Strategic Plan and the Department mission priorities
 - Map the IT strategic plan goals and Department mission goals with identified IT investments from PortfolioStat
- **Prioritize Improvement Opportunities**
 - Validate investment alignment
 - Review and prioritize investments in DOJ portfolio based on 70 percent IT spends
 - Review and identify IT commodity spend
 - Identify IT initiatives
- **Define Projects and Milestones**
 - Collaborate with components on updates to their investments, to include approach, risk, and performance
 - Collaborate with components on updates to the architecture description for each investment with system(s), services, security, spending, and schedule
 - Incorporate component comments
- **Review and Communicate Enterprise Roadmap**
 - Review DOJ Enterprise Roadmap with components
 - Obtain CIO signature
 - Communicate the Enterprise Roadmap via CIO Council

Component Self-Governance

Component responsibilities in the Enterprise Roadmap planning process

- Update, review, and validate architecture description, approach, risk, and performance
- Develop the future state by updating the milestones for a five-year period and build out the future state description with system, services, security, spending, and schedule

3.1.3 IT Investment Planning Process

The IT investment planning process concludes the IT planning phase. In this process, the component CIOs identify their IT investment plans for the coming budget cycle, including defining current IT investment needs and prioritizing IT investments, based on mission and business priorities from their component business leaders and from the Department's Strategic Plan, IT Strategic Plan, and IT budget planning guidance. The component CIOs and business leaders collaborate to identify and prioritize IT investments that support component mission and business priorities and align with the Department's business and mission priorities and IT planning guidance.¹⁶ The component IT investment plans are transmitted via the Spring Call for review by JMD Budget Staff and in consultation with the CIO. The component's internal IT portfolio summary serves as the component's IT investment plans for the budget formulation year.

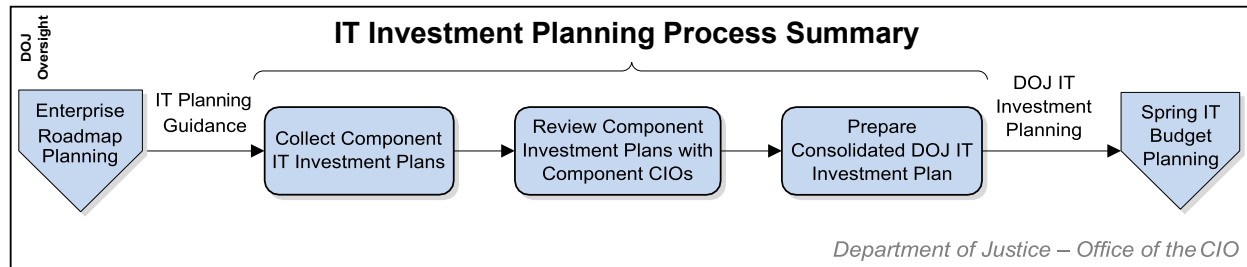


Figure 3-4: IT Investment Planning Process Summary

The DOJ IT portfolio summary identifies the investments with the highest priority for new funding that the DOJ CIO is able to support as the Department's OMB budget submission is formulated.

¹⁶ Investments are characterized as being IT based on the definition of IT provided in Section 1.3, and expanded in Appendix B – Definition of IT for DOJ.

The following process diagram shows the sequential sub-processing for the IT investment planning process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described following the model.

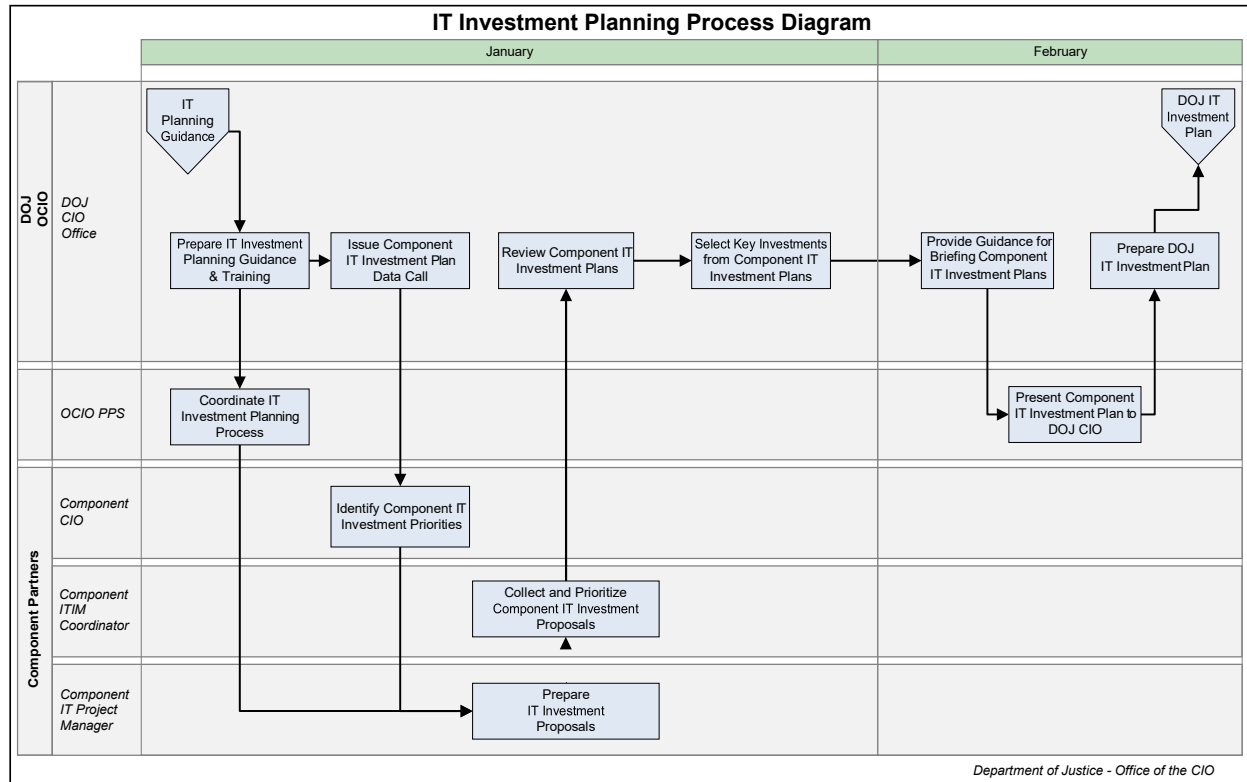


Figure 3-5: IT Investment Planning Process Diagram

- **Prepare IT Investment Planning Guidance & Training:** The DOJ OCIO will
 - Develop IT investment planning instructions that include the investment planning schedule, IT planning guidance, EA guidance, and Department planning priorities
 - Update the component IT investment plan template and the instructions for completing the template
- **Coordinate IT Investment Planning Process:**
 - The DOJ OCIO PPS will serve as the lead for coordinating interactions between the components and the DOJ OCIO during the IT investment planning process
 - Develop materials necessary to train the component ITIM coordinators who will prepare the component IT investment plans
 - Schedule training session

- **Identify Component IT Investment Priorities:** The component CIO will
 - Work with component business leaders to identify IT investment requirements that support mission and business priorities
 - Prioritize proposed IT investments with component business leaders
- **Prepare IT Investment Proposals:** The component IT project manager will
 - Develop new investment or enhancement proposals for the upcoming budget cycle
 - Provide the proposals to the component ITIM coordinator for review and inclusion in the Spring Call submission.
- **Collect and Prioritize Component IT Investment Proposals:** The component ITIM coordinator will
 - Collect IT investment budget proposals from the component IT project managers
 - Work with the component EA team to align the investment proposals using the Department IT planning guidance
 - Work with the component CIO to prioritize the IT investment proposals using the IT planning guidance and internal component priorities, as appropriate
 - Prepare the component IT investment plan and submit it to DOJ OCIO for review
- **Review Component IT Investment Plans:** The DOJ OCIO will
 - Collect the component IT investment priorities
 - Evaluate the IT investment proposals in the component IT investment plans for alignment, performance, and compliance using the EA transition guidance, DIRB summary reports and results from the investment compliance report, as appropriate
 - Recommend to the DOJ CIO key IT investments that should be discussed during the component IT investment plan briefings
- **Select Key IT Investments from Component IT Investment Plans:** The DOJ CIO will select key component IT (prospective) enhancement requests and special areas of interest for component CIOs to discuss during the component IT investment plan briefing.
- **Provide Guidance for Briefing Component IT Investment Plans:** The DOJ OCIO will
 - Develop the component IT investment plan briefing materials, including a proposed schedule, a list of key investments and suggested issues to discuss in the briefing and instructions for completing the briefing template
 - Issue the component IT investment plan briefing guidance to investor components
- **Present Component IT Investment Plan to DOJ CIO:** The component CIO will develop and present a briefing to the DOJ CIO that highlights the component's key IT enhancement requests.

- **Prepare DOJ IT Investment Plan:** The DOJ OCIO will
 - Help the DOJ CIO review investment proposals
 - Finalize the DOJ IT investment plan
 - Work with and advise JMD Budget Staff on IT enhancement requests submitted by components as part of the Spring Call.

Component Self-Governance

Responsibilities for designated components during the IT investment planning process:

- Develop and implement a process for collecting component IT investment proposals to support mission needs and IT integration objectives
- Establish a repeatable method for prioritizing IT investment proposals included in the component IT investment plan submitted to the DOJ OCIO

3.2 IT Budgeting Phase

The second phase of the governance life cycle is the IT budgeting phase. It begins with the completion of investment planning and concludes when Congress enacts and the President signs into law the Department's appropriation.

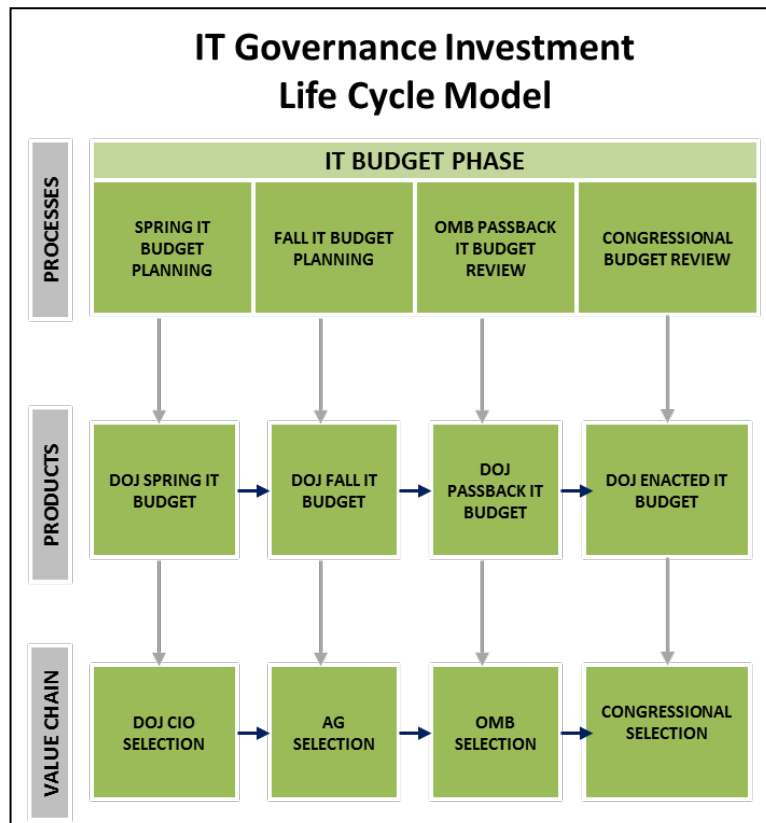


Figure 3-6: IT Budget Phase

The IT budget phase runs for approximately 18 months, spanning the third and fourth quarters of the planning year and the entire period of the year leading up to enactment of the Department's appropriation. Because the IT budget phase lasts for more than a year, it is important to recognize that the budgets for two succeeding fiscal years are usually under review concurrently, albeit at different stages.

The IT budget phase consists of four processes that deliver four key products:

- The spring IT budget planning process produces the DOJ spring IT budget
- The fall IT budget planning process produces the DOJ fall IT budget
- The OMB passback IT budget review process produces the DOJ passback IT budget
- The Congressional budget review process produces the DOJ Enacted IT Budget

3.2.1 Spring IT Budget Planning Process

During the spring IT budget planning process, the components use internal ITIM selection processes to prepare their IT budget requests. The DOJ OCIO collects the component IT budget requests, evaluates them against the Department IT investment objectives and priorities, prepares the DOJ spring IT budget recommendation, and submits the budget recommendation for review by the JMD Budget Staff.

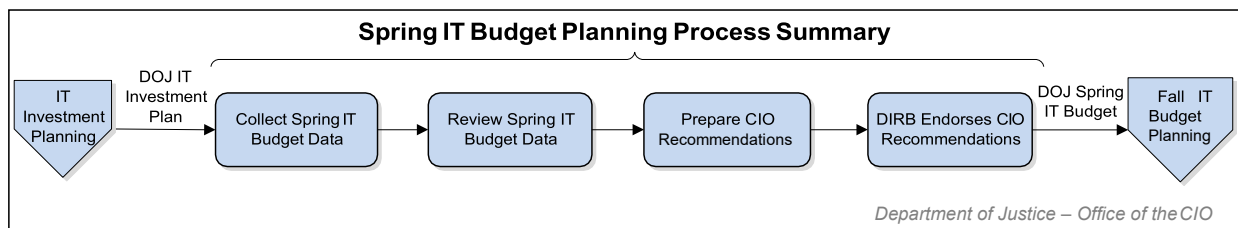


Figure 3-7: Spring IT Budget Planning Process Summary

The DOJ spring IT budget is the DOJ CIO recommended portfolio for IT investment for the budget year. It is reviewed by the Department senior leadership during the fall IT budget planning process as input to final Department budget decisions.

The process diagram in Figure 3-8 shows the sequential sub-processing for the spring IT budget planning process and the swim lanes show the responsible stakeholder for each activity. The activities are described below. Activities shown in light blue in the process diagram are general budget planning steps. Activities shown in light green directly support the preparation of the Major IT Business Case (formerly known as the OMB Exhibit 300).

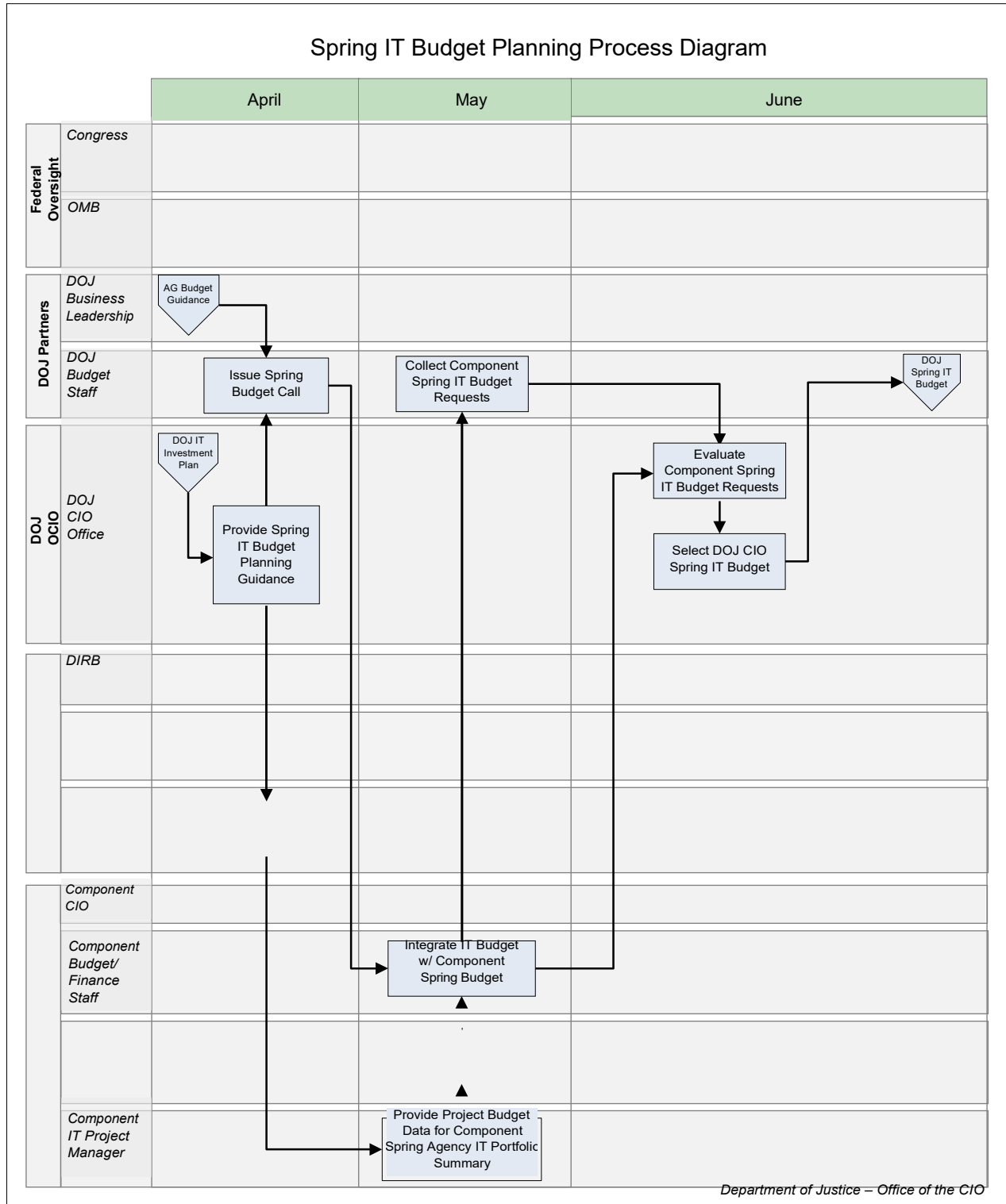


Figure 3-8: Spring IT Budget Planning Process Diagram

- **Prepare Spring IT Budget Planning Guidance and Training:** The DOJ OCIO will
 - Prepare spring IT budget planning guidance to include the schedule, the investment priorities from the DOJ IT investment plan, and instructions for completing the component Agency IT Portfolio Summary (formerly known as the OMB Exhibit 53)
 - Provide the spring IT budget planning guidance to the JMD Budget Staff for inclusion in the Department's spring budget call
 - Update or re-issue criteria for identifying investments that require preparation of a capital asset plan and business case summary of the Major IT Business Case
 - Prepare materials for training the component ITIM coordinators to complete the component Agency IT Portfolio Summary and schedule the training sessions
- **Issue Spring Budget Call:** The JMD Budget Staff will
 - Incorporate the attorney general's budget planning guidance and the OCIO IT budget planning guidance into the Department spring budget call instructions
 - Issue the spring budget call to components
- **Support Spring IT Budget Planning and Training:** The DOJ OCIO PPS will support the budget planning process by: reviewing and distributing IT budget planning schedules, providing component feedback for IT budget exhibit templates and addressing other component issues during the IT budget planning process
- **Provide Project Budget Data for Component Spring Agency IT Portfolio Summary:** The component IT project manager will provide project budget data to the component ITIM coordinator for inclusion in the spring Agency IT Portfolio Summary
- **Collect and Prioritize Component Spring IT Budget Request:** The component ITIM coordinator will
 - Collect project budget data from component IT project managers
 - Engage the component CIO to prioritize the spring IT budget requests using the DOJ IT investment planning guidance
 - Work with the component budget/finance staff to prepare the spring component Agency IT Portfolio Summary detailing the IT investments in the component spring budget request
 - Ensure that all investments that meet the definition of IT (provided in Section 1.2) are included in the spring component Agency IT Portfolio Summary
- **Integrate IT Budget with Component Spring Budget Request:** The component budget/finance staff will
 - Work with the component ITIM coordinator to prepare the spring component Agency IT Portfolio Summary
 - Ensure that all investments that meet the definition of IT are included in the spring component Agency IT Portfolio Summary
 - Submit the component spring budget request and component Agency IT Portfolio Summary to the JMD Budget Staff and to the DOJ OCIO

- **Collect Component Spring IT Budget Requests:** The JMD Budget Staff will collect components' spring budget requests and IT Agency Portfolio Summaries, and forward to the DOJ OCIO for review and preparation of the DOJ spring IT budget
- **Select DOJ CIO Spring IT Budget:** The DOJ OCIO will
 - Review component Agency IT Portfolio Summary for timeliness and completeness
 - Reconcile component Agency IT Portfolio Summary with component budgets
 - Consolidate the component IT budget requests into a draft CIO's IT budget recommendation working document
 - Evaluate the component IT budget requests using EA transition guidance and information from investment compliance reports to assign a recommended priority ranking to each request
 - Conduct a preliminary budget review with the DOJ OCIO staff directors and CIO Council Governance Committee and develop proposed investment rankings in preparation for the CIO spring IT budget review
 - Help DOJ CIO prioritize the component IT investments in the spring IT budget
 - Update Folio to reflect the CIO's IT budget recommendation so that the draft Agency IT Portfolio Summary can be produced. Folio is a GSA-managed modern IT portfolio management application that replaced the Electronic Capital Planning and Investment Control (eCPIC) in 2020. Amongst other benefits, Folio enables more efficient IT budget management, greater insight into IT portfolio performance, and improved support for FITARA implementation.
 - Submit the DOJ spring IT budget to the JMD Budget Staff as the CIO's IT budget recommendation

Component Self-Governance

Component responsibilities for the spring IT budget planning process

- Develop and implement a repeatable process for collecting IT budget requests to support mission needs and IT integration objectives.
- Establish a repeatable method for evaluating and prioritizing IT budget requests against internal component mission priorities and the DOJ IT investment plan guidance.
- Work with the component budget/finance staff to align component budget processes.

3.2.2 Fall IT Budget Planning Process

During the fall IT budget planning process, the Department's senior leadership selects the IT investments to be included in the Department's fall budget request to OMB. To accomplish this, the DOJ leadership reviews the DOJ spring IT budget recommendation from the DOJ CIO and the Attorney General (AG) determines final budget priorities and funding levels. The Components then modify their IT budgets to align with the AG's decisions and the DOJ OCIO prepares the DOJ fall IT budget for OMB review. The process occurs during the fourth quarter of the fiscal year. During this process, the Major IT Business Cases are prepared, reviewed, and submitted to OMB with the DOJ fall IT budget.

The process summary (Figure 3-9) and diagram (Figure 3-10) shows the sequence of activities for the fall IT budget planning process and the swim lanes show the responsible stakeholder for each activity. The activities are described on the following pages. Blue rectangles in the process summary and diagram represent general IT budget preparation steps, while activities in green ellipses directly support the preparation and review of the Major IT Business Case. Half-blue half-green stadiums represent both general IT budget preparation and the preparation and review of the Major IT Business Case.

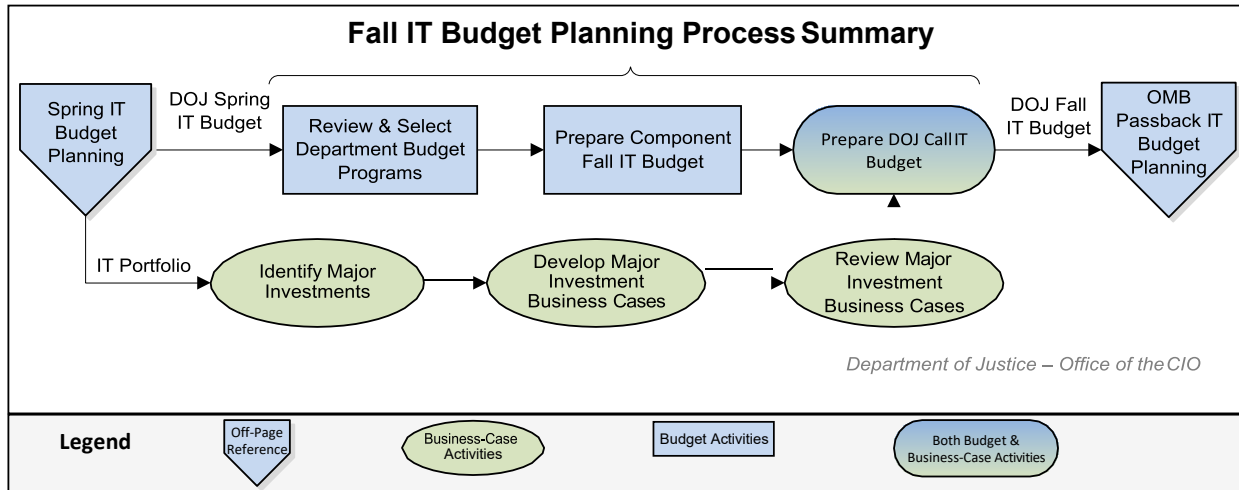


Figure 3-9: Fall IT Budget Planning Process Summary

The DOJ fall IT budget contains the final set of IT investments approved by the Attorney General and consists of the following IT budget and management report components:

- **Agency IT Investment Portfolio Summary:** Includes IT investment budget, management, and architecture information
- **Agency Provisioned IT Services Spending Summary:** Includes IT investment budget and management information by cloud computing deployment model and service model
- **Agency IT Infrastructure Spending Summary:** Includes a detailed spending breakout on all aspects of an agency's IT Infrastructure
- **Major IT Business Case:** Includes detailed IT investment budget and management information for major IT investments

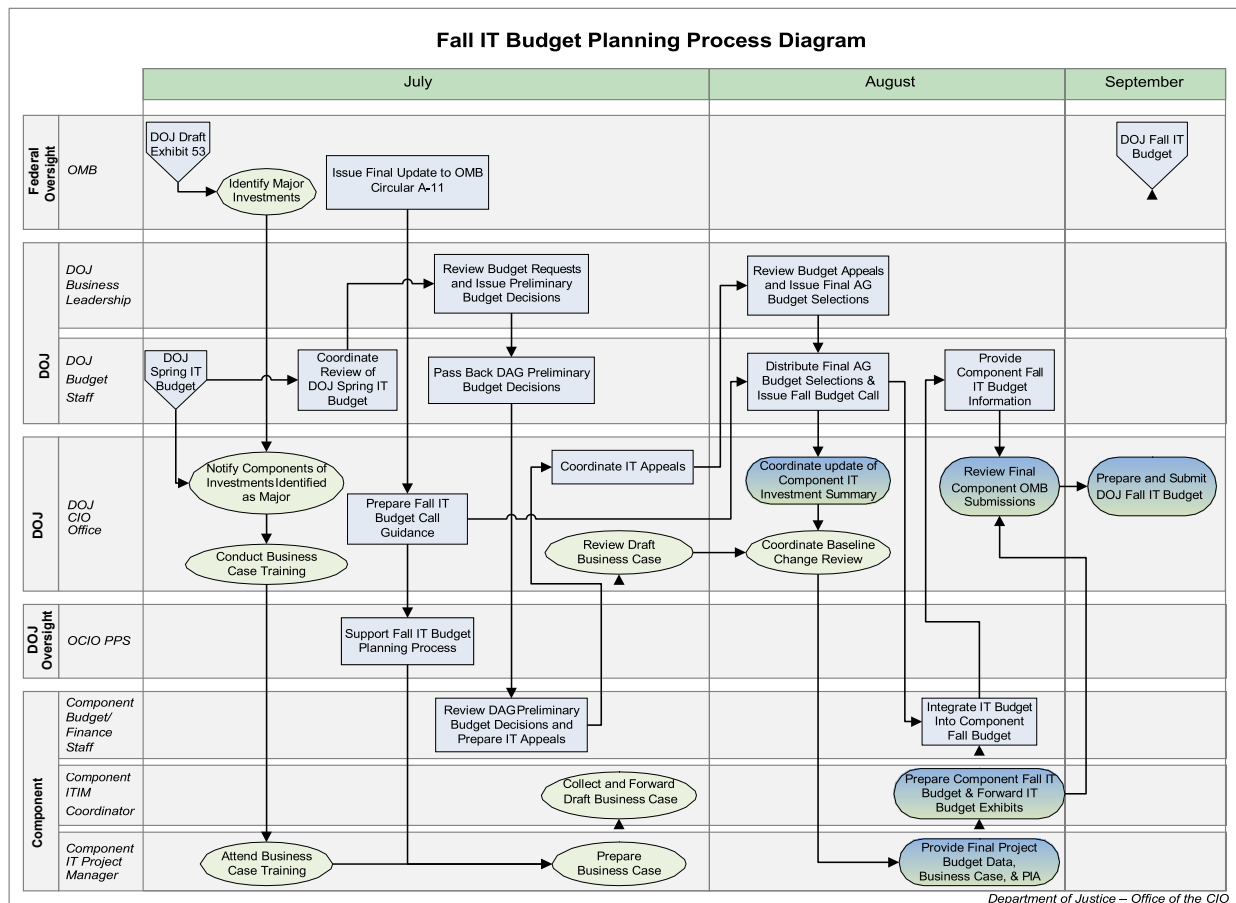


Figure 3-10: Fall IT Budget Planning Process Diagram

- **Coordinate Review of DOJ Spring IT Budget:** The JMD Budget Staff will
 - Review the DOJ spring IT budget for alignment with DOJ budget priorities and provide budget recommendations for consideration by senior leadership
 - Coordinate the review of the spring IT budget by the Department’s senior leadership team for selection of the fall Department budget
- **Identify Major IT Investments:** OMB will review DOJ’s draft Agency IT Portfolio Summary, select IT investments that require a Major IT Business Case, and inform the DOJ CIO of the investments selected
- **Notify Components of Investments Identified as Majors:** The DOJ OCIO will notify components of the investments that are identified as major investments that will require an investment business case

- **Conduct Major IT Business Case Training:** The DOJ OCIO will train the component IT project managers to prepare/update their major IT investment business case
- **Attend Major IT Business Case Training:** The component IT project manager will attend the Major IT Business Case training provided by the DOJ OCIO
- **Issue Final Update to OMB Capital Planning Guidance:** OMB will issue the final version of OMB Capital Planning Guidance for the fall budget submission, including the Agency IT Portfolio Summary, Agency Provisioned IT Services Spending Summary, Agency IT Infrastructure Spending Summary, and Major IT Business Case templates, and submission instructions
- **Prepare Fall IT Budget Call Guidance:** The DOJ OCIO will
 - Review the final updates to OMB capital planning guidance
 - Prepare fall IT budget call instructions including the schedule, templates, and instructions for preparing the component IT Portfolio Summary, Provisioned IT Services Spending Summary, IT Infrastructure Spending Summary, and Major IT Business Cases
 - Provide the IT budget call schedule to JMD Budget Staff for inclusion in the Department's fall budget call
- **Support Fall IT Budget Planning Process:** The OCIO PPS will support the fall IT budget planning process by distributing IT budget planning information and serving as the lead for resolving component IT budget planning issues
- **Review Budget Requests and Issue Preliminary Budget Decisions:** The DOJ business leadership will
 - Review spring IT budget requests and make preliminary budget selections for the Department's fall budget
 - Provide the preliminary budget decisions to the JMD Budget Staff for review and appeal
- **Pass Back DAG Preliminary Budget Decisions:** The JMD Budget Staff will distribute the results of the DAG preliminary budget review to components and provide instructions for the submission and review of budget appeals
- **Review DAG Preliminary Budget Decisions and Prepare IT Appeals:** The component budget/finance staffs will
 - Coordinate review of the DAG preliminary budget decisions
 - Work with the component CIO to identify any impacts to critical IT investments
 - Prepare and submit appeals, when appropriate, according to the appeals process
- **Coordinate IT Appeals:** The DOJ OCIO will coordinate the preparation of appeals for critical IT investments for the AG's final budget review.

- **Prepare/Update Draft Major IT Business Case:** The component IT project manager will
 - Prepare the draft Major IT Business Case for investments selected by OMB
 - Forward the draft Major IT Business Case to the component ITIM coordinator for internal component review and approval
 - Update/Revise as needed
- **Collect and Forward Draft Major IT Business Cases:** The component ITIM coordinator will
 - Collect the draft Major IT Business Cases from component IT project managers
 - Coordinate internal review of the major IT business cases for accuracy and completeness
 - Ensure that the draft Major IT Business Cases are entered into the DOJ Folio investment management tool
 - Notify the DOJ OCIO when the draft component Major IT Business Cases have been entered into Folio and are ready for review and comment
- **Review Draft Major IT Investment Business Cases:** The DOJ OCIO will
 - Review the draft Major IT Business Cases against review criteria provided in the DOJ IT capital planning and investment control guide and identify weaknesses
 - Inform the components of weaknesses discovered and provide recommended corrective actions
- **Review Budget Appeals and Issue Final Attorney General (AG) Budget Decisions :** The DOJ business leadership will
 - Review budget appeals submitted by components for consideration by the AG
 - Issue final AG budget decisions for the fall budget call
- **Distribute Final AG Budget Decisions and Issue Fall Budget Call:** The JMD Budget Staff will
 - Distribute the final AG budget decisions to the components
 - Issue fall budget call, including schedule for submitting IT budget exhibits
- **Coordinate Update of Component Documents:** The DOJ OCIO will provide components with instructions for the review of component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary with AG's final budget selection changes
- **Coordinate Major IT Business Case Baseline Change Review:** The DOJ OCIO will provide components with instructions for the review of Major IT Business Cases with proposed project baseline changes.
- **Provide Final Project Budget Data and Major IT Business Case:** The component IT project manager will

- Update the investment budget data and align it with the AG's budget decisions
 - Provide final investment budget data to the component ITIM coordinator for inclusion in the fall component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary
 - Update and align the IT investment budget data and project plan in the Major IT Business Case with the data submitted for the component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary
 - Forward final business case to component ITIM coordinator
- **Prepare Component Fall IT Budget:** The component ITIM coordinator will
 - Incorporate project budget updates into the component IT budget request
 - Work with the component budget/finance staff to align the component IT budget with the AG final budget decisions and prepare the fall component Agency IT Portfolio Summary
 - Collect final Major IT Business Cases and PIAs from the component IT project managers
 - Ensure the final Major IT Business Cases data and Agency IT Portfolio Summary data is entered into the DOJ CIO's Folio investment management tool and notify the DOJ OCIO when Major IT Business Cases are ready for review and submission to OMB
 - Forward new or updated PIAs to DOJ OCIO for review
- **Integrate IT Budget into Component Fall Budget:** The component budget/finance staff will
 - Work with the component ITIM coordinator to align the component IT budget with the AG final budget decisions and prepare the fall component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary
 - Submit the component fall budget, Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary to the JMD Budget Staff and DOJ OCIO
- **Provide Component Fall IT Budget Information:** The JMD Budget Staff will
 - Collect the component fall budgets from the component budget/finance staffs
 - Forward the fall component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary to DOJ OCIO to support review of the component fall IT budget and preparation of the DOJ fall IT budget
- **Review Component Final Documents:** The DOJ OCIO will
 - Collect final component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary from the JMD Budget Staff
 - Reconcile summaries with component fall budgets and identify any discrepancies
 - Review the final Major IT Business Cases from components.

- Evaluate the component budget exhibits for timeliness and completeness
 - Notify component ITIM coordinators when corrective action is needed
 - Prepares a component Agency IT Portfolio Summary, Agency IT Provisioned Services Spending Summary, and Agency IT Infrastructure Spending Summary for each component budget account and sends a copy to JMD Budget Staff
- **Prepare and Submit DOJ Fall IT Budget:** The DOJ OCIO will
 - Prepare the IT capital plan as specified by OMB Capital Planning Guidance
 - Prepare the final DOJ Agency IT Portfolio Summary, Agency Provisioned IT Spending Summary, and Agency IT Infrastructure Spending Summary for submission to OMB
 - Submit the IT capital plan, Agency IT Portfolio Summary, Agency Provisioned IT Spending Summary, Agency IT Infrastructure Spending Summary, and Major IT Business Cases to OMB in the format prescribed in OMB Capital Planning Guidance

Component Self-Governance

Component responsibilities for the fall IT budget planning process

- Review Department budget decisions, identify items for appeal, and prepare budget appeal justifications
- Implement a repeatable process for collecting and reviewing major investment business case for major investments, as required
- Work with the component budget/finance staff to align the component agency portfolio, cloud spending, and infrastructure-spending summaries with AG final budget decisions

3.2.3 OMB Passback IT Budget Review Process

During the first quarter of the fiscal year, OMB reviews the Department's fall IT budget request and provides DOJ a passback package detailing its review decisions. OMB also reviews and provides feedback on Major IT Business Cases. The Department updates the IT program budgets and investment business cases for OMB to incorporate into the President's Budget.

There is the opportunity for the Attorney General to make a formal appeal to OMB's decisions within a very concise window. Appeals may include resurfacing priority IT initiatives, and the OCIO will work with components, as necessary, to justify IT initiatives upon appeal.

The passback process is summarized in Figure 3-11 and detailed in the process diagram in Figure 3-12. The process diagram shows the sequential sub-processing for the congressional budget planning process and the swim lanes show the responsible stakeholder for each sub-process. The sub-processes are described on the pages following the diagram. Sub-processes shown in light blue rectangles in the process diagram are general budget planning steps. Sub-processes shown in light green ovals directly support the preparation and review of DOJ's major IT investment business cases and agency IT portfolio. Sub-processes that are part blue and part green stadiums involve general budget preparation and review of DOJ Major IT Business Cases and Agency IT Portfolio.

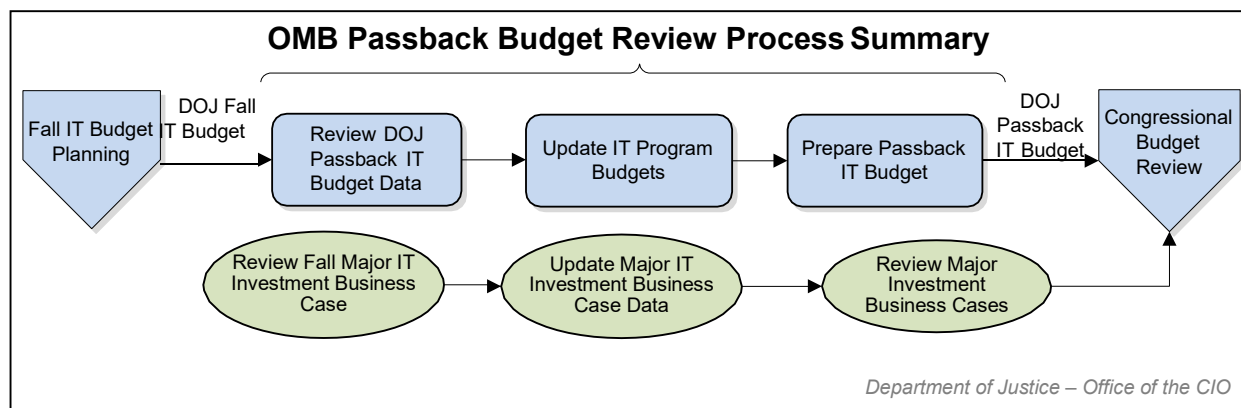


Figure 3-11: OMB Passback IT Budget Review Process Summary

The DOJ passback IT budget contains the final budget request agreed upon by OMB and the Department. OMB incorporates the passback IT budget into the President’s Budget that will be submitted to the Congress for review and enactment of budget legislation.

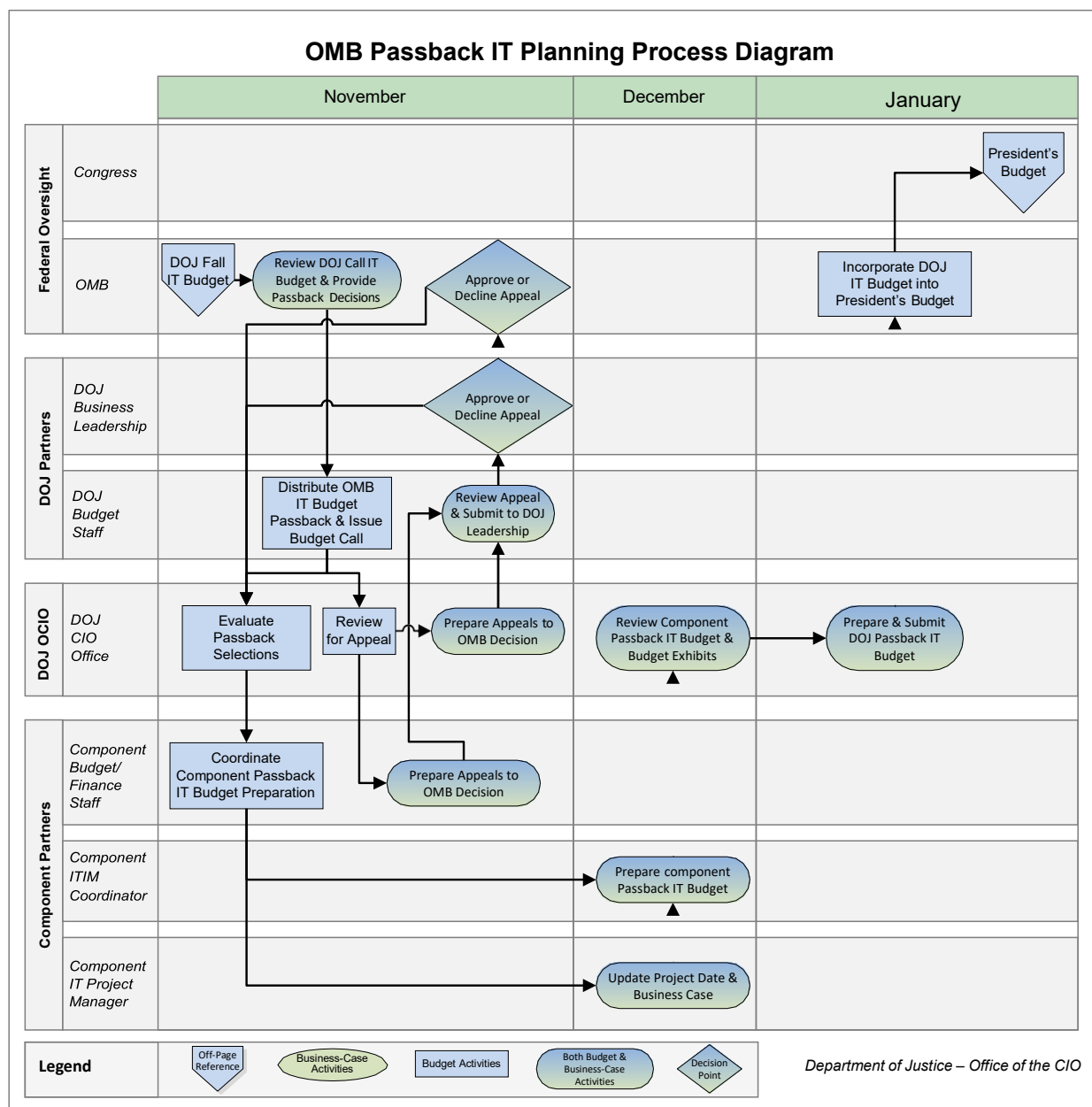


Figure 3-12: OMB Passback IT Planning Process Diagram

- **Review DOJ Fall IT Budget & Provide Passback Selections:** OMB will
 - Review the DOJ IT budget as part of the Department budget review
 - Provide budget passback decisions to the JMD Budget Staff
 - Review DOJ Major IT Business Cases and provide results to the DOJ OCIO

- **Distribute OMB IT Budget Passback & Issue Passback Budget Call:** The JMD Budget Staff will
 - Review OMB passback and distribute IT budget decisions to DOJ CIO
 - Coordinate presentation of budget appeals to OMB and communicate appeal decisions to the components concerned
 - Provide instructions to components for submitting OMB passback budget revisions
- **Evaluate OMB IT Budget Passback Decisions:** The DOJ OCIO will
 - Review the OMB IT budget passback to identify the effects on IT projects
 - Work with JMD Budget Staff and component CIOs to submit IT program appeals and to adjust IT budgets, when necessary.
 - Coordinate passback action times from OMB for the CIO
- **Review for Appeal:** The DOJ OCIO will review the OMB IT budget passback to identify any items that should be appealed
- **Prepare Appeal to OMB Decision:** The DOJ OCIO and component budget staff will prepare any necessary appeal(s) justification and forward to the JMD Budget Staff
- **Review Appeal & Submit to DOJ Leadership:** The JMD Budget Staff will review any IT budget appeals it receives and prepare decision by the DAG. The DAG in turn forwards agreed upon recommended appeals to the AG, who reviews and finalizes Department appeal decisions to OMB.
- **Approve or Decline Appeal:** OMB will review any appeals it receives, approve or decline, and notify the Department of the final disposition.
- **Coordinate Component Passback IT Budget Preparation:** The component budget/finance staff will distribute OMB passback decisions affecting component IT investments and coordinate any required updates of component IT budgets
- **Update Project Budget Data & Update DOJ Major IT Investment Business Cases as Required:** The component IT project manager will
 - Update project budget data to reflect OMB passback decisions
 - Update Major IT Business Cases with prior year actual data and budgetary changes, as required
 - Provide the updated project budget data and updated Major IT Business Cases to the component ITIM coordinator to update the component IT budgets in the Agency IT Portfolio
- **Prepare Component Passback IT Budget:** The component ITIM coordinator will
 - Collect updated project budget data from the component IT project managers

- Work with the component budget/finance staff to prepare the passback component portion of the agency IT portfolio
 - Collect updated Major IT Business Cases from component IT project managers and forward the updated Major IT Business Cases to the DOJ OCIO for review and submission to OMB
 - Update Folio to reflect the OMB’s budget for both DOJ Major IT Business Cases and agency IT portfolio investments
- **Review Component IT Budget & Budget Exhibits:** The DOJ OCIO will
 - Collect updated component agency IT portfolios and Major IT Business Cases from components and evaluate for accuracy and completeness
 - Reconcile portfolios with budget information from JMD Budget Staff and work with the component ITIM coordinators to resolve any discrepancies
 - **Prepare and Submit DOJ IT Budget:** The DOJ OCIO will
 - Prepare final business cases for submission to OMB
 - Update the DOJ Agency IT Portfolio for submission to OMB
 - Submit updated portfolio and business cases to OMB as instructed
 - **Incorporate DOJ IT Budget into President’s Budget:** OMB will incorporate the DOJ IT budget into the President’s Budget and submit to Congress for review

Component Self-Governance

Component responsibilities for the OMB passback IT planning process

- Define and implement a repeatable process for reviewing OMB passback decisions for impact to IT budget requests and selecting IT budget appeals, if necessary.
- Work with the component budget/finance staff to align the component agency IT portfolio with OMB budget decisions.
- Review and update investment cost data in Folio, and provide verification to the CIO

3.2.4 Congressional Budget Review Process

The purpose of the congressional budget review process is for the Congress to review the President’s Budget request and enact budget legislation to fund federal government operations for the coming fiscal year. This process occurs from February to September of each year. The process begins when the President’s Budget is transmitted to the Congress. Congress reviews the agency budget proposals in the President’s Budget and after deliberation and debate, drafts and enacts legislation to fund the DOJ Enacted IT Budget for the coming fiscal year. As part of this process, all OMB Major IT Business Cases must be made available for public access and review on the FITDB.

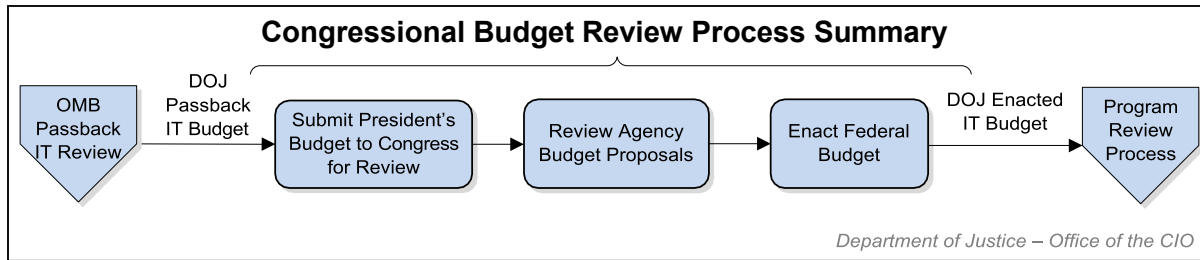


Figure 3-13: Congressional Budget Review Process Summary

The DOJ budget enacted by Congress specifies the funding authorized for IT investments for the coming fiscal year. The DOJ CIO and components are responsible for managing the funds appropriated to achieve desired program outcomes. These outcomes are continuously reviewed and assessed during the IT oversight phase.

The process diagram in Figure 3-14 shows the sequential sub-processing for the congressional budget review process and the swim lanes identify the stakeholder responsible for each activity. The activities are described on the pages following the diagram. Activities shown in light blue rectangles on the process diagram are general IT budget planning steps. Activities in light green ovals directly support preparation and posting of the OMB Major IT Business Cases on the FITDB.

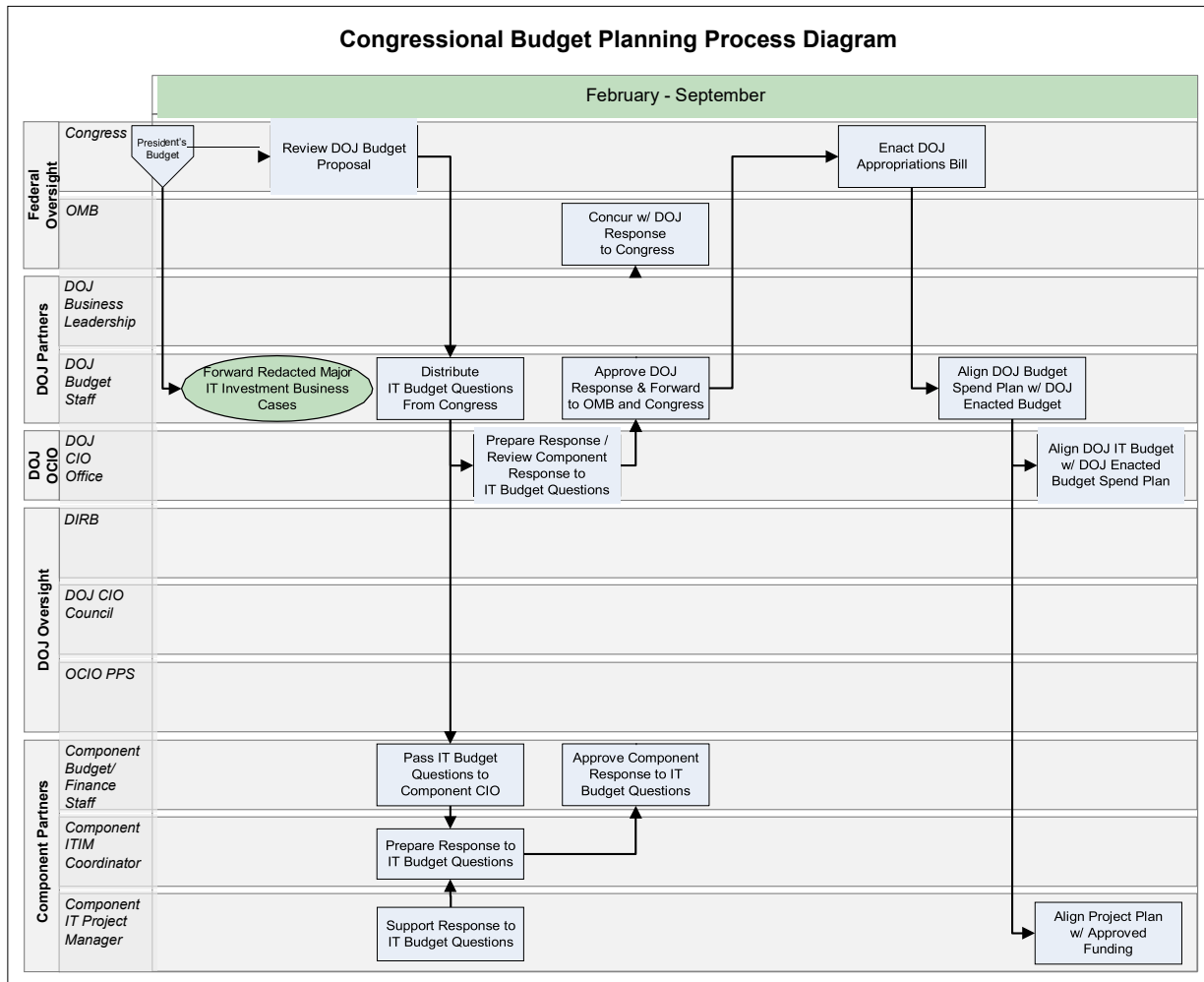


Figure 3-14: Congressional Budget Planning Process Diagram

During the course of congressional committee budget hearings and deliberations, the following actions occur:

- **Review DOJ Budget Proposal:** The congressional committees will
 - Review the Department's budget proposal in the President's Budget
 - Evaluate the programs and IT investments requested and prepare draft budget legislation
 - Submit questions for the record (QFRs) to the Department regarding funds for IT investments requested in the budget
 - Conduct budget hearings and draft appropriations and report language for legislative action

- **Distribute IT Budget Questions from Congress:** The JMD Budget Staff will distribute IT budget QFRs received from congressional committees for response by the DOJ OCIO or the component budget/finance staffs
- **Prepare Response / Review Component Response to IT Budget Questions:** The DOJ OCIO will prepare responses to congressional QFRs for DOJ CIO-managed investments and/or review component responses to IT budget questions, as needed
- **Pass IT Budget Questions to Component CIO:** The component budget/finance staff will work with component CIO offices preparing any responses to component-specific QFRs
- **Prepare Response to IT Budget Questions:** The component CIO organization will work with the component budget/finance staff and DOJ CIO, as required, to prepare a timely response to congressional QFRs
- **Support Response to IT Budget Questions:** The component IT project manager will provide information necessary to prepare responses to QFRs
- **Approve and Forward Component Response to IT Budget Questions:** The component budget/finance staff will review the proposed response prepared by the component OCIO and forward the proposed response to JMD Budget Staff for review and forwarding to Congress
- **Approve DOJ Response and Forward to OMB and Congress:** The JMD Budget Staff will
 - Review the proposed response submitted by the component and route it to the DOJ CIO for review and comment, as required
 - Forward the proposed response to OMB for review and concurrence
 - Forward the final response to OMB and Congress
- **Concur with DOJ Response to Congress:** OMB will review the Department's proposed response to Congress, recommend changes, when necessary and concur with the final response

After congressional committees have drafted the final appropriations bill, Congress enacts legislation authorizing the Department's budget. The major activities are

- **Enact DOJ Appropriations Bill:** Congress will negotiate the final appropriations bill and enact legislation to fund DOJ operations for the coming fiscal year
- **Align Budget Spend Plan with DOJ Enacted Budget:** The JMD Budget Staff will align the budget spend plan with the DOJ budget enacted into law
- **Align DOJ IT Budget with DOJ Enacted Budget Spend Plan:** The DOJ OCIO will work with components to align the DOJ IT budget with the DOJ enacted budget spend plan

- **Align Project Plan with Approved Funding:** The component IT project manager will align the project plan with the funds allotted from the DOJ Enacted IT Budget, and execute the project plan to achieve the funded project objectives

Component Self-Governance

Component responsibilities during the congressional budget planning process

- Provide IT investment information as needed to support the congressional budget review process.
- Review and update IT project plans and OMB major IT investment business cases as necessary to execute the enacted IT budget

3.2.5 Information Technology Infrastructure Library

3.2.5.1 IT Service Management Processes

The OCIO has adopted IT service management processes to align with the Information Technology Infrastructure Library (ITIL, version 3) best practices in order to improve service quality and overall value to the customer. The effort touches on all OCIO processes, staffs, IT services, IT infrastructure, and documentation.

During 2015, OCIO began modifying its current IT processes to conform to the ITIL guidelines and adhere to International Organization for Standardizing (ISO) 20000 standards. The primary objective of service management is to ensure that IT services are aligned with business needs. It is imperative that IT services underpin the business processes, but it is also increasingly important that IT act as an agent for change to facilitate business transformation. All organizations that use IT depend on IT to be successful. If IT processes and IT services are implemented, managed, and supported in the appropriate, consistent way, the business will be more successful, suffer less disruption and loss of productive hours, reduce costs, increase value, improve public relations, and achieve its business objectives. ITIL provides guidance throughout the service lifecycle to help senior business managers and IT managers achieve the objectives of service management and address the key issues they face in a systematic way.

3.2.5.2 OCIO Services Catalog

DOJ IT leadership is committed to a standards-based, enterprise shared services operating model. This operating model continuously identifies and effectively delivers information services across the enterprise, while supporting/enabling DOJ's mission and protecting its information assets.

The OCIO Services Catalog ensures that existing and potential customers of DOJ's enterprise and infrastructure service offerings across the Department are aware of current service offerings and the process for acquiring them. The service catalog provides a brief description of the capabilities provided under each service and describes, at a high level, the service level agreement, the process for acquiring the service; and the price of the service to be delivered. The OCIO Services Catalog is part of the process that aligns with ITIL best practices being implemented as a core methodology across OCIO. The catalog is structured into the following portfolios for existing and

future shared services.

- Application Services
- Enterprise Services
- Infrastructure Services
- Cybersecurity Services
- Data Center Services
- Future Services

As DOJ IT leadership improves and expands enterprise information services delivery, it seeks to take advantage of the economies of scale and consistency of performance achievable through enterprise-shared services. Services are expected to expand in this catalog to include new services as OCIO works with its business partners to understand demand and offerings for shared services expands.

3.3 IT Oversight Phase

The IT oversight phase is the third and longest phase of the IT governance life cycle. IT investments are funded in the previous phase and continuously monitored for satisfactory progress and results in the IT oversight phase. This phase monitors investments through their life cycle, beginning with planning and development, continuing through implementation and operations and maintenance (O&M) / service delivery, and concluding with retirement. Figure 3-15 shows how the IT oversight phase comprises both processes for executive review and compliance review, with IT investment performance reports as the output.

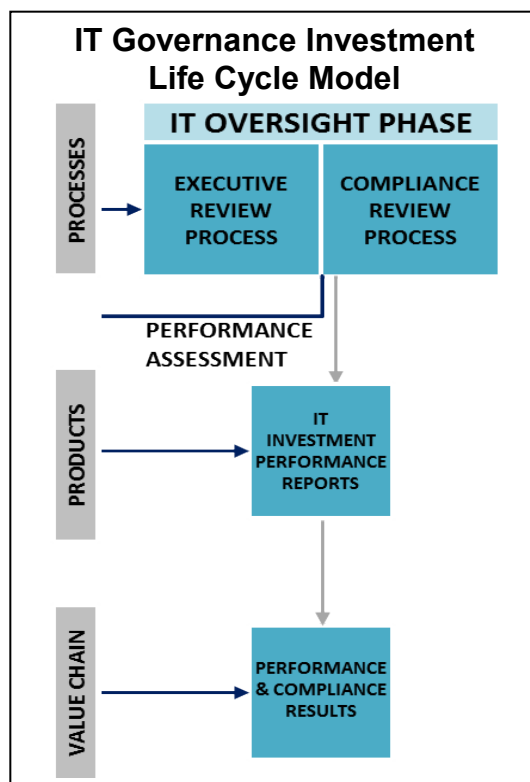


Figure 3-15: IT Oversight Phase

The executive review process monitors the Department’s most critical programs, audits component oversight processes involving those programs, and meets in-person with certain programs during the year based on thresholds or selection. The DIRC generates meeting summaries, action reports, program certification reports (as appropriate), and portfolio status reports.

The compliance review process ensures and facilitates regular and phase-based reporting and certifications. The process generates reporting on each individual investment, at the component, Department, and federal/OMB levels, as applicable.

The IT Oversight Model discussion in Section 2.8 describes the Department’s oversight structure, including key oversight stakeholders, the types of review processes and outcomes, and the interactions amongst oversight processes and other governance processes. The following sections describe the activities of the executive review and compliance review processes.

3.3.1 Executive Review Process

The Department executive review process applies to a select set of important investments¹⁷ that

¹⁷ Order 0903: Information Technology Management, p.5.

require executive oversight because of their high cost, risk, or visibility, or require specific review to comply with legislative requirements.¹⁸ Investments selected for investment review are typically multi-year development projects that influence or require integration with other important Department systems, programs, components, or other executive agencies. The DIRC performs the executive investment review for the Department's most critical IT programs. Components also perform executive reviews as part of the component self-governance model overviewed in Section 2.9.

The DIRC was chartered to oversee the management of the Department's IT investments and to ensure that these investments are aligned with the Department's mission and goals. Because the investment program-review process requires a high degree of coordination between project management offices (PMOs) and the board, the DIRC is supported by staff from OCIO PPS. The PPS is responsible for scheduling and coordinating review meetings, assisting PMOs in preparing for reviews and managing the various administrative functions of coordinating and publishing the DIRC schedule, preparing and posting reports, tracking completion of action items, and distributing project information to board members. The PPS supports the DOJ CIO on all matters concerning the DIRC and acts as the principal liaison between the board and the PMOs of projects being reviewed by the DIRC.

Each fall, the DOJ CIO and the DIRC review the Department's IT portfolio, select a set of critical investment programs to be monitored by the DIRC during the coming fiscal year, and establish a tentative investment review schedule. The DIRC reviews the progress of selected investments to ensure they are proceeding according to plan, remain sound investments for the Department, and continue to be relevant to component and the Department goals.

The board may direct the program manager or other stakeholders to complete specific corrective actions, provide reports, or prepare specific SDLC documentation to remedy deficiencies identified during the review. The results of each review are compiled into reports that document program status and monitor progress for subsequent reviews. The information in the reports is also used to support investment and budget planning decisions during the IT budget phase. Reprogramming actions during the year may also be reviewed and approved by the DIRC. The executive review process summary below provides an overview of the process, its outputs, and the connection to the IT budget phase.

¹⁸ Consolidated Appropriations Act, 2008: P.L. 110-161 Division B Title 2 SEC. 210 requires the DIRB to review and the DAG to certify that projects having total development costs over \$100M have "appropriate program management and contractor oversight mechanisms in place and that the program is compatible with the enterprise architecture."

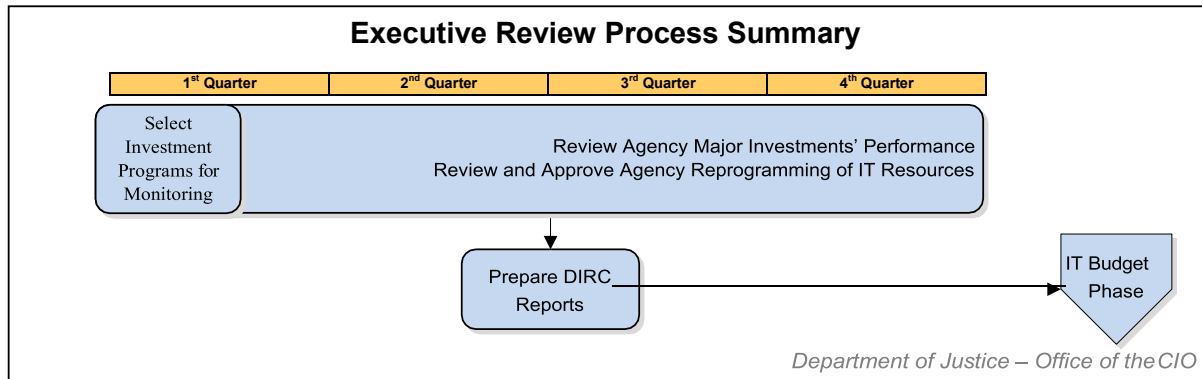


Figure 3-16: IT Governance - Executive Review Process

The DIRC outcomes produced from the executive review process serve the following purposes:

- Report status, progress, and completion of action items assigned by the DIRC
- Document meetings, identify key investment issues, and record action items assigned during a DIRC in-person review
- Review and approve agency reprogramming of funds involving IT resources
- Evaluate and issue oversight process guidance and action-plans for process improvement
- Report the DIRC's recommendation to the DIRB for investment certification according to requirements specified by Congress
- Make any appropriate recommendations to the DIRB regarding the suspension of funding for troubled investments (i.e. terminate, halt, re-scope, or de-scope investment)

Because the DIRC project review often includes business-sensitive and financial information, the investment review briefing, and DIRC Meeting Summary, are categorized and handled as "controlled unclassified information," (previously "sensitive but unclassified" information). If classified information is addressed before the DIRC, appropriate additional access and information handling procedures are implemented.

The following process diagram shows the sequential sub-processing for the investment review process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the following pages.

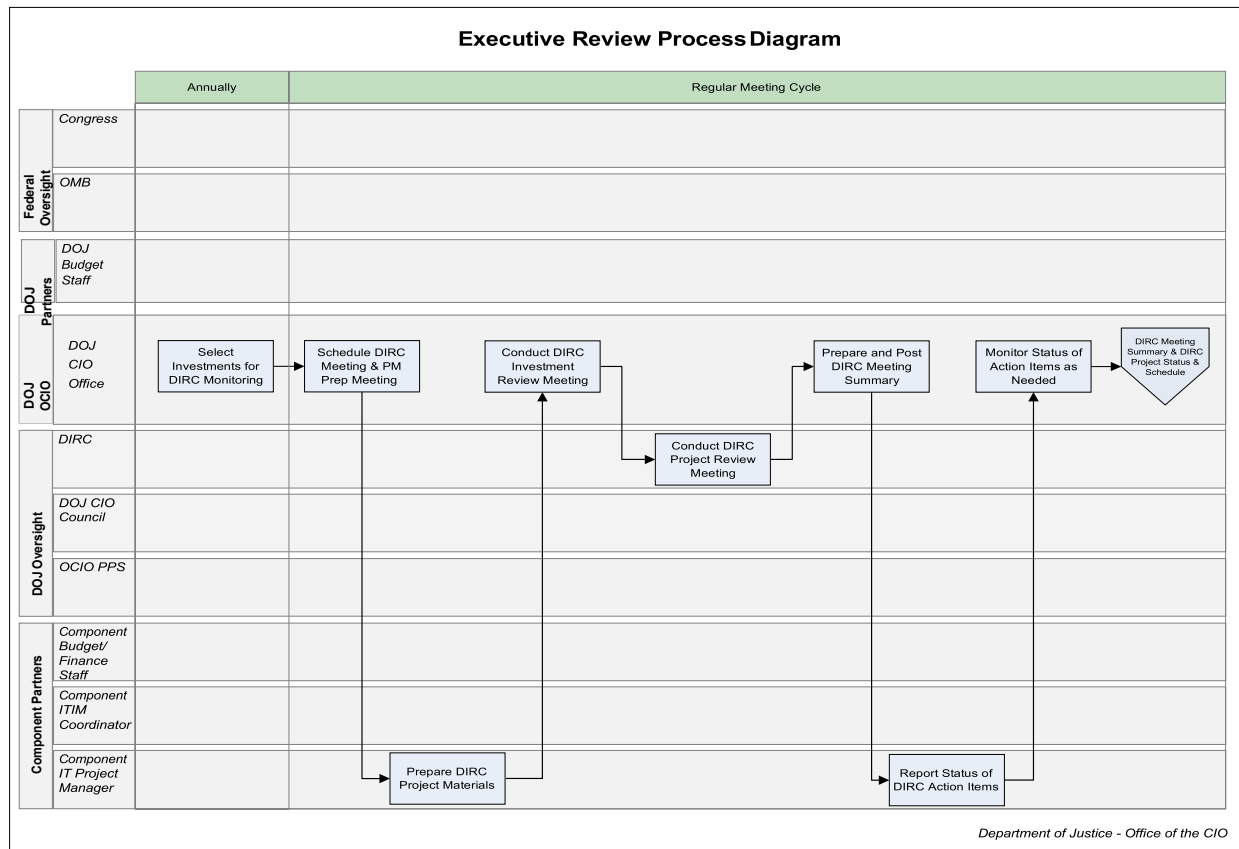


Figure 3-17: Executive Review Process Diagram

- Select Investments for DIRC Monitoring and Review:** At the beginning of each fiscal year, the CIO selects investments for DIRC portfolio monitoring and review over the course of the fiscal year. The investments are chosen based on at least one of the following criteria:
 - High Profile: project with high interest beyond the project office either inside or outside the department, such as media coverage or congressional interest
 - High Cost: any project that requires an OMB Major IT Business Case
 - High Risk: a project involving politically sensitive issues, significant cost and schedule variance, or business objectives that are unlikely to be achieved
 - DAG or CIO Discretion: projects may be added or removed at any time during the fiscal year at the discretion of the DAG or CIO
- Select Investments for DIRC In-Person Review:** During the course of the year, the DIRC selects those investments requiring in-person reviews, based on the defined selection criteria described earlier in this section. OMB requires that a TechStat session be scheduled for major IT investments that are identified as underperforming for 3 consecutive months. TechStat sessions are performed by the DIRC, and scheduled by the DOJ CIO¹⁹.

¹⁹ DOJ Order 0903: Information Technology Management, p. 6. See also 40 U.S. Code §11302: Capital planning and investment control.

- **Schedule Executive Review Meeting and PM Prep Meeting:** The DOJ OCIO will
 - Prepare and manage the DIRC investment list throughout the year, adding new investments when necessary and removing investments that no longer require executive review
 - Prepare and maintain DIRC schedule and status report throughout the year
 - Regularly notify the DOJ OCIO front office of the executive reviews planned for the next scheduled meeting and supply a list of mandatory and optional attendees for each review
 - Schedule the specific date, time, and location of executive review meetings
 - Contact the appropriate component CIO and IT program manager to inform them of the date and time the review will be held and provide the DIRC process checklist and other DIRC review templates
 - If the review is a TechStat of an underperforming investment, it must be scheduled before the investment reaches 4 consecutive months of underperformance and requires notification of the session 2 weeks in advance. The DOJ CIO has the discretion to schedule the TechStat session sooner, as deemed appropriate. Schedule a review preparation meeting with the component IT program manager 1-2 weeks prior to the executive review meeting
 - Schedule any other prep meetings (e.g. CIO pre-brief)
- **Prepare Investment Briefing Materials:** The component IT program manager will
 - Prepare the DIRC presentation by filling out the DIRC briefing template, preparing any other DIRC templates (e.g. investment self-assessment survey; EA investment review document), and organize any relevant follow-up materials relating to the last DIRC session
 - Submit an electronic draft copy of the DIRC briefing template, other DIRC templates, and relevant follow up materials to the DIRC support staff in accordance with the DIRC process checklist timeline
- **Conduct DIRC Investment Prep Meeting:** The DOJ OCIO PPS will
 - Meet with component IT program manager in advance of DIRC to review presentation materials for completeness and follow up on action items
 - Distribute an electronic copy of the briefing and last meeting minutes to all DIRC members in accordance with the DIRC process checklist timeline.
- **Conduct DIRC Review Meeting:** The DIRC will
 - Conduct a meeting to inform and/or evaluate the investment; component IT program manager will brief and answer questions from the board members
 - Assign action items, when necessary
 - Formulate any appropriate recommendations to the DIRB regarding the suspension of funding for troubled investments (i.e. terminate, halt, re-scope, or de-scope investment)
- **Prepare and Post DIRC Meeting Minutes:** The DOJ OCIO PPS will
 - Document the meeting's proceedings as DIRC meeting minutes, including attendees,

- action items to be completed, and discussion highlights
- Send draft minutes to CIO and component IT program manager for review and comment
- Send an electronic copy of the minutes to all DIRC members and attendees
- **Report the Status of DIRC Action Items:** The component IT Project Manager will report the completion of assigned action items to PPS, provide appropriate deliverables, and a status report of action items in progress
- **Monitor the Status of Action Items as Needed:** The DOJ OCIO PPS will
 - Work with CIO staff to complete any assigned action items assigned to OCIO before the next DIRC review
 - Contact the component IT program manager to determine action-item status and obtain documentation if necessary
 - Document the completion of action items in the DIRC action item records
 - Inform DIRC members when actions are closed and distribute documentation that closes action items, when appropriate

Component Self-Governance

Component responsibilities for the executive review process

- Elevate investments with significant governance, budget, and/or performance issues to the DOJ CIO for consideration for DIRC monitoring or review
- Ensure an internal monitoring process is in place, particularly for investments selected for DIRC monitoring or review
- Work with PPS to assist in reviewing component IT oversight processes
- Provide regular reporting and communications (e.g. status calls) on DIRC-selected projects
- Involve PPS in component review cycles, both regular and trigger-based, for DIRC-selected projects
- Perform and report on compliance reviews for DIRC-selected projects

3.3.2 Compliance Review Process

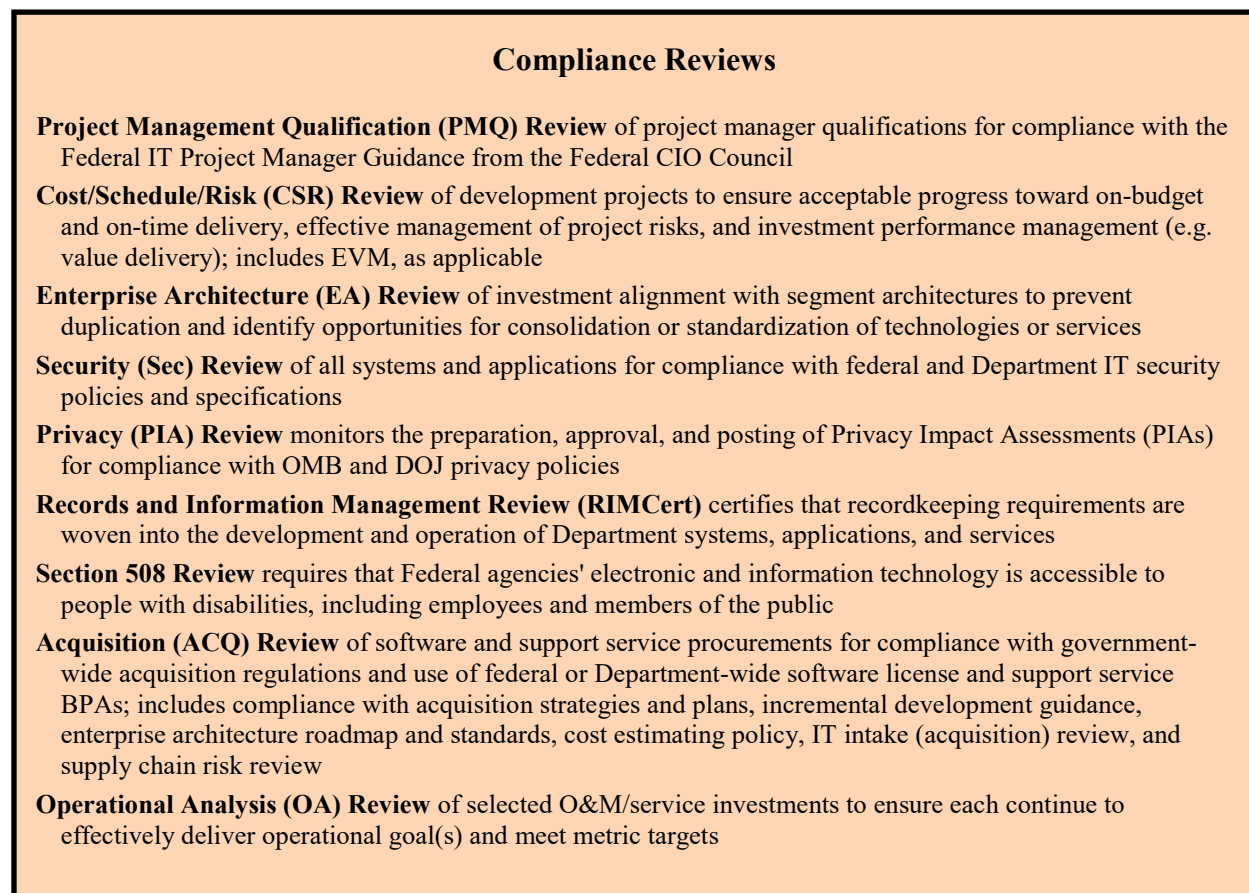


Figure 3-18: Compliance Reviews

The compliance review process determines how well investments conform to Department and federal IT policies and standards. All active programs, projects, and O&M system/service investments are subject to some aspect of the compliance review process. The compliance managers responsible for each compliance area schedule and conduct reviews throughout the fiscal year to satisfy the specific reporting requirement associated with the review. Compliance review information is monitored at the component and Department levels.

The compliance review process consists of two main activities – conducting one or more of the nine individual compliance review types and reporting the results. Compliance monitoring provides senior executives assurances that investments are being managed well and that the Department’s return on that investment is being maximized.

As described in the IT Oversight Model in Section 2.8, oversight of IT investments occurs at two levels – the Department and the component. In most cases, a relatively small number of key investments are selected for monitoring at the Department level based on very specific selection

criteria. Investments not monitored at the Department-level are monitored at the component-level only.

The descriptions of the compliance reviews on the following pages include the DOJ OCIO process owner, the review purpose, the timing or frequency for each review type, a brief description of the review process, and a description of the reports that are produced from the reviews.

3.3.2.1 IT Project Manager Qualification Review

PPS conducts the PMQ review, to comply with the requirements of OMB memorandum “M-04-19: Information Technology Project Manager Qualification Guidance” and DOJ Order 0903. The Department and its components use the criteria contained in the Federal IT Project Manager Guidance Matrix issued by the Federal CIO Council to determine if IT project managers for IT investments possess the necessary project management competencies and suggested work experience appropriate to the investments they manage. The review performed by the DOJ OCIO ensures that IT project managers for important Department-level projects are qualified according to the criteria in the Federal CIO Council Federal IT Project Manager Guidance Matrix.

The Office of Federal Procurement Policy (OFPP) established a certification for federal program and project managers known as the Federal Acquisition Certification for Program & Project Managers (FAC-P/PM). The process is governed by a memo from OFPP issued on December 16, 2013 titled “Revisions to the Federal Acquisition Certification for Program and Project Managers.” All program and project managers are required to be FAC-P/PM certified. The level of certification required varies based on the size of the program or project. Further information is available from the [Federal Acquisition Institute](#)²⁰ and the [DOJ Project Management Center of Excellence](#).²¹

- **Define Qualification Requirements:** OMB will
 - Define requirements for reporting project manager qualification in *Circular No A-11 Preparation, Submission, and Execution of the Budget*
 - Identify the criteria to be used for assessing PM qualification
 - Define qualification stages, as well as training and experience equivalencies
- **Reporting Guidance:** The DOJ OCIO will provide guidance to components for reporting PM qualifications as part of the instructions for preparing Major IT Business Cases
- **Evaluate Project Complexity, Establish PM Requirements:** The component CIO will
 - Use guidance in Federal IT Project Manager Guidance Matrix to assign levels of complexity to IT projects and establish qualification criteria for project managers
 - Assess the qualification status of project managers assigned to each investment using the appropriate qualification criteria from the matrix

²⁰ <http://www.fai.gov/drupal/certification/program-and-project-managers-fac-ppm>

²¹ <https://itim.doj.gov/projectmanagement/SitePages/FAC.aspx>

- **Report PM Qualification:** The component IT project manager will report PM qualification status in the Major IT Business Case according to the guidance provided by DOJ OCIO and OMB Circular A-11
- **Validate PM Qualification:** The component OCIO will review the PM qualification status reported in the major IT investment business case to ensure that the PM qualifications reported satisfy the requirements in the Federal IT Project Manager Guidance Matrix and are supported by documented training and experience
- **Review Qualifications Reported in Major IT Business Cases:** The DOJ OCIO will
 - Review PM qualification status reported in the Major IT Business Case
 - Confirm that the qualification information reported satisfies the requirements in the Federal IT Project Manager Guidance Matrix and is supported by documented training and experience
 - Ensure that appropriate corrective actions are planned to satisfy training requirements for PMs who are not fully qualified according to the Federal IT Project Manager Guidance criteria

Component Self-Governance

Component responsibilities for the project-manager qualification review

- Evaluate the complexity of component IT investments and assign a rating (i.e., Level 1, 2, or 3) to each investment using the criteria contained in the Federal IT Project Manager Guidance Matrix (Federal CIO Council's Workforce and Human Capital for Information Technology (IT) Committee, 2004)
- Assess project manager qualification compliance and assign qualification ratings using the guidance provided by DOJ OCIO and contained in OMB Circular A-11
- Report PM qualification status in major IT Investment business cases and/or on the component Agency IT Portfolio Summary
- Implement a project manager training process and monitor the completion of qualification requirements by component IT project managers who are not fully qualified for their current assignment

3.3.2.2 Cost/Schedule/Risk Compliance Review

The cost/schedule/risk (CSR) review is managed by the Assistant Director for PPS, using Folio, a variety of DOJ reporting formats (e.g. Excel and SharePoint), and the FITDB. The review process implements requirements defined by OMB for monitoring IT project cost, schedule, risk, and performance (e.g. value delivery) and for improving IT project planning and execution. These requirements are defined in OMB memorandum “M-04-24 entitled “*Expanded Electronic Government (e-Gov) President’s Management Agenda (PMA) Scorecard Cost, Schedule and Performance Standard for Success*” and OMB memorandum “M-05-23: *Improving Information Technology (IT) Project Planning and Execution*,” and are implemented in DOJ Order 0903.

The CSR review process provides the DOJ CIO, component CIOs, and project managers of selected IT investments with a “quick reference” on the current cost, schedule, risks, and

performance for important and highly visible DOJ IT investments. The CSR review examines these selected IT investments to ensure each are being managed within acceptable cost, schedule, and risk thresholds. The value proposition and business case for the investment are also reviewed for management of performance expectations (i.e. value delivery). Investments are selected annually for monitoring at the Department level (DIRC) using criteria described in Section 3.3.1.

The CSR review is also used to monitor earned value data for projects that must comply with the DOJ Investment Baseline Management & EVM Guide (version 2.0, June 2015) and the Earned Value Management Systems (EVMS) requirements of ANSI/EIA-748²². These investments include:

- IT investments with DME costs that exceed \$10 million annually or \$25 million over a five-year life cycle period
- Tech refresh/hardware upgrade projects with current year (CY) life cycle development costs (DME) greater than \$50 million or \$250 million over a five-year period
- Multi-agency collaboration investments such as e-Gov and line of business initiatives that require the efforts of more than one agency
- Projects specially designated by the DOJ CIO, component CIO, or OMB as a major investment, per OMB A-11, due to congressional interest, technological complexity, risk, a large commitment of resources, or the program is critical to achievement of a mission capability or set of capabilities

During preparation of the Major IT Business Case – Part 1, Section D (Acquisition/Contract Strategy) requires the investment to respond to question #2, “If Earned Value is not required or will not be a contract requirement for any of the contracts or task orders, explain why.”

OCIO PPS oversees the EVM surveillance system for the Department, and that investments requiring EVM are properly following Department guidelines as defined in the DOJ IT

Investment Baseline Management & EVM Guide found on the [DOJ Project Management Center of Excellence](#).²³

Components are responsible for oversight of EVM compliance for their component investments, with support from PPS in the areas of EVM training, SME support, and process improvement for EVM review processes. Component EVM compliance responsibility includes performing an annual Surveillance Review (audit) of those investments.

For regular (monthly) CSR monitoring by the DIRC, the Project Manager must provide project baseline information including target cost, project schedule and milestones, and risk information in the DOJ Folio database (or equivalent). Projections (e.g., cost & schedule) must then be recorded in Folio (or equivalent) each month along with risk & performance metric status for review not only at the component level, but also by the Department’s OCIO Assistant Director for PPS. Cost and schedule variances, risk scores, operational performance metrics, and component CIO ratings

²² American National Standards Institute/Electronic Industries Alliance

²³ <https://itim.doj.gov/projectmanagement/SitePages/FAC.aspx>

and comments are reviewed and discussed with the component ITIM coordinator. Finalized DOJ CIO ratings and comments are then discussed with the DOJ CIO and are uploaded to OMB's FITDB.

- **Direct PMs of Selected Investments to Submit Reports to DOJ OCIO:** Component CIOs will notify the PMs of investments selected for Department-level CSR review, and direct them to submit reports according to the instructions for DOJ dashboards and Folio.
- **Prepare and Report Metrics and Investment Status to DOJ OCIO:** The IT project manager will
 - Enter the key milestones that will be completed during the fiscal year, the required number of risks for the investment, and the funding for the investment
 - Report the investment status information to the Folio database (or equivalent) not later than the 10th business day of the month. Information required includes cost and schedule variance reports for variances that are greater than 10 percent; revised and/or actual start and completion dates for key investment milestones; and updated status of the top investment risks.
- **Review Metrics, Variance, and Project Status:** The DOJ OCIO will
 - Review the monthly metrics, validate the variance analysis reported by the project manager, and review the project risk status
 - Prepare a DOJ majors portfolio status report that discusses any corrective actions being taken or planned by the project manager and identifies any additional actions that are recommended
 - Brief the contents of the report to the DOJ CIO
- **Review Status Report and Assign Actions:** The DOJ CIO and/or Deputy CIO will
 - Review the DOJ majors' portfolio status report, and evaluate the adequacy of any corrective actions taken by the project manager
 - Discuss the status of projects with variance outside acceptable limits with the appropriate component CIO and assign additional corrective actions, when necessary
- **Direct PM to Take Corrective Actions:** The component CIO will
 - Direct the project manager to take corrective actions determined by the DOJ CIO
 - Monitor corrective action completion and evaluate results
- **Implement Corrective Actions and Report Results:** The component IT project manager will implement specified corrective actions and report results

Component Self-Governance

Component responsibilities for the cost/schedule/risk (CSR) review process

- Monitor the progress of investments selected for Department CSR review
- Ensure that project managers are following the Department-level reporting process, that the information is reviewed for accuracy and completeness with regular certification, and timely error correction prior to the Department's submission of the information to OMB
- Ensure a similar CSR process is in place for monitoring all important DME projects, at both program and project levels
- For investments requiring EVM, provide oversight of EVM compliance (with support from PPS) in accordance with the DOJ IT Investment Baseline Management & EVM Guide
- Provide component CIO-level rating to PPS for review, along with the CSR information, for the OCIO to develop a final CIO Rating for the Federal IT Dashboard.

3.3.2.3 Enterprise Architecture (EA) Review

The EA review process implements requirements contained in the OMB Circular No. A-130, *Managing Information as a Strategic Resource* and builds on the DOJ OCIO FITARA baseline.

At the Department level, the EA review process primarily focuses on the investments under DIRC review, including programs needing Department-level attention (i.e. underperforming programs requiring a “Deep Dive” or a TechStat review²⁴). The EA review process supports DIRC by providing an overall architectural review for the investment. The Enterprise Architecture Program Management Office (EAPMO) conducts the architecture review to evaluate the investment's approach, risk, performance, system, services, security, interoperability, standards, and schedule. The architecture review provides a valuable opportunity to prevent duplication and redundancies, reduce cost, minimize risk, increase interoperability, increase security, and enhance collaboration and to ensure alignment to DOJ future enterprise architecture and enterprise roadmap.

The DIRC determines the investments it will review, at which point:

- The investment PMO submits project documentation to the DIRC
- Enterprise Architecture PMO (EAPMO) reviews the documentation
- EAPMO reports its analysis to the DIRC

The EA reviews are conducted throughout the fiscal year to evaluate EA alignment status of DIRC selected investments, to ensure that they are proceeding according to plan and are still sound investments for the Department. EA investment reviews are conducted to fulfill CIO responsibilities for managing the IT portfolio, to identify improvements to the IT portfolios, to develop recommendations, and to comply with OMB and legislative requirements. The IT investment reviews implement mandates arising from federal statutes and policies, including the Clinger-Cohen Act, FITARA; and GAO recommendations for a more robust governance approach.

²⁴ DOJ Order 0903: Information Technology Management. See also 40 U.S. Code §11302: Capital planning and investment control.

Architecture review represents independent, unbiased assessments of IT projects' required artifacts that support several IT portfolio-related decisions during the design, development, testing, and implementation phases of the SDLC. Review criteria selection was based on DOJ *“EA Framework & Methodology,” “IT Project Manager Guide”* and *DOJ Enterprise Roadmap*.²⁵

The EAPMO reviews the required project documentation for DIRC review of individual system investments to ensure alignment with the EA and that it support DOJ's vision, strategy, goals, and objectives. The six required documents described in the DOJ *“EA Framework & Methodology”* and *“IT Project Manager Guide”* are used to assess the investment on approach, risk, performance, system, services, schedule, interoperability, and standards. The information reported from these reviews allows organizational leaders to develop actionable, fact-based, investment recommendations and decisions. The criteria, required documents, and process are described in detail in the *“Enterprise Architecture Investment Review Concept of Operations.”*

Component Self-Governance

Components will evaluate investments in accordance with Department EA guidance, and report EA alignment of those investments to the Department

3.3.2.4 IT Security Compliance Review

DOJ has established processes, procedures, and tools essential to performing the successful security assessment and authorization of DOJ IT systems in the *DOJ Security Assessment and Authorization (SA&A) Handbook*²⁶. Based on the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1*, and the *Committee on National Security Systems Policy (CNSSP) No. 22*, the SA&A process has been designed to align with existing policy, standards and guidance resulting in the assurance that security controls for DOJ IT systems are implemented and assessed in accordance with established DOJ security requirements.

Project managers must complete the following tasks:

- Designate an Information Systems Security Officer (ISSO) early in the design phase to implement proper security controls throughout the project
- Inform the CSS policy analyst about the project
- If an Authorization to Test (ATT) is necessary, complete in accordance with the DOJ SA&A Handbook prior to operational testing for new or major updates to applications or systems
- Work in conjunction with ISSO to complete the SA&A requirements, including CSAM output

²⁵ [Project Management Center of Excellence](https://itim.doj.gov/projectmanagement) (<https://itim.doj.gov/projectmanagement>)

²⁶ http://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/3-DOJ_Handbooks_Guides_Plans/sa-a-handbook-v8-4.pdf

- Achieve Authorization to Operate (ATO) by the end of ATT period. If an ATT is not required, ensure ATO is achieved prior to the consumption of production data or connection to the production network.

The SA&A Handbook provides a structured framework with identified roles and responsibilities to facilitate security assessment and authorization. The Handbook is designed for use by all DOJ stakeholders for the planning and execution of the security assessment and authorization process. Program, security, and procurement offices must ensure all contracts comply with *DOJ Procurement Guidance Document (PGD)* 15-03. Existing contracts without these requirements must be modified to ensure their inclusion. The DOJ security assessment and authorization process requires all DOJ stakeholders to work collectively in incorporating IT security throughout the full lifecycle of all developed and acquired government-operated and contractor-operated IT systems.

Component Self-Governance

Each component should work with their own ISSO to complete the SA&A process and achieve authority to operate.

3.3.2.5 Privacy Compliance Review

The privacy compliance review is coordinated jointly by the Senior Component Official for Privacy (SCOP) and by the DOJ Office of Privacy and Civil Liberties (OPCL).

OPCL reviews the Initial Privacy Assessment (IPA) to determine if there are any privacy issues and assesses whether additional privacy documentation is required, such as the full Privacy Impact Assessment (PIA), and to ensure the Department's compliance with applicable privacy laws and policies. A legal review, performed by JMD's Office of General Counsel (OGC), may be necessary to ensure that any legal issues have been addressed properly. The reviews are performed during the initial development of new investments and whenever major changes are approved for operational systems, to ensure privacy issues are identified, addressed, and mitigated.

The Senior Component Official for Privacy (SCOP) serve as OPCL's main point of contact and are responsible at the Component level for preparing the required privacy compliance documentation and managing the implementation of DOJ privacy policies established by Department leadership, and/or OPCL. Privacy compliance status for investments is tracked using the CSS' C&A Web IT security dashboard and reported to OMB through the FISMA compliance reporting process.

The component IT project manager is responsible for the following actions:

- **Perform PTA to Determine PIA Requirements**
 - Perform the Privacy Threshold Assessment (PTA) described in the DOJ privacy impact assessments official guidance

- Upload the PTA into CSAM Trusted Agent and complete all applicable fields in the privacy section of Trusted Agent
- Based on the results of the PTA, determine if a new PIA, or an update to an existing PIA, is required. If determination is that no PIA or PIA update is required, there is no further action.
- **Determine Privacy Act Applicability**
 - Work with the senior component official for privacy and/or OPCL to determine if the Privacy Act applies to the IT system. When the Privacy Act applies, determine whether a system of records notice (SORN) must be created or if the system is covered by existing component, departmental or government-wide SORNs.
 - Complete all applicable SORN fields in the privacy section of Trusted Agent.
- **Perform PIA and Prepare or Update the PIA Report**
 - Perform a PIA in accordance with the DOJ privacy impact assessment's official guidance.
 - Prepare a complete PIA report for new investments, or update the applicable sections of the existing PIA to address new privacy issues associated with system changes.
 - Submit the PIA for review and approval within the component and incorporate changes, as required.
 - After the component approves, submit the PIA to DOJ OPCL for approval. Load approved PIA into the CSAM Trusted Agent system.
- **Publish PIA for Public Access as Instructed by the DOJ OPCL**

The Department OPCL is responsible for the following:

- **Validate PTA Results:** The Department OPCL will review and validate the results of the PTA in Trusted Agent, and notify the component if a PIA must be completed
- **Coordinate PIA Privacy Review**
 - Review the PIA to ensure the assessment addresses all the appropriate issues regarding protection of information in identifiable form for the system or the enhancement.
 - Coordinate a review of privacy issues by the DOJ OGC, when required.
 - Collect comments from the DOJ CIO technical review and OGC privacy review, when required, and provide comments to the component for revision of the PIA, if required.
 - Issue final approval for the PIA and provide publication instructions to the component.

Component Self-Governance

Component responsibilities for the privacy compliance review

- Assess all new IT systems or enhancements to existing systems for privacy impacts
- Coordinate privacy reviews of PIAs within components before submitting for Department review
- Ensure PIAs for all component IT systems are reviewed periodically for compliance with up-to-date policies, security standards and privacy laws

3.3.2.6 RIMCert Review

The Records and Information Management Certification (RIMCert) is performed by the ORMP and OCIO and was established in DOJ Order 0801, *Records and Information Management*. This process incorporates recordkeeping requirements into the development and operation of Department systems, applications, and services that capture, create, or maintain federal records. In a subsequent policy statement (DOJ 0801.01) to all DOJ components, the Assistant Attorney General provided guidance for the establishment of the RIMCert beginning on October 1, 2014. This policy applies to

- New systems in development as of October 1, 2014 and forward
- Existing systems within three years of June 23, 2014
- Major system updates

Components with a comparable process that ensures recordkeeping requirements are evaluated/planned throughout development and implementation are able to apply for exemption from the Department RIMCert process.

Project Managers must complete the following tasks:

- Contact the ORMP and obtain a copy of the RIMCert application. A copy of the RIMCert application is also available at the Project Management Center of Excellence²⁷
- Assist the system owner in answering the questions on the RIMCert application
- Submit completed RIMCert application to DOJ ORMP for review and approval

Component Self-Governance

Component responsibilities for the RIMCert process are:

- Assess all major IT systems or enhancements to existing systems for RIM changes.
- Coordinate reviews of RIM within component before submitting for Department review.
- Ensure RIMCerts for all component IT systems are reviewed for all major system updates.

²⁷ <https://itim.doj.gov/projectmanagement/default.aspx>

3.3.2.7 Section 508 Compliance Review

Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public. Section 508 establishes requirements for any electronic and information technology developed, maintained, procured, or used by the Federal Government. The term "electronic and information technology" has been defined by the [Access Board](http://www.access-board.gov)²⁸ in regulations published December 21, 2000. Section 508 exempts national security systems from its requirements. Information regarding all aspects of assistive technologies and accessibility under Section 508 is available at section508.gov.

It is DOJ policy to require that all individuals with disabilities (whether Federal employees or members of the general public) have access to and use of information and data comparable to that provided to individuals without disabilities, unless making such content accessible would impose an undue burden on the Department. All DOJ public websites shall comply with the requirements of the Access Board set forth in response to Section 508 of the Rehabilitation Act.

Guidance for project managers is as follows:

- Content managers shall ensure that core requirements are met on all webpages, IT systems, and applications. See the [DOJ Policy for 508 Compliance](#) for a list of those core requirements.²⁹
- Content managers shall provide appropriate contact information to assist users with disabilities for any web content that cannot be made compliant.
- The Department OCIO will test all new web technology, script, or coding methods used to create web content before posting content on the DOJ web server.

Component Self-Governance

Component responsibilities for 508-compliance

- Assess all major IT systems or enhancements to existing systems for 508-compliance
- Coordinate reviews of 508-compliance within component before submitting for Department review
- Ensure 508-compliance for all component IT systems are reviewed for all major system updates

²⁸ <http://www.access-board.gov>

²⁹ <http://dojnet.doj.gov/webdevelopment/accessibility.php>

3.3.2.8 Acquisition Compliance Review

Acquisition Strategy and Planning

Per FITARA guidance, agencies shall not approve an acquisition strategy or acquisition plan, as required in the Federal Acquisition Regulations (FAR) Part 7.1 – Acquisition Plans, or interagency agreement, such as those used to support purchases through another agency, which includes IT, without review and approval by the agency CIO. The CIO shall primarily consider the following factors when reviewing acquisition strategies and plans:

- Appropriateness of contract type
- Appropriateness of IT-related portions of statement of needs or Statement of Work
- Appropriateness of above with respect to the mission and business objectives supported by the IT Strategic Plan
- Alignment with mission and program objectives in consultation with program leadership

The DOJ Senior Procurement Executive (SPE) is responsible for ensuring contract actions that contain IT are consistent with CIO-approved acquisition strategies and plans. The SPE shall indicate to the CIO when planned acquisition strategies and plans include IT. The SPE shall ensure the agency shall initiate no contract actions, interagency agreements, or contract modifications that include IT unless they are reviewed and approved by the CIO, or are consistent with the acquisition strategy and plan previously approved by the CIO.

Shared Acquisition and Procurement Responsibilities

The CIO reviews all cost estimates of IT investment proposals and ensures all acquisition strategies and plans that include IT apply adequate incremental development principles. The SPE, in consultation with the CIO and CFO, oversee the agency-wide process to ensure all acquisitions that include any IT are:

- Led by personnel with appropriate federal acquisition certifications (FACs), including specialized IT certifications as appropriate
- Reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting, and use such approaches, as appropriate
- Supported by cost estimates that have been reviewed by the CIO
- Adequately implement incremental development

Supply Chain Risk Review

DOJ PMs must comply with *PGD 14-03 - Acquisition of High or Moderate Impact Information Technology Systems (Supply Chain Risk Assessment)*. Section 515 of the Department of Justice's

fiscal year 2014 appropriations act (Public Law 113-76, Division B, Title II) provides that funds appropriated under the act may not be used to “acquire a high-impact or moderate-impact

information system, as defined for security categorization in the NIST *Federal Information Processing Standard Publication 199*, Standards for Security Categorization of Federal Information and Information Systems,” unless the Department has conducted assessments of supply chain risk and the risk of cyberespionage or sabotage, including any risk associated with a system being produced, manufactured, or assembled by entities the United States has identified as posing a cyber-threat, including but not limited to those owned, directed, or subsidized by the People’s Republic of China. Additional procurement guidance and information on Section 515 Guidance and is available on the [DOJ Acquisition Management page](#).³⁰

Project managers must complete the following tasks:

- Ensure an ISSO is designated to assist the Contractor Officer (CO) with the risk management intake form (Attachment 3 of PGD14-03)
- Work with CO and ISSO to complete the risk management intake form
- Once CSS renders risk acceptance determination, ensure this document is included in the ATO sign-off by DOJ CIO and system owner

The CO must complete the following tasks:

- After selection of successful offeror but prior to issuing any award, notify CSS of intent to issue award and provide the following information:
 - Summary of the procurement, including quantity and type of equipment or software to be acquired
 - Ensure offeror completes security risk questionnaire (Attachment 2 of PGD 14-03)
 - Complete risk management intake form
 - Identify any known cyber or sabotage vulnerabilities presented by the procurement
- Ensure all above information is submitted to CSS. CSS and FBI will conduct a national security risk assessment and render decision

IT Acquisition Review (ITAR)

The ITAR process is managed by the OCIO Policy and Compliance staff. The PGD entitled *DOJ Procurement Guidance Document (PGD) 16-02 Acquisition of IT Equipment, Software, and/or services*, and issued by the DOJ SPE in February 2016 is the basis for the process. The ITAR process requires components to report all IT procurement actions to the departmental OCIO via a SharePoint portal. Approval of procurement actions equal to or below the defined threshold of \$500k is delegated to the component CIO and these items are submitted for reporting purposes. Procurement actions over the \$500k threshold require approval from the IT Acquisition Review

³⁰ <http://dojnet.doj.gov/jmd/cao/procurement-guidance.php>

Board (ITARB). The ITARB is comprised of officials designated by the Department CIO, and reviews procurements for compliance with EA, vendor management, standard infrastructure, cybersecurity, and portfolio management standards and practices. The Department CIO and the ITARB review procurement actions over \$2.5 million. PPS performs the Acquisition (IT Intake) Review.

Component Self-Governance

Component responsibilities for acquisition compliance review

- Ensure component investments are being acquired under CIO-approved acquisition strategies and plans
- Ensure investments are led by personnel with appropriate federal acquisition certifications (FACs), including specialized IT certifications as appropriate
- Ensure investments are reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting, and use such approaches, as appropriate
- Ensure investments are supported by cost estimates that have been reviewed by the CIO
- Ensure investments adequately implement incremental development
- Ensure that project managers and COs collaborate to assess risk within the supply chain risk management guidelines pertaining to IT systems produced with involvement of entities identified as cyber-threats
- Identify investments making purchases of IT products and services above specified thresholds and submit those purchases to DOJ OCIO for approval using the IT intake request SharePoint site. Coordinate internal component reviews of those IT purchases when appropriate
- For investments making purchases of IT products and services below the specified thresholds, coordinate internal component CIO review and approval of those purchases, and submit a report of those purchases to the Department CIO

3.3.2.9 Operational Analysis Review

Operational analysis is a method of examining the ongoing performance of an IT system or service and measuring that performance against established metric targets. (For more information on operational analysis, refer to the *OMB Capital Programming Guide*).³¹ The operational analysis review process is designed to determine if the Department's mixed life cycle and operational systems/services comply with the following:

- Deliver the expected mission or business performance and improvement
- Operate and can be maintained within the approved budget according to the system operations plan (or equivalent)
- Expect to meet the projected needs for the planned life cycle of the system/service
- Share any enterprise services via the OCIO Services Catalog

Operational analysis reviews are performed monthly for all major IT investments in the O&M

³¹ https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/capital_programming_guide.pdf

systems/services or mixed life cycle stage, that must report to the OMB FITDB; some metrics may have measurement frequencies that are quarterly or annually. Components are encouraged to perform operational metrics performance measurement and analysis on all other major and non-major investments as well in order to demonstrate value and business results realization. DIRC monitoring processes and OMB reporting processes involve analysis of operational metrics, as part of the monthly Folio update process. The identification, establishment, measurement, and analysis of these metrics, including those that are customer oriented, is performed monthly with trending, follow-up, and/or corrective action plans for unmet expectations.³²

Component Self-Governance

Component responsibilities for the operational analysis review

- Establish O&M system/service metric performance targets for selected Department-level mixed lifecycle and steady state investments
- Report operational performance metrics monthly for all major investments that report up to the OMB FITDB, as well as other DIRC-monitored major investments as appropriate
- Implement a similar process for monitoring the O&M system/service metric performance of important component-level mixed lifecycle and steady state investments

3.3.3 IT Performance Measurement

The purpose of IT performance measurement is to identify, collect, and measure IT performance, health, and cost savings pertaining to Department and federal initiatives supporting the efficient and effective use of IT. The internal and external reporting of IT performance measures drives outcomes. These outcomes affect the Department strategic planning, enterprise architecture road map and IT investment planning activities but also play a role in federal planning and decisions. This section will cover the various mechanism used to collect IT performance measures and how these measures are used to meet external and internal reporting requirements.

3.3.3.1 Data Collection Mechanisms

Various data gathering and analytics activities measure IT performance information associated with the governance phases and processes. These activities collect data from DOJ OCIO, JMD, and components across the Department, and this data in turn is used for internal analysis by departmental and domain oversight bodies, and external reporting to federal oversight bodies (such as OMB).

Several data collection mechanisms are employed by OMB, other federal oversight bodies, and the Department to gather IT performance information to support decision making and strategic direction of IT and IT spending. These mechanisms support the immediate need to collect or validate information dependent on the current IT environment. They range from routine data collection exercises, such as integrated data collection (IDC), to ad hoc requests for information,

³² OMB Capital Planning Guide, Supplement to Circular A-11, (<https://www.whitehouse.gov/omb>)

such as cyber security health assessments. See Figure 3-19 for an example of the current federal IT performance data calls.

In response to numerous requests for information, the Department utilizes the following methods to collect information from the DOJ OCIO and across DOJ components.

- **Component Data Call:** A data call format for collection information directly from components using a streamlined approach, instructions, communications, and collection templates to ensure information is collected in a standard fashion. This mechanism is in place to provide a singular platform for soliciting information across components with decreased burden of multiple requests for the same or similar information. In addition to support federal requests for IT performance measures, Department specific inquiries are incorporated into the component data call to capture information that will support Department planning and the decision-making process. This mechanism is most commonly used to collect information in response to OMB's quarterly IDC.
- **Ad Hoc Request/Directed Component Communication:** This format is used when responding to direct requests for information that is individualized or specific to an area, project, program, or component. These communications usually run concurrently with the major component data calls.
- **Ongoing Collection:** As the need for information grows, the Department also employs an "ongoing" collection mechanism that provides components/projects/programs the opportunity to provide information as it comes available. This mechanism is usually in the form of an online form or survey. This mechanism is currently used to collect cost savings and avoidance information.

Example Data Calls

Integrated Data Collection (IDC): A quarterly data call to agencies to aggregate information pertaining to Department-wide initiatives supporting the efficient and effective use of IT.

Cost Savings and Avoidance: On-going and quarterly data to support direct and oversee an on-going departmental effort to identify and implement best practices for saving taxpayer money, realizing efficiencies, and monitoring the department's savings progress.

Data Center Transformation Initiative (DCTI): Data call effort to support the Federal Data Center Consolidation Initiative (FDCCI) strategy to achieve greater efficiencies via data center consolidation and shared services to better understand the IT infrastructure inventory, performance objectives, future plans, and challenges.

FISMA Audit: Ensures IT Systems are compliant with departmental, OMB, and Department of Homeland Security IT security requirements.

Open Data: A data call to agencies to measure to transparency, public participation, and collaboration in support of the Open Government Initiative.

Figure 3-19: Example Data Calls

3.3.3.2 *External Reporting*

In the federal oversight arena, data collection activities are released to agencies to support and report back on the federal wide initiatives in the area of effective and efficient use IT. These activities are actioned, by the following stakeholders and activities:

- **Office of Management and Budget (OMB):** In March 2012, OMB initiated PortfolioStat (M-12-10) to examine agency IT portfolios to identify areas of common IT spending with the goal of reducing/eliminating duplicative spending and in turn drive down costs. PortfolioStat consists of a data-driven yearly review of agency portfolio management between the Federal CIO and senior agency officials. In addition to helping agencies achieve financial savings through reform efforts, PortfolioStat analyzes agency progress using a variety of performance metrics designed to measure whether agencies are delivering their IT investments on budget and on schedule, driving innovation to meet customer needs, and adequately protecting Federal IT Assets and Information.³³
- **President's Management Council:** The 2018 President's Management Agenda (PMA) includes Improving Outcomes through Federal IT Spending Transparency as one of its Cross Agency Priority (CAP) Goals. This goal aims to
 - Improve business, financial, and acquisition outcomes;
 - Enable Federal executives to make data-driven decisions and analyze trade-offs between cost, quality, and value of IT investments;
 - Reduce agency burden for reporting IT budget, spend, and performance data by automating the use of authoritative data sources; and
 - Enable IT benchmarking across Federal Government agencies and with other public and private sector organizations.

3.3.3.3 *Internal Reporting*

Within the Department, IT performance measures collected through various federally mandated data calls are used to support internal activities. The following stakeholders and activities use this information to report on the Department's compliance with federal initiatives (i.e. PIV mandate) and make strategic decisions for the Department:

- **CIO Council:** Information collected in various data-collection activities is used to report on compliance and provide enterprise wide-metrics on current IT endeavors and as a spring board for identifying new IT and enterprise opportunities.
- **CIO Council Committees:** Evaluates IT and supports the formulation of enterprise recommendations for the direction of IT in different areas (i.e. IT security, data centers, and telecommunications).
- **Component CIO:** Updates from the spring IT budget call are presented alongside metrics

³³ <https://itdashboard.gov/#analyze-pstat>; also see 40 U.S. Code §11319: Resources, planning, and portfolio management

collected to prepare a holistic picture of a component's current IT spending, savings, and health (i.e. compliance with OMB mandates) as a precursor to the fall IT budget call and data collection activities. This information consists of departmental reports, individual component CIO briefings, and semi-annual portfolio reviews used to evaluate component-specific progress and status in the areas of IT spending and other compliance activities.

- **DOJ OCIO:** The measures collected in support of PortfolioStat and PMA benchmarking are used to shape Department IT strategic plan and IT priorities.

Appendix A – Acronyms

ACEIT: Automated Cost Estimating Integrated Tools

ACQ: Acquisition

AG: Attorney General

AoA: Analysis of Alternatives

ARB: IT Acquisition Review Board

ATO: Authorization to Operate

ATT: Authorization to Test

C&A: Certification and Accreditation

CFO: Chief Financial Officer

CHCO: Chief Human Capital Officer

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CO: Contracting Officer

CONOPS: Concept of Operations

CPIC: Capital Planning and Investment Control

CSAM: Cyber Security Assessment & Management

CSR: Cost/Schedule/Risk

CSS: Cybersecurity Services Staff

CTO: Chief Technology Officer

CY: Current Year

DAG: Deputy Attorney General

DCTI: Data Center Transformation Initiative

DIRB: Department Investment Review Board

DIRC: Department Investment Review Council

DME: Development, Modernization, and Enhancement

DOJ: Department of Justice

EA: Enterprise Architecture

EAC: Estimate at Completion

EAPMO: Enterprise Architecture Program Management Office

e-Gov: Electronic Government

EPM: Enterprise Performance Management

EVM: Earned Value Management

EVMS: Earned Value Management System

FAC-P/PM: Federal Acquisition Certification for Program and Project Managers

FACs: Federal Acquisition Certifications

FAR: Federal Acquisition Regulations

FDCCI: Federal Data Center Consolidation Initiative

FEA: Federal Enterprise Architecture

FISMA: Federal Information Security Management Act of 2002

FITARA: Federal Information Technology Acquisition Reform Act of 2014

FITDB: Federal IT Dashboard

FTE: Full Time Equivalent

FY: Fiscal Year

GAO: Government Accountability Office

HR: Human Resources

ICE: Independent Cost Estimate

IDC: Integrated Data Collection

IEC: International Electrotechnical Commission

IGCE: Independent Government Cost Estimate

IPA: Initial Privacy Assessment

IRB: Investment Review Board

IRM: Information Resources Management

ISCP: Information System Contingency Plan

ISO: International Organization for Standardization

ISSO: Information Systems Security Officer

IT: Information Technology

ITAR: IT Acquisition Review

ITARB: IT Acquisition Review Board

ITIL: Information Technology Infrastructure Library

ITIM: IT Investment Management

JABS: Joint Automated Booking System

JMD: Justice Management Division

LCC: Law Enforcement Coordinating Council

LCCE: Life Cycle Cost Estimate

LEISP: Law Enforcement Information Sharing Program

LOB: Line of Business

NIST: National Institute of Standards and Technology

O&M: Operations and Maintenance OA: Operational Analysis

OBD: Office, Board, and Divisions

OCIO: Office of the Chief Information Officer

OFDT: Office of the Federal Detention Trustee

OFPP: Office of Federal Procurement Policy

OGC: Office of General Counsel OIG: Office of the Inspector General OLA: Operational-Level Agreement

OMB: Office of Management and Budget

OPCL: Office of Privacy and Civil Liberties

ORMP: Office of Records Management Policy

PGD: Procurement Guidance Document

PIA: Privacy Impact Assessments

PIV: Personal Identity Verification

PM: Project Manager

PM CoE: Project Management Center of Excellence

PMA: President's Management Agenda

PMO: Program Management Office

PMQ: Program/Project Manager Qualification

PPS: Policy and Planning Staff

PTA: Privacy Threshold Assessment

RIMCert: Records Information Management

ROI: Return on Investment

QFR: Questions for the Record

SA&A: DOJ Security Assessment and Authorization Handbook

SCOP: Senior Component Official for Privacy

SDD: System Design Document

SDLC: System Development Life Cycle

SDS: Systems Delivery Staff

SIP: Service Improvement Plan

SME: Subject Matter Expert

SMS: Service Management System

SORN: System of Records Notices

SPE: Senior Procurement Executive

UC: Underpinning Contract

UFMS: Unified Financial Management
System

WBS: Work Breakdown Structure

Appendix B – Definition of IT for DOJ

The Clinger-Cohen Act of 1996 defines Information Technology (IT) as “any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Department. ‘Information technology’ includes computers, ancillary equipment, software, software maintenance and support, firmware and similar procedures, services (including support services) and related resources.”

In order to understand and apply the IT definition above, and to ensure full and consistent reporting across the Department, the OCIO issued an additional explanation on what is considered IT. There are three broad areas of IT that support the diverse mission and goals of the Department of Justice: mission-delivery and business solutions; IT infrastructure; and IT practices and management.

Mission Delivery and Business Solutions

Mission-delivery and business solutions are comprised of software applications, systems, services and the people, processes, commercial contracts, overhead occupancy and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department. Mission-delivery and business solutions provide support for the missions of the Department as stated in the DOJ Strategic Plan:

- Prevent terrorism and promote the nation’s security
- Prevent crime, enforce federal laws, and represent the rights and interests of the American people
- Ensure the fair and efficient administration of justice

Core Functions

These strategic goals are advanced through core mission functions as noted in the IT Strategic Plan. These core functions are listed here with an illustrative example of an IT investment in that area:

- **Intelligence Operations:** An example of this is the component “ABC” investment in IT systems that collect data by audio, telephone, microphone telecommunications intercepts, and other electronic surveillance methods in support of its intelligence and counter-terrorism mission. Another example is the component “ABC” investment in IT systems that are used in detection, identification, tracking, and assessment of individuals and entities that pose threats to the United States and its interests
- **Law Enforcement and Investigations:** An example would be component “ABC” investment in a system that provides electronic case, records, workflow, evidence management, case tracking and records search and reporting capabilities for the collection and sharing of investigative data. Another example would be an investment in an IT system that maintains a record, inventory, and catalog of improvised explosive Devices used to support forensic examination.

- **Litigation and Judicial Activities:** An example would be a case management system used by a component to support the management and administration of the legal cases with which it is involved.
- **Correctional Activities:** An example of this would be component “ABC” investment in a mission support system used real-time to manage and report all inmate information such as work assignments that is critical to the safe and orderly operation of all federal prisons.
- **Justice Program Coordination:** An example of this would be component “ABC” investment in a system that provides automated support for the application, approval, tracking, and closeout of federal grant funds.
- **Justice Information Services:** An example of this would be component “ABC” investment in a system that provides fingerprint identification services for local, state, federal and international law enforcement community and homeland security.
- **Regulatory Activities:** An example would be component “ABC” investment in an IT system that tracks and reports interstate cigarette sales information.

Support Functions

These core mission functions are assisted by support functions. They are listed here with an illustrative example:

- **Administrative Management** such as tracking systems, correspondence management, training, or records management: An example of this is the component “ABC” investment in a correspondence management system used to support the executive office of the Department
- **Financial Management Systems** and related functions such as accounting, payroll, personnel, procurement and property management application systems: An example of this is the component “ABC” investment in an information system that supports the accounting functions of the component
- **e-Gov Contributions, Assessments, and Service Fees** are the costs levied against DOJ for partner resource funding contributions and service fees for the federal e-government initiatives and lines of businesses. The Department accounts for these on behalf of all components.

IT Infrastructure

IT Infrastructure is the people, processes, commercial contracts, overhead occupancy, and technology used to interconnect computers and users and automate business processes. Infrastructure can also acquire process, store, send, receive, interchange, manage, switch, transmit, and receive electronic data and information.

- **End User Systems and Support** includes the people, processes, commercial contracts, overhead occupancy, and technology necessary to enable and support an end user in their interaction with information technology services. The titles and terminology used in this section are drawn directly from the *e-Government Information Technology Infrastructure Line of Business* (ITI LoB). Examples include
 - Client Hardware (desktops, mobile, handheld devices)
 - Peripheral Hardware (local printers, shared printers)
 - IT Management Hardware (hardware supporting an IS process such as IT management client devices and IT management servers that support testing and training, network management, or asset management)
 - User Client software (PC operating systems, personal productivity, personnel database, messaging and groupware)
 - IT Management Software (of end user systems and support) (e.g., client/server hardware and software used exclusively for supporting IS functions such as network, systems storage, asset management, testing and training.)
 - Occupancy (fully burdened costs for the facilities being used by the staff such as space, furniture and utilities, etc.)
 - Personnel (Full-Time Equivalent or FTEs) (Fully burdened salaries and benefits for government FTEs that provide the following functions: technical services, planning and process management, finance and administration and asset management.)
 - Help Desk (i.e. hardware and software used for helpdesk support, government FTEs, commercial contract services, and transmission telecommunications associated with the help desk function.)
- **Mainframes and Server Systems and Support** includes the people, processes, commercial contracts, overhead occupancy and technology to provide physical or logical, centralized or aggregated computer systems and related services to one or more parts of the enterprise(s). The titles and terminology used in this section are drawn directly from the E-Government ITI LoB. Examples include
 - Mainframe systems and support (e.g., IBM or compatible, or other)
 - Server rooms and closets (e.g., Wintel, Unix, Linux, other)
 - Security Operations Command Centers
 - Data Center Operations and Disaster Recovery Facilities
 - Web hosting hardware and software operations (licenses, maintenance, back up, disaster recovery)
 - Electronic messaging (e-mail, voice mail, video mail)

- Storage hardware and software operations (licenses, maintenance, back up)
- **Telecommunications Systems and Support** includes the people, processes, commercial contracts, overhead occupancy, and technology to provide "any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. The titles and terminology used in this section are drawn directly from the E-Government ITI LoB. Examples include:
 - Network Operations Centers
 - Wire closets and cable management
 - Data Networks hardware and software
 - Telecommunications hardware and software
 - IPv6
 - Video hardware and software
 - Wireless communications
 - Metropolitan Area Networks
 - Wide Area Networks
 - Local Area Networks
 - Internet Access
 - Wide Area Voice (Long Distance)
 - Local Area Voice (Phones, PBX)
 - Video Teleconferencing

IT associated with construction, i.e. network cabling, wiring, or fiber optic infrastructure associated with facility construction, should not be reported.

IT Practices and Management

IT Practices and Management are programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support all the IT investments of the component. Some examples of what would be reported under IT Practices and Management include:

- **Enterprise Architecture** staff FTEs, systems and contracts supporting the Enterprise Architecture program for the component: An example of this would be the "EA Program" investment of component "ABC." This investment would account for the FTE resources for the staff of the EA program office, any contract costs that support this investment, and any systems used by the program office to manage the program.
- **IT Investment Management and Capital Planning and Investment Control** staff FTEs, systems and contracts supporting the ITIM or CPIC program for the component: This could include related earned value management and IT governance activities as well. An example of this would be the "IT Capital Planning" investment of component ABC. This investment would account for the FTE resources for the staff of the ITIM office, any systems used to

manage and administer the ITIM program, and any service costs in the form of commercial contracts to support the program.

- **Information sharing activities** of a general nature not attributable to a specific investment: An example of this would be the “Information Sharing” investment that provides the common standards, data definitions, and protocols to share information across the Department and the larger federal and state governments.
- **IT Program Management** staff FTEs, systems, and contracts that support the IT program of the component as a whole. This could include such activities such as the records management, financial management, human resources management, and IT training. An example of this would be the “IT Program Management” investment of component ABC. This investment accounts for the immediate OCIO staff, the budget officer and HR staff for that office, as well as any commercial contracts used to support the component IT program as a whole.
- **IT Security Program** includes the people, processes, commercial contracts, overhead occupancy, and technology used to manage the IT Security program of the component. Included here would be FTEs, systems, and contract support to deliver this program. Not included here are the IT security costs directly associated with a specific IT investment. Those costs should be reported as part of that investment. An example of this would be the “IT Security” investment by component “ABC” that accounts for the staff FTEs managing the component IT security program and information system, and a contract with a commercial service provider for contract help and technical expertise.

Appendix C – Workforce Management

The purpose of DOJ workforce management is to ensure an adequately skilled and equipped workforce to perform the work necessary to maintain the current state, and to achieve the strategic goals. This includes the appointment of component CIOs to build and oversee a component IT workforce, in accordance with DOJ standard IT workforce management practices.

Component CIOs

The Department Chief Information Officer (CIO) concurs with the component head in the appointment of component CIOs. FITARA requires components to consult with the Department CIO in the recruitment and selection of component CIOs and equivalent positions.³⁴ Component heads that appoint a CIO will inform the Department CIO of the person's qualifications for the position, the organizational placement of the position, and of any responsibilities assigned to the person other than information resources management.³⁵

OMB guidance on FITARA implementation also requires that the Department CHCO and CIO jointly establish agency-wide critical elements to be included in all component CIOs' performance evaluations. The Department CIO must identify "key bureau CIOs" and provide input to the rating official for this critical element(s) for at least all "key bureau CIOs" at the time of the initial summary rating and for any required progress reviews. The rating official will consider the input from the Department CIO when determining the initial summary rating and discuss it with the component CIO during progress reviews.³⁶

Workforce Knowledge & Skills

The Clinger Cohen Act of 1996 requires the Department CIO to assess the requirements established for Department personnel regarding knowledge and skill in Information Resource Management, and to ensure personnel at the executive and management level meet these requirements to determine their adequacy for facilitating achievements of performance goals. The Department CIO must also rectify any deficiencies in meeting those requirements, and develop strategies and specific plans for hiring, training, and professional development. OMB Circular A-130 requires the Agency Head to ensure the Department develops a well-trained corps of information resource professionals.

To satisfy these requirements, the Department CIO shall:

- Determine the Department's IT human capital requirements
- Assess IT workforce skills and competencies and determine gaps and areas for improvement
- Develop strategies and plans for recruiting or training current staff to satisfy required skills

³⁴ DOJ Memorandum: FITARA Hiring Requirements, 8/17/2015

³⁵ DOJ Order 0903

³⁶ OMB Memorandum M-15-14: Management & Oversight of Federal Information Technology, 6/10/2015

- Establish qualifications requirements for critical IT management staff positions
- Monitor Component compliance with Department policies and guidelines.

Component Heads shall:

- Ensure compliance with the requirements of the DOJ Human Capital Strategic Plan
- Ensure IT project and program managers and other IT professionals are qualified or certified according to OMB and Department requirements as specified by Federal and Department directives.