U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer

DOL
IT Investment Management
Life Cycle
Guide

Version 1.0
July 2014

U.S. Department of Labor
Office of the Chief Information Officer
200 Constitution Avenue, N.W.
Washington, DC 20210

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Executive Summary

This document describes the Department of Labor's (DOL's) Information Technology (IT) Investment Management Life Cycle (IMLC). The goal of this guide is to assist and support DOL IT Project or Program Managers (PMs), Integrated Project Team (IPT) members, DOL IT Management stakeholders, as well as senior DOL management decision makers in understanding DOL's IT IMLC including the interrelated components of the life cycle as well as the associated policies, processes, and procedures and how they apply to support PMs and IPTs in successfully managing DOL's IT Investments including IT projects, programs, systems, and/or services. Example systems includes core agency business mission IT systems and services, mission support systems and services, administration systems, subsystems, and services, software operating systems, software applications, as well as IT infrastructure systems at the national, regional, and local levels used to interconnect agency systems, services, and/or applications directly or via the Internet.

The DOL IT IMLC framework presented in this document is not a new concept or approach as the core life cycle processes included within the framework have been a fundamental part of the DOL Systems Development Life Cycle Management (SDLCM) Manual since 2002 and implemented by DOL IT Investment PMs and IPTs for over a decade.

In addition, the IT IMLC framework presented leverages and utilizes the standard principles and practices found in the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) Guide, Fifth Edition. The PMBOK Guide is an internationally recognized standard for managing all types of projects – across various industries. The Guide is an important reference for DOL PM's as it supports and describes the fundamental project management processes and knowledge areas that are recognized as good practices and form the foundation of the DOL IT IMLC. Yet, it's important to understand the IT IMLC framework supports and is in compliance with DOL IT policies, regulations, and/or guidelines or practices as well as Federal IT management requirements including federal laws such as the Clinger-Cohen Act of 1996, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA) of 2002, the Paperwork Reduction Act (PRA).

Thus, the life cycle concepts and the approach of the DOL's IT IMLC framework presented in this document is standards based, proven, and is able to be applied and support the successful life cycle management of DOL's IT investments.

1 Introduction

For almost a century, the U.S. Department of Labor ("DOL" or "Department") has been helping Americans find employment, feel more secure in the workplace, and benefit fairly from their hard work. Information Technology (IT) has been a critical enabler in helping the Department deliver its core services over the years and today IT is an indispensable component supporting the mission success of the Department. Each year the Department spends over $500 million dollars on its IT portfolio of investments including IT projects, programs, systems, and/or services. Example systems includes core agency business mission IT systems and services, mission support systems and services, administration systems, subsystems, and services, software operating systems, software applications, as well as IT infrastructure systems at the national, regional, and local levels used to interconnect agency systems, services, and/or applications directly or via the Internet.

Managing this IT investment portfolio efficiently and effectively as well as in accordance and compliance with legislative mandates is essential and critical to not only being good stewards of taxpayers' dollars but, to ensure the successful implementation and operation of the IT systems. IT systems that fulfill the business mission needs as well as support and/or deliver quality customer service. At the same time, it is essential to balance the growing demand for more and better IT services while IT budgets and funding continue to decline and /or be cut. These conflicting demands require more than ever that DOL's IT investment be managed efficiently and effectively using standard and proven IT management practices and flexible and/or adaptable IT processes that are applied throughout the life cycle of an IT investment.

This document represents DOL's IT Investment Management Life Cycle (IMLC) Guide.

1.1 Purpose

This guide describes DOL's universal and standards based IT IMLC as well as the associated policies, processes, and procedures and how they apply to support PMs and IPTs in successfully managing DOL's IT Investments. In particular, this document describes the individual life-cycle processes (i.e., including the Strategic Business Management (SBM), Capital Planning and Investment Control (CPIC), Systems Development Life Cycle Management (SDLCM), and IT Security life cycle processes) that comprise the DOL IMLC including the associated and interrelated life cycle phases. It describes the activities to be completed in each phase of an IT investment's life cycle, to ensure DOL's IT investment are being managed efficiently and effectively as well as support the Department's business mission goals and management reviews.

This guide serves to:

- Introduce the concept of IT life cycle management to IT PMs, IPT members, and agency stakeholders
- Standardize (as much as possible and as applicable) the IT life cycle management processes across the Department
- Describe the OCIOs expectations and requirements for IT investment life cycle management across the Department

- Provide an overall reference that describes the relationships between the Systems Development Life Cycle Management (SDLCM), Capital Planning and Investment Control (CPIC), IT Security, and Strategic Business Management (SBM) processes and their IT investment management requirements including their deliverables and key phases. It also illustrates the linkages that exist between and/or across these life cycle processes
- Highlight deliverable templates, resources and other reference documents and/or guides that are available to assist PMs and IPTs in completing individual life cycle phases.

The outcome goal of this guide is to enhance awareness and knowledge of DOL's IT IMLC as well as to assist and support DOL IT Investment PMs, IPT members, DOL IT Management stakeholders, as well as senior DOL management decision makers in improving the management of DOLs portfolio of IT investments.

1.2 Benefits of the Framework

The DOL IT IMLC presented in this document provides the following benefits:

- Improves the planning, implementation, operations, and disposition of DOL IT investments across the Department including IT systems, software applications, and/or services

- Ensures DOL PMs and IPTs have a clear understanding of the standards of practice and expectation required by DOL senior leadership to efficiently, effectively, and consistently manage DOL's IT investments – based on a universal standard

- Improves the quality of the DOL agency and departmental business management and IT decision making process through the application of sound IT business management practices

- Supports and/or drives internal business mission performance and results in IT solutions that support greater operational efficiencies

- Ensure DOL IT investments are managed in accordance and compliance with applicable federal IT legislation, OMB circulars, memorandums, and guidance, as well as GAO and National Institute for Standards and Technology (NIST) standards, recommendations, administrative priorities and DOL IT policies and procedures

- Enhance the overall understanding and implementation of a common and standard IT life cycle management framework, as a core DOL business management practice

- Supports the control and in many cases the reduction of IT investment life cycle costs in spite of the costs associated with implementing a standard and disciplined IT IMLC.

1.3 Points of Contact

Table 1 identifies the points of contact (POCs) responsible for this document and the associated components of the DOL IT IMLC.

Table 1: POCs for DOL's IT IMLC Components

Name	Role	Contact Info	Responsibility
Peter Sullivan	Director, OCIO Governance	Sullivan.Peter@dol.gov	Business Owner responsible for this Guide.
Kevin G. Clark	Program Manager, OCIO IT Investment Management/CPIC Program	Clark.Kevin.G@dol.gov	Successful implementation of the OCIO IT Investment Management/CPIC Program and life cycle in this Guide.
Kimberly Boudreaux	Program Manager, OCIO Strategic Business Management (SBM)	Boudreaux.Kimberly@dol.gov	Successful implementation of the SBM Program and life cycle in this Guide.
Tonya Manning	Program Manager, OCIO Information Assurance	Manning.Tonya@dol.gov	Successful implementation of the DOL's IT Security life cycle implementation as per the Computer Security Handbook (CSH) for DOL's IT Investments
Hamid Ouyachi	Chief Technology Officer	Ouyachi.Hamid@dol.gov	Technical Components of DOL's Enterprise Architecture and SBM life cycle phases

1.4 Document Overview

Section 1.0 covers the purpose, benefit of the life cycle framework, points of contact, document overview, background, scope and audience, assumptions and constraints, and document history. Section 2.0 introduces the DOL IT IMLC phases, the IT IMLC Framework including the fifteen IT business management areas, and the integrated IT investment management life cycles (i.e., the SBM, SDLCM, CPIC, and IT Security) management processes. Section 3.0 describes the DOL IT IMLC phases and associated activities in greater detail. Section 4 describes the IT investment management life cycles in greater detail including individual phases in each life cycle and the

associated deliverables and program/project management activities to be completed. Section 5 describes the roles and responsibilities of the various DOL individuals and/or stakeholders in regards to the DOL IT IMLC.

Appendix A includes a description of the ten DOL business management areas including the principles, terms, tools (if applicable), requirements, and/or management practices or techniques associated with each area. **Appendix B** includes a description of the entities comprising DOL's IT Governance structure. **Appendix C** includes a reference copy of the SDLCM phase gate review checklists. **Appendix D** includes a summary of software life cycle models. **Appendix E** includes a list of relevant acronyms associated with this guide. **Appendix F** includes a Glossary of Terms associated with this guide. **Appendix G** includes a list of references associated with this guide.

1.5 Background

Too many Federal IT projects run over budget, fall behind schedule, or fail to deliver promised functionality, hampering agency missions and wasting taxpayer dollars. To address these Federal IT investment issues and challenges, IT management reform legislation, such as the Clinger-Cohen Act of 1996 have been enacted to elevated the priority of IT management within Federal agencies to implement IT management processes, integrate management and budget processes, inventory IT investments, and designate a Chief Information Officer.

The Paperwork Reduction Act (PRA) of 1995 required agencies to manage their information technology resources in an efficient, effective and economical manner. In 2000, the PRA was supplemented by the Government Paperwork Elimination Act (GPEA), which furthered the effort by requiring agencies to leverage improved network technologies by proving electronic transactions. This concept was promoted even further with the passage of the e-Government Act of 2002 (P.L. 107-347) which required agencies to support e-Government projects and to leverage cross-agency initiatives to further e-Government. It also required agencies to submit privacy impact assessments for all new IT investments using personally identifiable data from or about members of the public.

Federal IT management practices continue to evolve and mature driven most recently by the Obama Administration through, for example, administrative led or driven IT strategies and initiatives, OMB memorandum, and Executive Orders. For example, the 25 Point Implementation Plan to Reform Federal Information Technology (IT) Management was released in December 2010, initiating among the 25 reforms the cloud first policy, clarifying the role and authority of the federal CIOs, establishing the OMB IT Dashboard, TechStat reviews, initiating a shared services strategy, and IT acquisition reforms. The Federal Cloud Computing Strategy (February 2011) was published followed by A Common Approach to Federal Enterprise Architecture (May 2012), Federal IT Shared Services Strategy (May 2012), Digital Government Strategy (May 2012), and Open Data Policy (May 2013) initiatives.

DOL has also undertaken and supported the administration reform efforts in all of the areas mentioned above. In addition, the DOL OCIO has developed a five year IRM Strategic Plan defining the future goals and objectives of Information Technology at the Department as well as

an Enterprise Roadmap that describes the annual steps being taken to achieve the IRM Strategic Plan. In addition, the OCIO has implemented improvements in its IT management practices including a new IT Governance Structure.

In the past few years alone, DOL has made great strides in standardizing and enhancing its IT management practices including standard documents templates for many of its Systems Development Life Cycle Management (SDLCM). These standardized templates have significantly improved the quality of IT investment management and management reporting at DOL. DOL has also made strides in rebuilding its strategic business management capabilities, resulting in the aforementioned DOL IRM Strategic Plan and Enterprise Roadmap.

The logical next step in DOL's IT investment management maturity is to enhance, modernize, and optimize its IT investment management integrated life cycle framework. The goal is to increase knowledge, awareness, and understanding of the framework including the numerous interrelated IT investment management life cycle process and associated activities that are critical and essential to successfully managing, deploying, and operating IT investments at DOL. This document reflects this next step and represents a single source for IT PMs, IPT members, and/or DOL business management decision makers to better understand DOL's ILCF and what they need to know, when they need to do it, and how to do it to support the success of their IT investments.

1.6 Scope and Audience

This guide describes the DOL IT IMLC including the components of the framework (i.e., the life cycle phases, the fifteen IT IMLC business management areas, and the integrated IT investment management life cycles (i.e., the SBM, SDLCM, CPIC, and IT Security) management processes. In short, this guide describes the phases, processes, and activities that are required to take place throughout the life cycle of a DOL IT investment to ensure it is successfully implemented, operated, and managed. This guide is intended for DOL IT PMs, IPT members, and/or DOL business management decision makers to better understand DOL's IT IMLC as well as the "who", "what", "when", and "how" associated with managing DOL IT investments throughout their life cycle.

1.7 Policy

This guide supports and/or is builds upon the following DOL policies:

- Department of Labor Manual Series (DLMS) 9 – Information Technology policy
- DLMS 1 - Records Management policy

1.8 Assumptions and Constraints

The following list of bullets describes the assumptions and/or constraints that were made, used, and/or applied in the development of this document.

- This guide has been developed in accordance and compliance with DOL OCIO IT investment management policies, processes, and practices as well as applicable Office of Management and Budget (OMB) and other federal IT investment management requirements.
- This guide has also been developed utilizing the standard principles and practices found in the PMI PMBOK Guide, Fifth Edition. Unless otherwise stated, the PMBOK Guide standard principles, practices, and/or processes apply. In the unlikely event there is a conflict between the PMBOK Guide and the principles, practices, and/or processes in this guide, this guide will prevail as it has been tailored to comply with DOL IT management policies, practices, and /or processes.
- The life cycle processes included in this guide are consistent with generally accepted IT Investment Management best practices, federal IT practices, and include proven DOL IT Investment Management practices.
- DOL IT Investment PMs, IPT members, and senior management stakeholders have a basic life cycle knowledge and/or experience supporting and/or working directly on an IT investment.
- The guide applies to DOL's IT investments including IT projects, programs, systems, and/or services. Example systems includes core agency business mission IT systems and services, mission support systems and services, administration systems, subsystems, and services, software operating systems, software applications, as well as IT infrastructure systems at the national, regional, and local levels used to interconnect agency systems, services, and/or applications directly or via the Internet.

1.9 Revision History

The following table summarizes the revision history of this guide.

This guide is considered a living document and as such is subject to change. This document will be updated in time, as necessary, to reflect any changes and/or new information that becomes known or available.

Date	Version	Section	Change	Modified By
7/1/2014	1.0	All	Initial Document Created	OCIO

2 DOL IT Investment Management Life Cycle (IMLC) Framework Overview

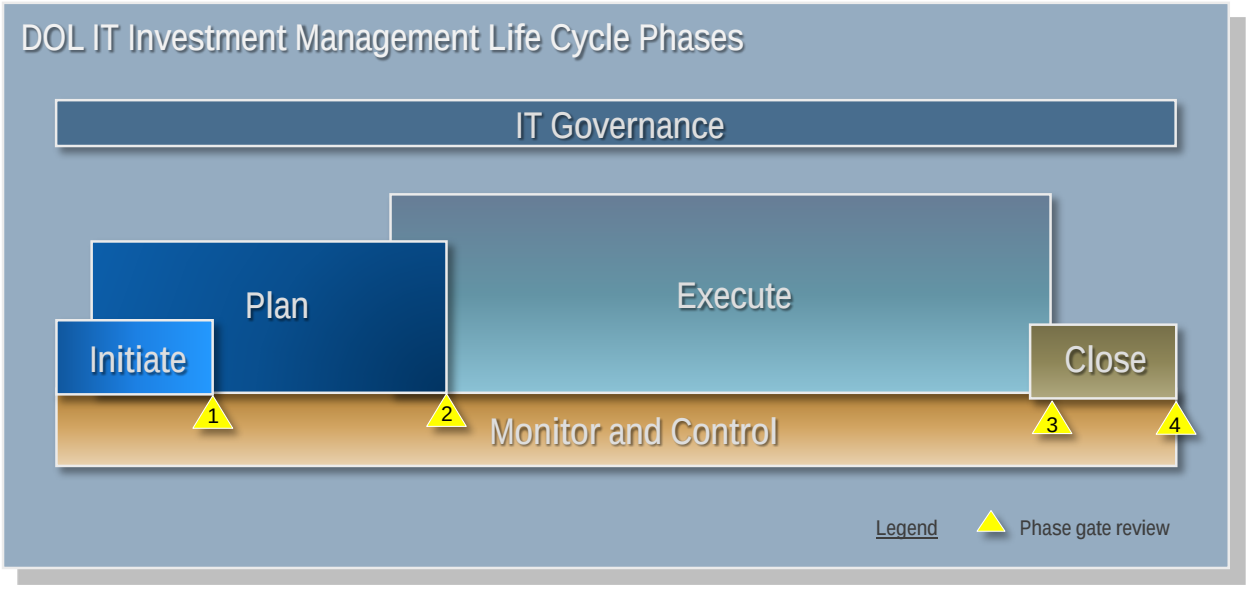
As mentioned in Section 1, it is critical and essential that DOL's IT investments be managed efficiently and effectively as well as in accordance and compliance with legislative mandates. This is to ensure that taxpayers' dollars are being managed and utilized properly as well as to provide for the successful implementation and operation of the IT investment that fulfills its purpose in supporting the business mission – on time, within budget, and as promised. At the same time, it's paramount to balance the growing demand for more and better IT services with the reality of limited and declining budgets. These conflicting demands require IT organizations, more than ever, to manage IT investments more efficiently and effectively. This includes the use of standard and proven IT management practices and flexible and/or adaptable IT processes that are applied throughout the life cycle of an IT investment.

Figure 1 illustrates the Department's agile, universal, and standards based IMLC phases. The figure shows six life cycle phases and the general sequencing of the phases relative to each other. The six phases include the Initiate, Plan, Execute, Monitor & Control, Close, and IT Governance phases. The first five phases of the framework are consistent with the phases found in the in the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) Guide[1]. The sixth life cycle phase is the IT Governance phase. This phase has been added since management review and oversight (i.e., governance) is a requirement for all DOL IT projects and programs. Each phase is described in detail in Section 3.

The benefit and advantage of this IMLC framework is in its simplicity – its ease of use and understanding as well as its agility i.e., universal applicability, flexibility, and scalability. It can be applied and utilized to manage the life cycle activities associated with a wide range and/or variety of initiatives, projects, and/or programs large or small the Department implements to fulfill its business mission.

[1] The PMBOK Guide is an internationally recognized standard for managing projects. The PMBOK is an important reference as it describes a comprehensive set of interrelated project management processes that are generally recognized as good practices for managing all types of projects – across various industries.

Figure 1: DOL's IT Investment Management Life Cycle Phases

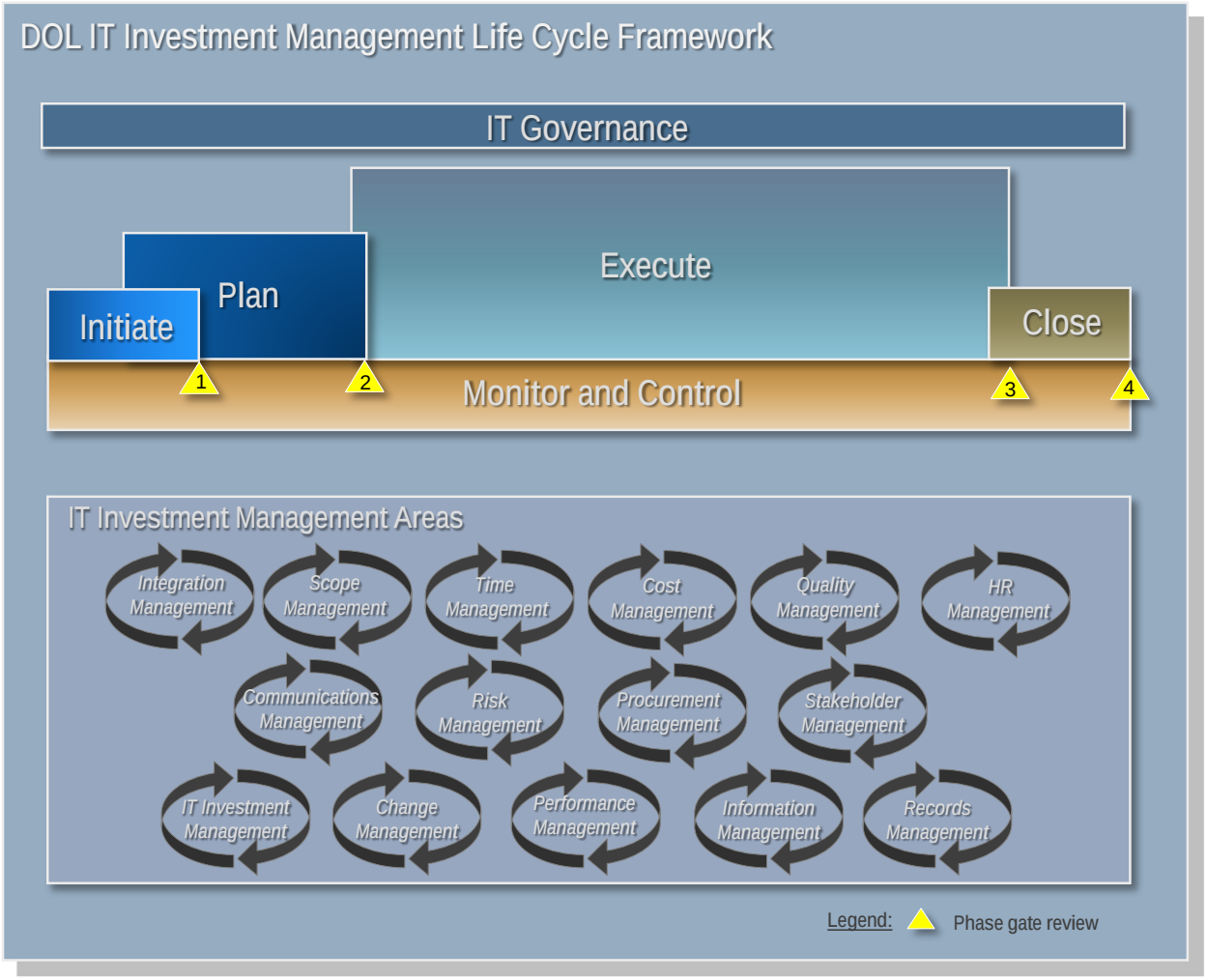


It is important for DOL PMs and IPTs to understand that in order to efficiently and effectively manage and implement the DOL IT investment management life cycle phases, the life cycle phases need to be implemented and managed in an integrated and correlated fashion with the nine PMBOK knowledge areas (i.e., Integration, Scope, Time, Cost, Quality, Human Resource, Communications, Risk, and Procurement management). At DOL, the PMBOK knowledge areas are referred to as business management areas since PMs and IPTs are expected to manage each of these areas as part of their IT investment management activities.

Figure 2 shows DOL's IT Investment Management Life Cycle Framework with fifteen IT investment management areas that are an integral part of the IT investment management life cycle phases shown in Figure 1. PM's and IPT members are required to implement and manage these areas throughout the life cycle of a DOL IT investment.

The first nine management areas shown in Figure 2 are consistent with the PMBOK knowledge areas (i.e., Integration, Scope, Time, Cost, Quality, Human Resource, Communications, Risk, Procurement, and Stakeholder Management). The six remaining management areas (i.e., Stakeholder, IT Investment, Change, Performance, Information, and Records Management) are required by DOL policy and IT investments. The management areas are described in detail in Appendix A.

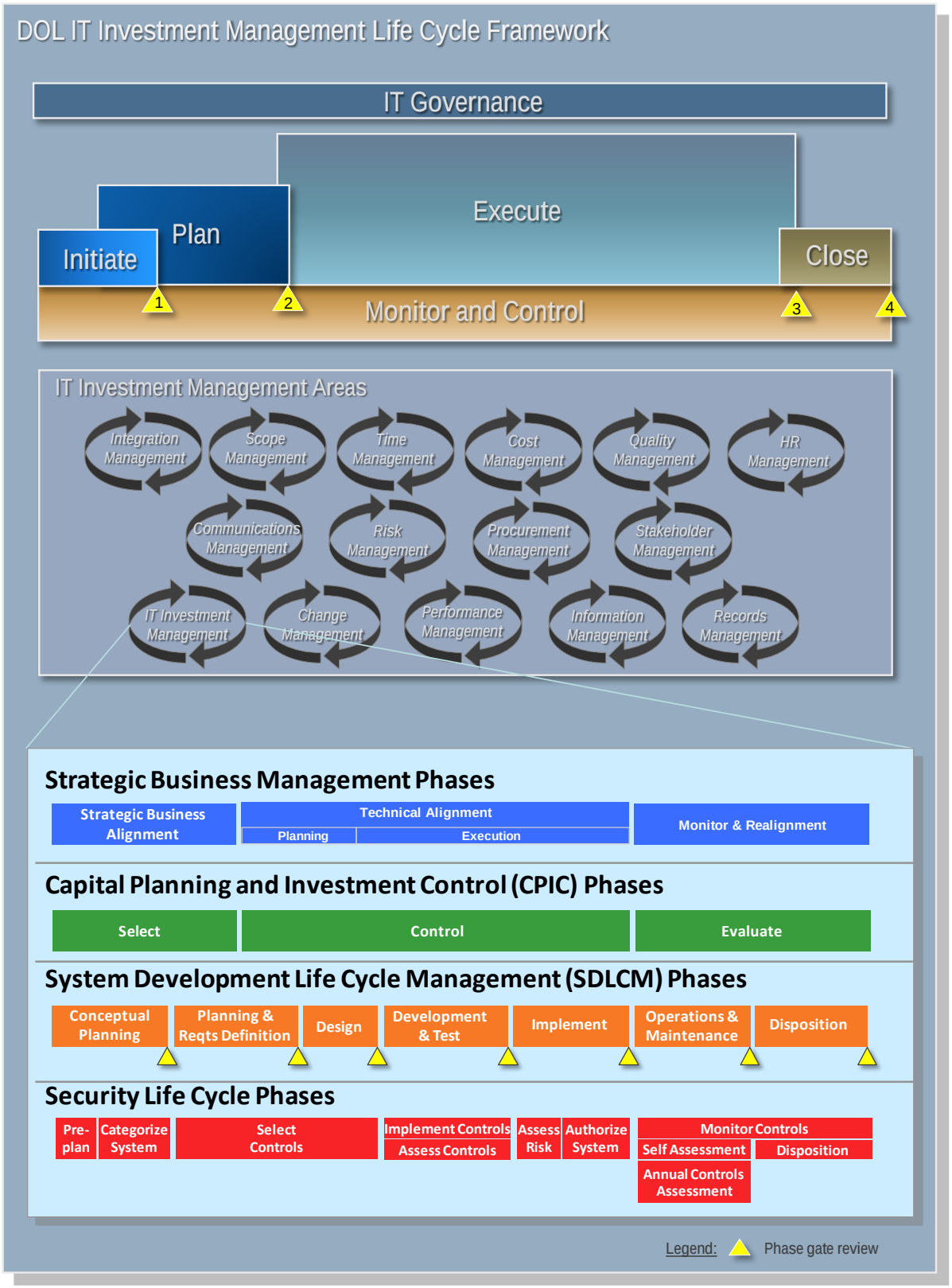
Figure 2: DOL's IT Investment Management Life Cycle Framework



It's also important to understand that the scope and level of detail of the required life cycle documents produced for an IT investment for each of the IT investment management areas depends on many factors including the size, complexity, criticality (i.e., business mission need and/or importance), and DOL and/or administration management priority.

Figure 3 illustrates the entire DOL IT IMLC framework with the four interrelated and standard IT investment management life cycles. Each of the standard IT investment management life cycles, including their phases as well as the processes and activities performed in each phase, are described in detail in Section 4.

Figure 3: DOL's IT Investment Management Life Cycle showing the Four Interrelated and Standard IT Investment Life Cycles



3 DOL IT IMLC Phases

This section describes each of the DOL IT IMLC phases (i.e., the Initiate, Plan, Execute, Monitor and Control, Close, and IT Governance phases) as shown at the top of Figure 1.

It is important to note the processes and work activities associated with each of the following life cycle phases is consistent with the PMBOK guide. To ensure greater value, alignment and applicability to DOL PMs and IPTs, the life cycle processes and activities are described in the context of DOL's IT environment reflecting DOL IT management terminology, policies, guidelines, processes, and/or procedures.

3.1 Initiate Phase

The Initiate phase represents the beginning of a DOL IT investment driven typically by an agency's business mission need or requirement or by the need to modernize, enhance, or replace an existing IT investment. The processes and activities performed in this phase focus on "ideation" or the formulation of the idea and creation of the possible IT solutions to fill the identified business need and/or performance gap.

During this phase a DOL agency should assess and document the business need and/or performance gap(s) and investigate possible business solutions. This may require, once the business needs/gaps have been identified and documented, conducting market research and/or reaching out to the OCIO Customer Service Organization (CSO) to determine possible information technology solutions that may exist to meet or fulfill the business needs/gaps. In addition, an Agency will need to determine and/or assess the initial level of effort and funding required and available to begin developing a more detailed business case to convince senior management and/or the OCIO that a possible IT solution should be pursued.

If a DOL Agency has identified existing funding to support the needed IT investment, then this phase typically culminates with the DOL agency developing a Request for Information Technology Services (RITS) and submitting the RITS to the OCIO Customer Service Organization (CSO) for review and development of a more detailed resource estimate by the OCIO Technical Service Organization (TSO). See the OCIO RITS template for details on how to complete a RITS.

If a DOL Agency has no existing funding to support the needed IT investment, then a business proposal and budget request, otherwise known as a Performance Budget Issue Paper (PBIP) needs to be developed. The PBIP is required to be completed and submitted at the beginning of the annual budget process led by the Departmental Budget Center (DBC). A PBIP must follow DBCs instructions and be reviewed and approved by senior DOL management across numerous organizations before being included in the Departments annual budget submission process. The Initiate phase is concluded upon agency submission of a signature approved RITS to the OCIO or the OCIO approval of an agency IT PBIP.

See the annual DBC budget process instructions as well as the associated PBIP instructions for details on how to complete a PBIP.

3.2 Plan Phase

Once an IT Investment's RITS or PBIP is approved and a budget is acquired, an IT investment progresses to the Plan phase. It is during this phase that a business lead and a technical Project or Program Manager is identified to oversee and lead the IT investment. In some cases, depending on the size, scope, and/or complexity of the IT investment, an Integrated Project Team (IPT) and/or a Project/Program Management Office (PMO) is planned and the mission, purpose, and scope of the IT Investment is further analyzed, more clearly defined, and/or fleshed out in greater detail. It is during this phase that a project or program charter is developed, reviewed, and approved via signature by the key players and stakeholders. In addition, high level strategic planning activities as well as initial project management planning and administrative activities are performed to convince and acquire senior management approval to progress to the Execute phase. A draft Project or Program Management Plan (PMP) is developed during this phase to assist and support the PM and/or the IPT in understanding and selling the need for the IT investment to senior management.

As funding is locked in and IPT members are identified and on boarded, the planning phase quickly evolves into the Execution phase. Up to this point in an IT investment's life cycle, the IT management activities can be less formal and structured allowing the PM and/or IPT members the flexibility to plan accordingly for the Execute phase.

In cases where an IT investment will collect information from the public, the PM and/or IPT is required to submit an information collection request to initiate or revise any OMB approvals under the Paperwork Reduction Act to the Information Compliance Management Program within the OCIO. PMs and/or IPT members should work with their Agency PRA Clearance Officer to ensure this process is performed in a timely fashion.

3.3 Execute Phase

The Execute phase brings a greater level of IT management seriousness, structure and deliverable requirements as financial, labor and material resources are being applied and utilized by the IT Investment. The Execute phase requires the completion, management approval, and implementation of a PMP. The Execute phase also requires the four major interrelated investment management life cycles (i.e., the Strategic Business Management (SBM), Capital Planning and Investment Control (CPIC), SDLCM, and IT Security) to be followed and implemented by the IT Investments PM and IPT. Each of these IT management life cycles are essential and need to be managed in a coordinated fashion to ensure the successful planning, implementation, and ongoing operations and maintenance of a DOL IT investment. These four life cycles are described in detail in Section 4 of this document.

In addition, consistent with the principles and practices of the PMBOK, PMs and IPTs will being implementing and managing the four IT investment management life cycles by utilizing and/or applying the principles and practices associated with nine interrelated knowledge areas, otherwise known at DOL as the IT business management areas as described in Appendix A of this document.

3.4 Monitor and Control Phase

As shown in Figure 1, the Monitor and Control phase and associated processes and activities start at the beginning and continue throughout the entire life of the IT investment. This phase involves tracking, monitoring, and controlling the progress and performance of the activities associated with an IT investment. This phase may include weekly and monthly status reports summarizing work activities and/or accomplishments as well as periodic meetings with senior management and/or key stakeholders to brief them on the progress and/or to address issues/concerns. Control activities may include or involve identifying and implementing corrective actions to fix a current problem or issue. It may also include implementing preventive actions to avoid potential issues and/or problems that may negatively impact the IT investment. Monitoring and control activities may include internal DOL management reviews (i.e.., reviews required by the OCIO and/or the Office of the Inspector General) and/or reviews required by external DOL entities such as OMB, GAO, and/or Congress.

For instance, as part of the DOL OCIO CPIC Control phase, DOL IT investments are required to submit IT investment documents on a quarterly basis (or as defined by the OCIO CPIC team) to the OCIO CPIC team for review and evaluation. This quarterly OCIO Control Review process is a key part of the IT investment performance monitoring and control activities required by the Clinger-Cohen Act of 1996. For further details regarding the DOL OCIO Control Review process, please see the OCIO's CPIC Guide and the Control Review schedule posted on LaborNet.

A good example of an external reporting requirement is OMB's IT Dashboard. On a monthly basis, major federal IT investments from all federal agencies including DOL are required to report cost, schedule, and performance information on the IT Dashboard. At DOL, major IT investment PMs and/or IPTs submit cost, schedule, and performance information on a monthly basis to the OCIO CPIC team for review and submission to OMB. See the DOL CPIC Guide and/or contact the DOL CPIC team for details regarding the monthly OMB IT Dashboard reporting process. Another good example is OMB's monthly Integrated Data Collection (IDC) reporting process. This process requires DOL IT investments to report various status and performance information including for example IT security and privacy metrics, commodity IT baseline status, cost savings and avoidance status, and status information for other key IT initiatives being driven by OMB and the administration.

3.5 Close Phase

The Close phase includes the processes and activities associated with terminating, shutting down, and/or decommissioning the services, software, hardware, and/or contracts associated with an IT investment at the end of its life cycle. It is possible that an IT investment may be cancelled, shutdown, or closed prematurely due to any number of reasons including for example but not limited to changes in priority, budget cuts, poor performance, vendor or contractor issues, technical and/or contractual issues. Each of the IT Investment Management life cycle processes, shown in Figure 1, need to be closed out in an orderly fashion. For example, as described in the SDLCM Manual, the Disposition phase requires the implementation of the IT investment's

Disposition Plan - developed during the O&M phase of the IT Investment's life cycle. A sample Disposition Plan template can be found in Appendix A of the DOL SDLCM Manual.

For further IT investment closeout requirements and process details see the OCIO's SDLCM Manual, CPIC Guide, and CSH posted on LaborNet.

Also, in cases where an IT investment has collected information from the public, the PM and/or IPT is required to submit an information collection request to discontinue or revise, as appropriate, any OMB approvals under the Paperwork Reduction Act to the Information Compliance Management Program within the OCIO. PMs and/or IPT members should work with their Agency PRA Clearance Officer to ensure this process is performed in a timely fashion.

3.6 IT Governance Phase

As shown at the top of Figure 1, IT Governance is an overarching component of the DOL IT IMLC. In order to understand and appreciate the purpose and function of the IT Governance phase, it requires an explanation and understanding of governance in general and an overview of DOL's IT Governance Framework.

Governance, in general, is a fundamental business management decision making, control and oversight function that seeks to manage and balance the business needs, resources, and interests of stakeholders within an organization. This is typically done by establishing a management structure involving senior organizational leadership, key business managers and stakeholders who are responsible for defining, guiding, monitoring, overseeing, and/or controlling the direction, policies, practices, standards, processes, and/or activities within an organization. In the private sector, a corporate board of directors typically represents the pinnacle of the organizational governance structure followed by senior management staff including the CXO positions. These governance entities oversee, at a high level, the direction and operations of the business and make critical organizational business decisions. A board of directors typically delegates the implementation of business strategies and/or specific business activities to applicable lines of business, such as the CIO for IT related actions, or they may choose to establish lower level groups or committees to perform or ensure the implementation of specific or unique business functions or activities. The ultimate goal of IT related governance is to ensure IT investment decisions, planning, deployments, operations, and maintenance activities are business focused, business driven, and generate business value in the most efficient and effective manner possible.

At DOL, the IT Governance framework includes two key components: (1) an agency sponsor – who is responsible for defining and overseeing the execution of the DOL IT governance process and (2) a specific governance structure that illustrates and defines the Department's governing entities including their hierarchical relationship to one another.

The DOL Office of the Chief Information Officer (OCIO) is the specific agency sponsor responsible for, among other responsibilities, Department-wide IT leadership in defining, guiding, monitoring, overseeing, and/or controlling the IT direction, policies, practices, standards, processes, and/or activities as well as the IT portfolio and investment management

oversight for the Department. This includes the establishment, management and oversight of the Department's IT Governance structure and the associated Department-wide IT governance activities performed by the various governing entities or bodies (i.e., boards, committees, forums, etc.) that comprise the DOL IT Governance structure.

3.6.1 DOL IT Governance Structure

Like private industry, DOL has established a hierarchical decision making IT governance structure, involving senior organizational leadership, key business managers and stakeholders, responsible for directing, managing, and balancing the IT business needs, resources, and interests of the stakeholders (i.e., DOL agencies) within the Department. This includes overseeing, coordinating, and/or guiding the Department's implementation and modernization of information technology investments. DOL IT Governance Structure including the various hierarchical entities comprising the structure is illustrated in Figure 4 below.

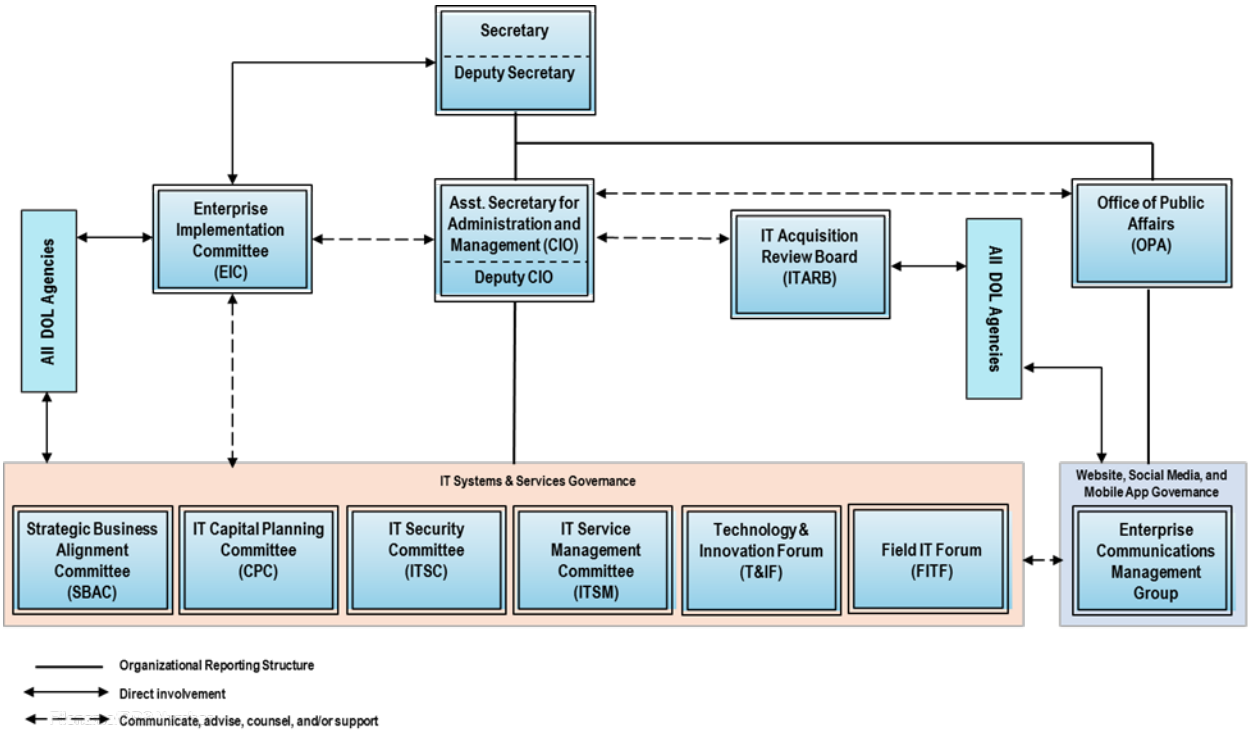


Figure 4: DOL's IT Governance Structure

The IT governance structure by design supports a hierarchical decision-making process in alignment with the Department's organizational structure and business management (i.e., strategic planning, mission and goals, and operations) - thus ensuring IT is used as a strategic business asset to support, enhance, and modernize the operation of the Department.

In addition, as shown in the Figure 4, the OCIO works collaboratively with DOL's Office of Public Affairs (OPA) to ensure the successful implementation of DOL's Digital Government

Strategy (DGS). Numerous digital government related policies and procedures are in place to address and support the delivery and implementation of quality digital services to DOL customers, consistent with the DGS.

Appendix B includes a detailed description of each of the entities, including their roles and the responsibilities, shown within the DOL's IT governance structure.

3.6.2 DOL OCIO IT Governance Division

The DOL OCIO IT Governance Division serves an important management and oversight role of the DOL IT Governance framework. Specifically, the Division serves as a Department-wide IT leadership, strategic business, investment, and information management guidance and assistance to Departmental agencies enabling them to implement their IT resources in a manner that balances risks and returns, while achieving the organizations' business mission and program goals. The Governance division also has Department-wide IT investment management oversight responsibilities to ensure DOL's IT portfolio is managed in compliance with legislative mandates including the Clinger Cohen Act of 1996 (CCA), Government Performance and Results Act (GPRA), Paperwork Reduction Act (PRA), Information Quality Act, and the E-Government Act of 2002. The Division also oversees and guides agency implementation of IT directives, regulations, and/or guidance issued by the Office of Management and Budget (OMB).

4 DOL IT Investment Management Life Cycles

This section describes the four standard DOL IT Investment Management Life Cycles shown in Figure 3 including their associated life cycle phases and activities. This section also identifies specific management principles, terms, tools (i.e. references to applicable and/or useful templates), requirements, and/or management practices associated with each life cycle.

Note these IT investment management life cycles do not appear in the PMBOK Guide. These IT Investment Management areas fulfill federal IT management legislative requirements (i.e., the CCA of 1996, GPRA, PRA, FISMA of 2002, and the E-Gov Act of 2002) and OMB related IT directives, circulars, and/or memorandum requirements. These areas are also consistent with sound, long-standing, and proven DOL and federal IT investment management practices.

4.1 Strategic Business Management

At DOL, Strategic Business Management (SBM) ensures that information technology is a key enabler to achieving business mission success and not the business driver. SBM improves the alignment between business and technology across DOL to improve program performance and contribute to achieving the Secretary's outcome goals. The value of SBM is realized via:

- Supporting and enhancing DOL's business mission operations
- Enhancing DOL's ability to achieve business mission success
- DOL business optimization (i.e., greater business and technology alignment, greater IT efficiencies and effectiveness, and greater IT modernization and innovation)
- Improved DOL performance (i.e., business efficiency and effectiveness leads to higher levels of operational performance)
- Better business and information technology decision making
- Greater agility to meet future business needs (i.e., future capable and ready)
- Greater DOL business transparency
- Greater DOL alignment with the President's Management Agenda and OMB initiatives and strategies (i.e., Digital Government Strategy, Shared First, Cloud-first, Cybersecurity, Mobile Strategy, Open Data Policy).

SBM improves the alignment between the Departments planning activities, Agency operating plans, operations, and business, mission and goals —thus ensuring information technology is used strategically to enhance the performance capabilities (i.e., to modernize) the Department.

SBM encourages DOL agencies to take a near-term and long-term view of technology across DOL to leverage economies of scale (e.g., standardization, consolidation, shared services, and new technologies such as cloud-computing), understand the demand for IT services as the business evolves, manage and justify IT costs from a business perspective, and ensure that the "right" IT projects are being funded to meet current and future agency business processes and mission needs.

As shown in Figure 2, there are three SBM life cycle phases, they include:

1. Strategic Business Alignment
2. Technical Alignment
3. Monitor and Realignment

The focus of the Strategic Business Alignment (SBA) phase is on aligning a DOL agency IT investment to the strategic business mission goal and objectives of the agency the investment is supporting as well as the Department's five year Information Resources Management (IRM) Strategic Plan, which describes the Department's IT strategy including the strategic goals and objectives as well as the annual DOL Enterprise Roadmap. By aligning to the DOL IRM Strategic Plan and Roadmap, an IT investment is ensuring its alignment with the Department's IT strategic plans, the Department's Strategic Plan as well as the President's Management Agenda (PMA) and/or Office of Management Budget (OMB) driven strategic initiatives. This alignment is important to meeting Departmental as well as Administration goals and objectives. It's also essential to show alignment to increase the chances of securing necessary IT investment funding from OMB during the annual budget planning and request process. (For further information on the DOL IRM Strategic Plan and Enterprise Roadmap, see the applicable subsections below.)

The SBA phase also ensures that an IT investment is in alignment and/or compliance with the Federal Enterprise Architecture Framework (FEAF) Business and Performance Reference Models as described in OMB's, *The Common Approach to Federal Enterprise Architecture*, May 2012. This supports and allows DOL agencies to better manage their IT investments as strategic business assets and as a component of their IT portfolio to identify various opportunities including for example strategic sourcing, standardization, consolidation, and/or shared services to enhance and/or optimize the utilization of agency resources. To assist and support agency IT investment PMs and/or IPTs in complying with the intended goals and requirements associated with this phase, the DOL OCIO has developed an IT Investment Target Architecture (TA) and Transition Strategy and Sequencing Plan (TS&SP) template to be completed and submitted as part of the DOL IT CPIC quarterly Control Review process. The OCIO reviews agency IT Investment TAs and TS&SP to ensure compliance with policies and standards but analyzes the information to identify potential opportunities to enhance and/or optimize the utilization of resources across the Department. A copy of the TA and TS&SP templates can be found in the OCIO Resource Library on LaborNet under the Strategic Business Management (SBM) subject area. (For further details on the CPIC quarterly Control Review process, see the CPIC section below.)

The Technical Alignment phase focuses on the planning, development, alignment, and/or compliance of an IT investment's Data & Information, System & Application, Network & Infrastructure, and Security & Privacy architectures in accordance DOL associated policies, guidance, processes, and standards as well as in compliance with the associated components and requirements of the TA and applicable FEAF models. Technical alignment allows DOL agencies to manage their IT investments on an individual basis and as part of their portfolio to identify opportunities to enhance and/or optimize the utilization of their resources. It also supports the OCIO in identifying potential opportunities to enhance and/or optimize the

utilization of resources at the Department level. The DOL Chief Technology Officer (CTO), who also chairs the DOL Enterprise-wide Technology Innovation Forum, is responsible for implementing and ensuring the activities associated with the Technical Alignment phase. This includes for example the Data and Information, Systems and Applications, and Network and Infrastructure domains of the enterprise architecture[2], as well as the technology standards and configuration management. The CTO is responsible for ensuring DOL agencies are in compliance with the requirements of this phase.

The Monitor and Realignment phase is focused on monitoring and controlling the SBM status of DOL's IT investments including most notably the review and evaluation of IT Investment TAs and TS&SP's as part of the CPIC Control Review process. The review and evaluation process ensures alignment with DOL SBM goals, objectives and established standards as well as compliance with the FEAF and the associated components and requirements of the Common Approach. Based on the outcome of this SBM review and compliance assessment/evaluation process, DOL agency IT investments are provided guidance and feedback from the OCIO on how to better align the IT investment's architecture (i.e., Business Reference Model (BRM) and Performance Reference Model (PRM)) to the OCIO's Enterprise Roadmap and to the Departmental IT goals and objectives as described in the DOL five year IRM Strategic Plan.

The DOL OCIO SBM program manages the business, investment performance and common services elements within traditional federal Enterprise Architecture program scope. This ensures close alignment with the Capital Planning and Investment Control (CPIC) and management functions.

4.1.1 DOL IRM Strategic Plan

The DOL IRM Strategic Plan serves as the Department's authoritative five year IT strategic planning document.

The Department of Labor Strategic Plan describes key areas of innovation and reform occurring at the Department and focuses around the following areas: systems and structures, employees, programs, and transparency to the public – which are described in detail in the Plan.
One of the key strategic initiatives launched as a direct result and in support of the transformative reforms was the DOL IT Modernization Initiative. The DOL IT Modernization Program was announced with the following overarching goals:

- Improved Delivery of Services: IT modernization is focused on helping DOL employees better perform their jobs by enabling the Department to quickly implement new IT solutions to improve the level and quality of services available to the agencies and public.

[2] See *The Common Approach to Federal Enterprise Architecture*, May 2, 2012 for further details on the concepts, standards, and principles associated with the Federal Enterprise Architecture Framework.

- Better Information Sharing: IT modernization will eliminate internal barriers to accessing cross-agency information, by reducing technical complexity and improving data sharing between agencies and offices to meet business missions.

- Greater Efficiency: IT modernization will focus on streamlining operations and providing a better return on investment on technology expenditures, to support cost savings across the Department.

The DOL IRM Strategic Plan can be found in the DOL OCIO Resource Library on LaborNet.

4.1.2 DOL Enterprise Roadmap

The DOL Enterprise Roadmap (ER) serves as the Department's authoritative reference providing a near term (12 to 18 month) view for IT implementation across the Department. The DOL ER describes DOL's current and future enterprise-wide view of its business and IT environment from an architectural perspective. It reflects the implementation of new and updated business capabilities and enabling technologies which support the Department's strategic goals.

The DOL Enterprise Roadmap can be found in the DOL OCIO Resource Library on LaborNet.

4.2 Capital Planning and Investment Control (CPIC)

DOL's CPIC process is managed and maintained by the OCIO through a deliberate and structured approach to managing DOL's IT investments. Agencies are directed to follow DOL's established and highly structured CPIC process in their planning, development, acquisition, funding and budgeting of IT investments. This mature and structured CPIC process ensures a uniform approach to IT investment management at DOL.

As shown in Figure 2, there are three CPIC life cycle phases, they include:

1. Select
2. Control
3. Evaluate

These three phases are described briefly below. A more detailed description of these phases including the activities and deliverables required can be found in the DOL OCIO CPIC Guide. Also, see the DOL Resource Library for other CPIC related guidance including helpful calendars, instructions, templates, and copies of applicable CPIC training materials provided to Departmental staff.

Select: The Deputy Secretary and the Assistant Secretary for Administration and Management (ASAM and OCIO), review specific proposed initiatives and prioritize them based on how each supports the Department's strategic goals and objectives through the budget process. This process is informed by the Department's Strategic Plan, Agency Operating Plans, Agency priorities and recommendations of the Deputy CIO. These priorities are incorporated into the Department's budget submission to OMB.

Control: Control is applied to major and non-major IT investments at the departmental level through the CPIC processes.

DOL uses Net Present Value (NPV) and ROI as evaluation criteria to comparatively evaluate investments. Through the CPIC process, investment selections are made based on both an Alternative Analysis and Cost-Benefit Analysis (CBA). At a more granular level, the OCIO has established control of individual projects through Program Management Reviews of key milestones and deliverables associated with SDLCM processes to monitor interim results of IT service acquisition, development, and consolidation projects. This program management methodology and process allow the OCIO to identify and take corrective action when needed. These mechanisms provide visibility into IT projects and establish management control points for assessing project cost, schedule, and quality.

As part of DOL's quarterly CPIC Control phase IT investment review process, the portfolio of DOL IT investments is reviewed and assessed for policy and lifecycle process compliance with respect to each of the IT process lifecycle areas including EA. Specifically, based on threshold levels and work patterns, OCIO staff review these IT investments with respect to performance management and transition planning, including the alignment of the IT Investment with the business mission and functional needs of the Agency; Agency architecture updates to capture core business functions and processes and alignment with the Common Approach to the Federal Enterprise Architecture (FEA) including the consolidated reference models and the Collaborative Planning Methodology (CPM). In addition, as part of the annual budget formulation process, the OCIO staff review each IT investment Exhibit 300 document to ensure the investment is aligned with the Agency business mission and goals, as outlined in operating plans and the DOL's Strategic Plan. Project plans are developed to support major IT investments identified in the Agency Operating Plans and IRM SP. The project plans and key project life cycle deliverables contain a sufficient level of detail to ensure that they satisfy requirements for achieving Departmental IT services' scope and objectives. Deliverables include those related to communications and change management, training, testing, facilities, security, contingency operations and disaster recovery.

Evaluate: A key element in evaluating the Department's IT assets is identifying performance measures for determining whether the services are delivered as they are defined and projected. Performance measures must be identified for incorporation in Service Level Agreements (SLAs) and acquisition specifications during the concept phase of the life cycle. Post-implementation service metrics are monitored to determine whether those objectives have been and continue to be achieved.

IT performance measures fall into two categories. One covers program-area-related measures considered when making investment decisions. The other addresses measures associated with the delivery of such services, including but not limited to availability, performance, reliability and functionality. The operational measures become service standards that are incorporated into service-level agreements and service catalogues. The Performance Improvement section outlines DOL's approach to program management strategies and the Program Review Board.

4.3 System Development Life Cycle Management (SDLCM)

The DOL System Development Life Cycle Management (SDLCM) Manual establishes and describes the standard methodology including principles, practices, and guidelines for governing the conceptual planning, requirements definition, design, development & test, implementation, operations & maintenance, and disposition of IT investments within the DOL. The manual has been created to assist and support DOL Agencies in successfully managing their IT investments throughout the entire life cycle of the investment. It applies to all IT investments including for example custom software application development, COTS application implementation, integration, IT infrastructure changes, as well as IT services (i.e., fully outsourced services, cloud computing solutions, etc.). The manual provides a proven, structured, and standardized life cycle management approach to all DOL IT investments.

The DOL SDLCM methodology is based on standard SDLC principles and practices that are time-tested and have been proven successful for managing IT investments in the private sector as well as in the Federal Government including civilian agencies and the Department of Defense. The SDLCM methodology serves as the structured mechanism to ensure that DOL IT investments are developed, modified, enhanced, as well as operated and maintained efficiently and effectively. Following the SDLCM methodology ensures DOL IT Investments are managed properly and are delivered on budget, schedule, and with the promised functionality. It also assists and supports IT investment managers in achieving the intended or planned investment mission, goals, financial benefits as well as applicable DOL IT strategic goals and critical success factors. It sets forth a standard, repeatable, and reliable process for managing IT investment development, acquisition, implementation, and operating activities. The life cycle process ensures IT investment are monitored, controlled, measured, documented, and managed efficiently and effectively in accordance and compliance with DOL IT policy and legislation (e.g., the Clinger Cohen Act). The SDLCM adds value to DOL IT investments by establishing a uniform and standardized approach to IT investment management. The methodology supports as well as guides IT investment PMs and IPT members through many required activities and challenging issues throughout the life cycle of an IT investment.

The SDLCM methodology is flexible and adaptable as DOL IT PMs and IPTs are able to choose the best approach to implementing the life cycle phases for their IT Investment. For example, IT PMs and IPTs are able to choose between phased, sequential, modular, iterative and/or incremental development approaches depending on the nature (e.g., size, scope, complexity, criticality, and/or timing) of the IT investment being developed.

For large and/or complex IT investments, the DOL OCIO and OMB are requiring modular, iterative, and/or incremental development approaches. See OMB's "Contracting Guidance to Support Modular Development", June 14, 2012, for details regarding module development as well as guidance with contracting and implementing a modular development approach for IT investments

To assist and support DOL IT PMs and/or IPTs in understanding and applying the SDLCM methodology, the DOL OCIO developed the System Development Life Cycle Management Manual (SDLCMM). The SDLCMM serves as the mechanism to ensure IT investments follow

an established, proven, and standard life cycle process. The DOL SDLCMM is consistent and in accordance with the following:

- National Technology Transfer and Advancement Act of 1995
- Information Technology Management Reform Act of 1996 – ITMRA (Clinger Cohen Act)
- OMB Circulars (i.e. A-11, A-130, A-94, A-109)

As shown in Figure 2, there are seven SDLCM life cycle phases, they include:

1. Conceptual Planning
2. Planning and Requirements
3. Design
4. Development & Test
5. Implement
6. Operations & Maintenance
7. Disposition

These seven phases are described briefly below. (Note that a detailed description of these phases including the associated inputs, activities, and required deliverables can be found in the DOL OCIO SDLCM Manual.)

Conceptual Planning: During this initial phase, the need to develop or significantly enhance an IT investment is identified; the feasibility and costs are assessed; and the risks and investment-planning approaches are defined.

Planning and Requirements: This phase includes detailed planning as well as the development of business and functional requirements that the IT investment will fulfill or address.

Design: During this phase, functional requirements are translated into preliminary and detailed designs. Decisions are made to address how the IT investment will meet functional, physical, interface, and data requirements.

Development and Testing: The IT investment is validated through a sequence of unit, integration, system, and acceptance test activities. The objective is to ensure that the IT investment solution functions as expected and user requirements are satisfied.

Implementation: During this phase, the new or enhanced IT investment is installed in the production environment, users are trained, data is converted (as needed), and the IT solution is turned over to the IT Investment owner and/or the operations staff.

Operations and Maintenance: This phase covers the operations and maintenance of the IT investment solution to ensure that user needs continue to be met and that the solution continues to perform according to business needs/requirements and define performance requirement or Service Level Agreement (SLA) criteria. Routine hardware and software maintenance and upgrades are performed to ensure effective IT Investment operations.

Disposition: This final SDLCM phase represents the end of the IT investment's life cycle. It provides for the systematic decommissioning and/or termination of an IT investment to ensure that vital information is preserved for potential future access and/or reactivation. All sensitive information not preserved for future use must be fully sanitized to prevent disclosure to unauthorized parties.

4.3.1 Software Life Cycle Management

Today more than ever, software[3] (otherwise known as computer software, programs, operating systems, or applications) is an integral part of an IT investment (i.e., system and/or service). By definition, software is an automated system or tool that provides various capabilities and typically performs numerous functions depending on the intended use and/or application of the software.

In addition, a software operating system or application has a life cycle and the software life cycle needs to be understood and efficiently and effectively managed to ensure the software operates as needed or required.

A DOL software application needs to be carefully planned, designed, developed (i.e., created and/or configured), tested, and implemented in an operational environment. Once implemented in an operation environment it needs to be administered and maintained via updates to ensure it is operating correctly.

Software applications can vary in size, scope, complexity, cost, and/or business mission criticality. Size refers to either the actual file size of the program typically measured in kilobytes, megabytes, or gigabytes. Scope refers to or includes the capability, functionality, the number of instances of the software that are or will be implemented within a DOL agency, the number of users supported or licensed to use the software application, the number of DOL agencies using the software, the total number of internal and/or external users, and/or business mission importance. Complexity refers to or includes the combination of size, scope, and the number of internal and external interfaces it requires to other software applications. Complexity also includes factors such as the amount of time and/or resources necessary to develop, configure, implement, administer, train, and/or maintain. Cost refers to the one-time acquisition and implementation costs as well as the annual recurring costs to operate and maintain the software.

[3] Most software today falls into one of two categories, either as an operating system or as an application. An operating system is used to control the associated computer hardware and external interfaces. Software applications, on the other hand, are dependent on an operating system for it to be used or run. In either case, in order to run or operate the software, it needs to be loaded and/or installed on a hardware system such as computer system or one or more computer-based servers. A deployment of a DOL IT investment may require the deployment of one or more operating systems and/or one or more applications, depending on the IT solution.

Business mission criticality refers to the operational importance or priority of the software application in supporting or performing DOL business mission functions.

Figure 5 below illustrates the DOL software life cycle phases in the context of the DOL IT IMLC. The upper portion of the figure shows the DOL IT IMLC as described in Section 3. The bottom half shows an example (for illustrative purposes) incremental/iterative software development approach with three release cycles implemented utilizing the SDLCM life cycle phases. In this example, the three releases are implemented in six month increments and it is assume they are tested and approved in a development environment before being loaded and run in a production environment.

The SDLCM manual allows PMs and IPT to choose the software development model and/or deployment approach that works best for the system solution – whether the solution includes one or more software applications and/or interfaces, custom software, Commercial-of the-Shelf (COTS), and/or Government-of-the-shelf (GOTS) software that needs to be developed or configured and/or integrated into a system solution. The SDLCM manual provides a proven, structured, and standardized life cycle management approach applicable to most if not all DOL IT investments – whether considered a software system, application, or interface.

The SDLCM methodology presented in this manual is flexible and adaptable as the life cycle phases can be implemented using a phased, sequential, modular, iterative and/or incremental development approach depending on the nature (e.g., size, scope, complexity, criticality, and/or timing) of the system being developed. The life cycle principles and practices presented in this manual apply regardless of the development approach. Likewise, PMBOK principles, processes, and the associated knowledge areas apply regardless of the size, scope, complexity, criticality, and/or timing of projects – whether a software or system development project or investment.

See Appendix F for more information on various Software Life Cycle Models that may be implemented. Figure 7 in the appendix illustrates, as an example, an iterative/incremental software development approach implemented utilizing the SDLCM life cycle phases.

The DOL SDLCM manual can and should be used throughout the entire life cycle of a software-based IT investment - from conceptual planning to disposition. The software development model and deployment approach is to be defined by DOL PMs and/or IPTs and approved by the OCIO during the conceptual planning phase or as part of the integrated baseline review process. For more information on the DOL IT investment baseline review process see the DOL IT Baseline Management Policy and the associated IT Baseline Management Guide, both can be found in the OCIO Resource Library on the DOL LaborNet under the Baseline Management topic area.

Figure 5: DOL's Software Life Cycle Phases in the IT IMLC

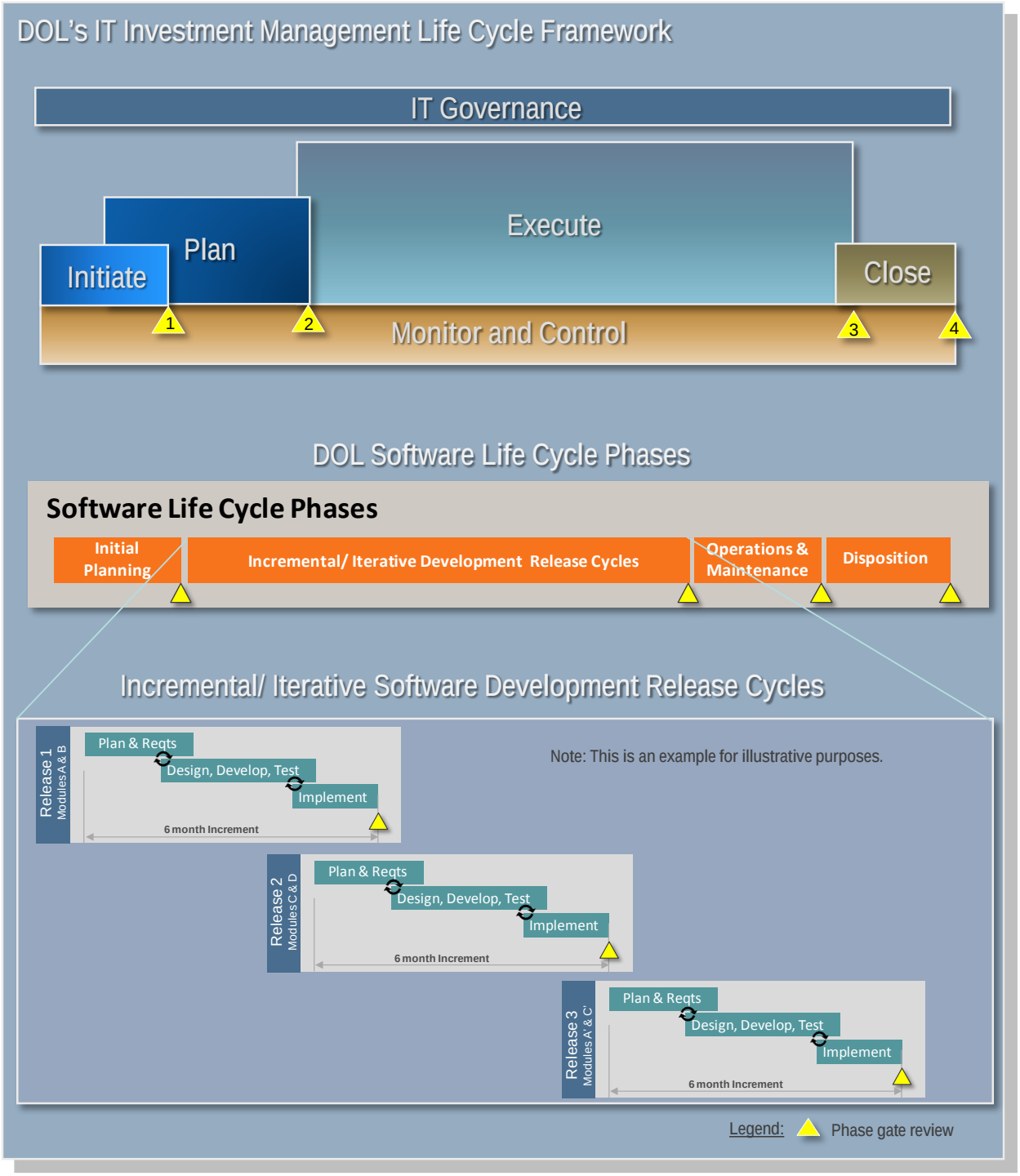
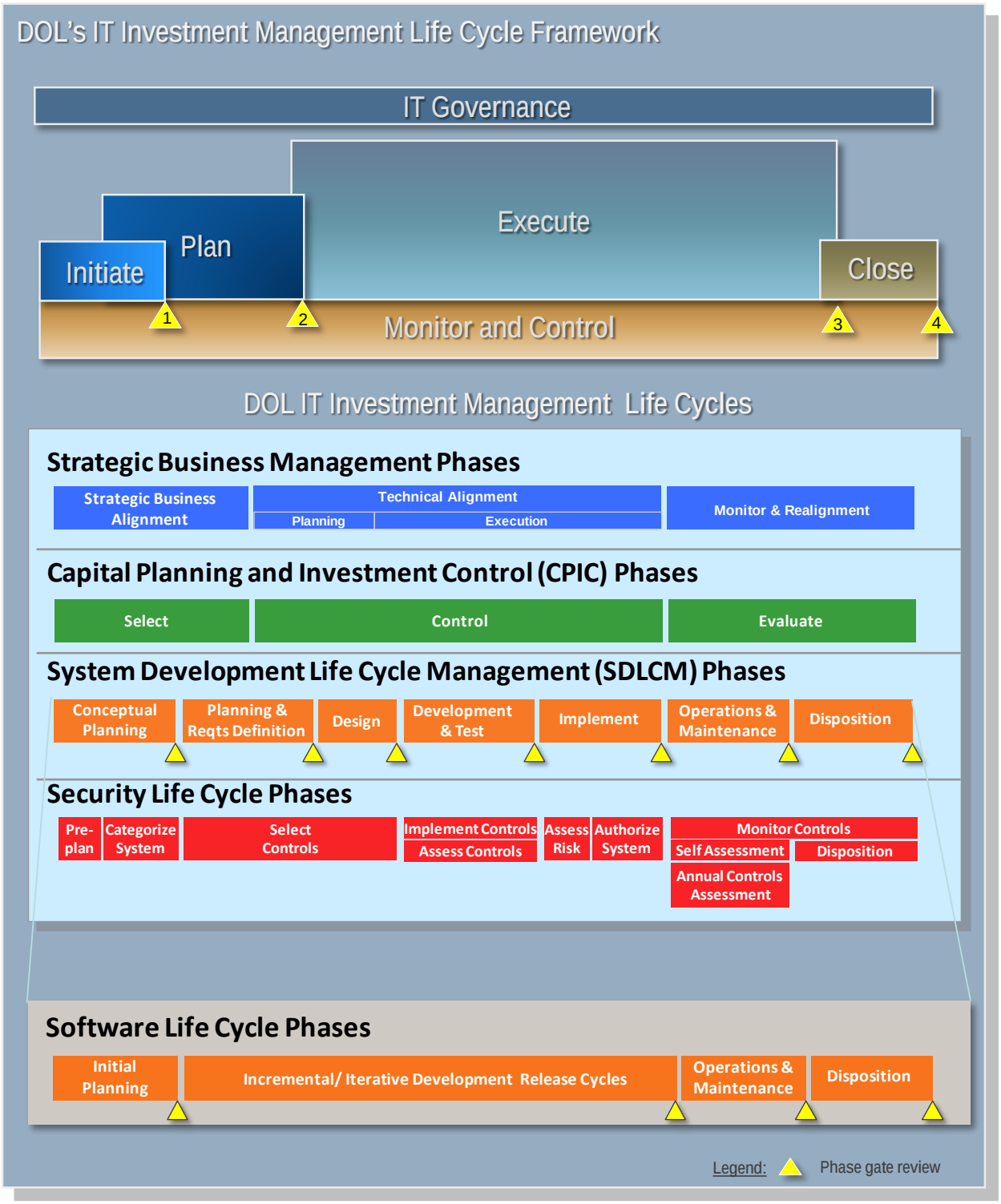


Figure 6 below illustrates the DOL software life cycle phases in the context of the DOL IT IMLC and IT Investment Management Life Cycles.

Figure 6: DOL's Software Life Cycle in context of the SDLCM, the IT Investment Management Framework, and IT IMLC



4.4 IT Security (Information Assurance)

The OCIO Information Assurance Division (IAD) is responsible for implementing and managing DOL's Cyber Security Program, a critical part of sustaining the momentum of the DOL IT Modernization effort. The DOL Cyber Security Program is governed by DOL policies and procedures as well as the DOL Cyber Security Strategic Program Plan (CSSPP). In addition to the CSSPP, the OCIO IT Security team has created and maintains a twenty-three (23) volume Computer Security Handbook (CSH), which defines and describes the Department's IT security policies, processes, procedures, and associated guidelines. DOL's Cyber Security Program formulates the structure of DOL's IT Security Framework which is comprised of several enterprise security objectives, including but not limited to:

- Enterprise Security Continuous Monitoring Program
- Enterprise Risk Management Strategy
- Enhanced Security Training & Awareness Program
- Enterprise Security Services Architecture
- Enterprise Privacy Program

Each of the security objectives outlined above comprises only a fractional component of the overall IT Security Framework. This IT Security Framework provides a high-level structure identifying enterprise security policies and managing the distribution, utilization, and administration of security services throughout the enterprise. IAD will model this framework through the Department's EA solution and address all architectural layers including Performance, Business, Data, Application, Technology and Security. The framework is consistent with the Federal Enterprise Architecture (FEA), Security and Privacy Profile and the DOL Consolidated Target Enterprise Architecture. The DOL IT Security Framework is in compliance with the Federal Information Security Management Act (FISMA) and follows benchmark standards and guidelines as established by the National Institute for Standards and Technology (NIST). This security framework sets the stage for DOL to implement an enterprise-wide approach to security within the design, development, deployment, and use of information, applications, and infrastructure in a manner consistent with federal policies, guidelines, and the DOL SDLCM Manual.

DOL, like all Federal agencies, is faced with challenges from the evolving realities of IT investment and portfolio decisions. During fiscal year FY 2012, DOL's OCIO stood-up a Program Management Office (PMO) which provides oversight, review and tracking for all OCIO initiatives, including the key cyber security initiatives. DOL remains focused on ensuring all major IT investments yield the expected outcomes and the highest return on investment. As such, all major DOL IT investments and portfolio decisions are integrated into the overall capital planning process to ensure IT security goals are incorporated and aligned with the objectives outlined in the DOL CSSPP. The CSSPP supports DOL's broader vision for IT Modernization strategic initiatives of improved delivery of services, better information sharing, and greater efficiency. For each IT investment, all IT security deliverables, defined in DOL's SDLCM manual, are monitored by the OCIO IAD to ensure they align with DOL's IT security requirements. To ensure IT investments and portfolio decisions align with the Department's IT security goals, DOL continually assesses the efficiency achieved throughout the life cycle.

As shown in Figure 2, there are eight IT Security life cycle phases, they include:

1. Pre-Plan
2. Categorize System
3. Select Controls
4. Implement Controls & Assess Controls
5. Assess Risk
6. Authorize System
7. Monitor Controls, Self-Assessment, & Annual Controls Assessment
8. Disposition

The DOL OCIO Information Assurance Division oversees and manages the IT Security life cycle phases with respect to DOL's IT investments.

DOL's IAD within the OCIO is responsible for implementing and managing DOL's Cyber Security Program. DOL has established and maintains a Computer Security Handbook (CSH) defining and describing the Department's IT security policies, procedures, and guidelines. A copy of the DOL CSH can be found on LaborNet.

DOL's IT security program enables the Department to implement and manage an enterprise approach to IT security for the design, development, deployment, and use of information, applications, and infrastructure in a manner consistent with applicable federal law, policy, guidelines, DOL's SDLCM, and DOL's CSH. Some deliverables within the SDLCM are received, reviewed, and then monitored by the IAD ensuring they align with DOL's and Federal IT security requirements and standards.

The OCIO IAD is responsible for implementing and managing DOL's Cyber Security Program, a critical part of sustaining the momentum of the DOL IT Modernization effort. The DOL Cyber Security Program is governed by DOL policies and procedures as well as the DOL CSSPP. In addition to the CSSPP, the OCIO IT Security team has created and maintains a twenty-three (23) volume CSH, which defines and describes the Department's IT security policies, processes, procedures, and associated guidelines. DOL's Cyber Security Program formulates the structure of DOL's IT Security Framework which is comprised of several enterprise security objectives, including but not limited to:

- Enterprise Security Continuous Monitoring Program
- Enterprise Risk Management Strategy
- Enhanced Security Training & Awareness Program
- Enterprise Security Services Architecture
- Enterprise Privacy Program

Each of the security objectives outlined above is only a fractional component of the overall IT Security framework. This IT Security Framework provides a high-level structure identifying enterprise security policies and managing the distribution, utilization, and administration of security services throughout the enterprise. OCIO IT Security will model this framework through

the Department's EA solution and address all architectural layers that include Performance, Business, Data, Application, Technology and Security. The framework is consistent with the Federal Enterprise Architecture (FEA), Security and Privacy Profile and the DOL Consolidated Target Enterprise Architecture. The DOL IT Security Framework is in compliance with the FISMA and follows benchmark standards and guidelines as established by the National Institute for Standards and Technology (NIST). Our security framework enables DOL and the agencies to implement an enterprise-wide approach to security within the design, development, deployment, and use of information, applications, and infrastructure in a manner consistent with federal policies, guidelines, and the DOL System Development Life Cycle Management Manual.

For more IT security information as it relates to DOL IT investments, see the DOL CSH. A copy of the DOL CSH can be found on LaborNet.

5 IT IMLC Roles & Responsibilities

The section describes the roles and responsibilities of various individuals and/or stakeholders responsible for implementing the DOL IT IMLC.

The following subsections describe the role and responsibilities of the DOL:

- Project Manager
- IT System Owner
- End Users
- Integrated Project Team Members
- Agency Head
- Contracting Officer
- Contracting Officer Representative

5.1 Project Manager

The Project Manager has overall responsibility for coordinating the management and technical aspects of the life cycle of a system, including activities related to the development of a system. Responsibilities of a Project Manager may include (but are not limited to) the following: developing a Project Management Plan, developing a cost and schedule baseline, and completing an investment within schedule and budget constraints while meeting the customer's needs. In addition, a Project Manager is responsible for coordinating the development, implementation, and operation and maintenance of a system with appropriate units within an Agency (including centralized IT staff such as network operations staff, security personnel, database management staff, the IRM manager, etc.) as well as reporting the results of investments to the System Owner and other appropriate Agency staff. When appropriate, a Project Manager should present the progress of critical investments to the OCIO, EIC, and the CPIC program management team. The Project Manager performs the following functions:

- Determine investment team organization based on user and information systems organization recommendations.
- Provide detailed work assignments, making sure there are written tasks for all work.
- Develop measurement criteria that define acceptable performance of each task.
- Manage investment development risks in accordance with SDLCM guidance, providing prioritized risk lists, probability of risk occurrence, impact to the investment, and mitigating activities for all identified investment risks. Risk management planning should include the contingency costs of mitigation.
- Coordinate and/or perform system planning, design, and implementation. Report on the progress of these efforts at quarterly capital planning control reviews.
- Coordinate user involvement, ensuring adequate involvement for all phases of the investment is maintained. Particular emphasis in the requirements and testing phases is

critical. It is the Project Manager's responsibility to ensure the System Owner is involved in authorizing the completeness of the requirements.

- Schedule and direct SDLCM documentation and milestone reviews and participate in reviews conducted by independent staff or a review committee.
- Lead the resolution of problems during all phases.
- Ensure delivery of base lined and fully documented deliverables required to initiate system implementation.
- Oversee preparation of required documentation and maintenance of an investment file.
- Serve as the overall Quality Assurance (QA) manager for all required document sets and deliverables. When required, report on the QA status of all required investment documents and deliverables as part of an OCIO generated Quality Assurance Audit.
- Follow SDLCM guidance as outlined in this manual.
- Coordinate with the Computer Security Officer (CSO) to ensure all security activities are completed. The DOL Computer Security Handbook contains more in-depth information on this subject.

5.2 IT System Owner

An IT System Owner is a typically a DOL agency manager that is the single point of contact responsible for overseeing and managing an IT system throughout its life cycle. An IT System Owner performs the following functions:

- Maintains active senior-level involvement throughout the development of the system.
- Initiates the need identification process to generate a request for a new information system or modification to an existing system.
- Participates in investment review activities and reviews investment deliverables.
- Coordinates activities with the Agency Senior IT Executive.
- Obtains and manages the budget throughout the investment's life cycle against a Project Manger's delivered locked baseline.
- Identifies high-level business functions and the need for new development.
- Defines the scope and context of the new development.
- Selects functional organization representatives as the essential participants on the investment team with responsibility for defining functional and user needs.
- Holds review and approval authority for ensuring that developed products meet user requirements.
- Conducts a review of Privacy Act issues to determine applicability. If determined to be appropriate, the System Owner will prepare or oversee preparation of the Privacy Act

Notice and coordinate with the Records Management representative on the Privacy Act System Notice.

- Conducts review of Section 508 compliance issues to determine applicability.
- Provides baseline assessment performance measures to evaluate the delivered IT investment against.

5.3 End Users

Active end user participation is essential at all levels in the definition, design, and development of an IT system. Users are responsible for initiating and expeditiously resolving issues relating to both system development efforts and identification and documentation of requirements. Specifically, user objectives are as follows:

- Provide a quick and consistent review of the requirements.
- Provide statistical information relative to the work processes.
- Develop performance standards.
- Review and refine the functional requirements and their documentation.
- Approve and prioritize requirements.
- Perform user acceptance testing.

5.3 Integrated Project Team

Integrated project team (IPT) members bring technical and functional expertise to the investment with each member planning and performing tasks in that individual's area of expertise. Team members may not necessarily serve on the investment team for the duration of the investment; however, all essential investment team members must be identified in the Conceptual Planning Phase of the investment.

The investment team may include individuals fulfilling the roles of: system developer; system tester; data administrator; database administrator; quality assurance (QA) representative; risk representative; Computer Security Officer (CSO); Configuration Management (CM) representative; telecommunications representative; Acquisitions Management representative; Systems Operations representative; Freedom of Information Act/Privacy Act (FOIA/PA) representative; and other representatives required by the investment. Not every investment will have full-time staff assigned to every role, and some investments may not need all roles fulfilled. However, consider all roles during investment planning.

5.4 Agency Head

As stated in the Secretary's Order 03-2003**,** roles and responsibilities of the Agency Head are as follows:

- All Agency Heads are assigned responsibility to fully support the CIO in matters concerning information collection and burden reduction and to ensure compliance by their organizations with CIO, OMB, and PRA guidance and policies.
- All Agency Heads are assigned responsibility to fully support the EIC in matters pertaining to IT investments and to ensure compliance by their organizations with CCA and DOL IT guidance and policies.
- All Agency Heads are assigned responsibility to fully support the Department-wide investments approved by EIC and sponsored by the CIO, re-engineer Agencies' mission related processes to maximize return on IT expenditures, and ensure that IT investments are managed for successful implementation.
- The Solicitor of Labor is responsible for providing legal assistance and advice to all officials of the Department who are responsible for activities under PRA and the Clinger-Cohen Act and under this Order, except as provided in Secretary's Order 2-90 (January 31, 1990) with respect to the Office of the Inspector General.

5.5 Contracting Officer

The Contracting Officer (CO) is in charge of the contract(s) associated with the IT investment.

5.6 Contracting Officer Representative

The Contracting Officer Representative (COR) is in charge of the managing the execution of the Statement of Work and/or task order(s) associated with an IT investment in accordance with the applicable IT investment contract.

Appendix A – DOL IT IMLC Management Areas

This section describes the IT IMLC management principles, terms, tools (i.e. references to applicable and/or useful templates), requirements, and/or management practices or techniques associated with the following fifteen DOL IT IMLC business management areas:

1) Integration Management
2) Scope Management
3) Time Management
4) Cost Management
5) Quality Management
6) Human Resource Management
7) Communications Management
8) Risk Management
9) Procurement Management
10) Stakeholder Management
11) IT Investment Management
12) Change Management
13) Performance Management
14) Information Management
15) Records Management

It is important to note that unless otherwise stated or explained the principles, terms, tools, requirements, and/or techniques associated with the first nine DOL IT Investment Business Management Areas are consistent with the nine current and similarly named PMBOK Knowledge Areas. DOL PMs and IPTs are expected to apply the principles and practices found in the PMBOK Guide for each of these business areas. Therefore, the PMBOK Guide should be consulted and utilized as a resource and/or reference for understanding and applying the first nine DOL Business Management Areas. While the last six DOL IT Investment Business Management Areas are not found in the PMBOK Guide, they are important and are applicable to federal IT project/program management and are therefore described in the applicable subsections below.

Also note that the DOL IT Investment Business Management Areas described below reflect enhancements behind the general definitions and descriptions in the PMBOK Guide to accommodate the DOL environment including, for example, DOL's business and/or IT management policies, guidelines, principles, practices, and/or processes. In the unlikely event there is a conflict between the PMBOK Guide and the sections below, the language and/or information in this guide will prevail unless an exception is documented in writing and approved by the OCIO.

1. Integration Management

Integration Management, as described in the PMBOK, involves identifying, interrelating, unifying, coordinating, and documenting the various actions and interactions of the 15 business

management areas in support of the IT investment management. This includes identifying the associated business processes in each area and allocating limited resources to successfully execute and achieve the business goals and technical requirements of the IT investment. Integration Management including the following:

- Developing and completing a Project Charter,
- Developing and completing a Project Management Plan (PMP)
- Directing and managing the execution of the IT investment
- Monitoring and controlling the work of the IT investment
- Performing integrated change control
- Closing the life cycle phase of the IT investment or the entire IT investment

See the PMI PMBOK Guide, Fifth Edition for greater insight and details for these standard activities and associated inputs, tools and techniques, and outputs.

The following subsections describe these integration management activities and associated deliverables from a DOL perspective.

1.1 Project Charter

DOL PMs and/or IPTs are responsible for developing a Project Charter for all IT investments. A charter document initiates, establishes, and authorizes the existence of the IT investment. It includes and describes key high level information about the IT investment including the business need or gap that it is intended to address; the high level requirements and description of the work; the high level risks associated with implementing a solution; a summary schedule and budget information; critical success factors; and pre-assigned resources. A signed Project Charter document serves as the formal authorization to proceed in developing a PMP.

The DOL OCIO has developed a standard Project Charter template to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the Acquisition Plan. A copy of the Project Charter template can be found in the DOL OCIO Resource Library on LaborNet.

1.2 Project Management Plan (PMP)

Like the Project Charter, DOL PMs and/or IPTs are responsible for developing a PMP for all IT investments as it is a key investment management planning document. It describes the investment's goals, scope and objectives, assumptions and constraints, project organization, roles, and responsibilities as well as the work breakdown structure (WBS), schedule, resource estimates, management and technical process plans, and security and privacy requirements for the IT investment. The PMP document represents and/or describes how the PM and/or IPT members will identify, interrelate, unify, coordinate, and perform the various actions and interactions of the 15 business management areas in support of the IT investment management.

Revisions to the PMP occur at the end of each phase and as new information becomes available or as existing information such as the investment schedule or WBS are updated. Software tools designed for work breakdown structures (WBSs), Gantt charts, network diagrams, and activity

detail reports are available and should be used to complete the PMP. The size and scope of the PMP should be commensurate with the size, scope, funding level, and complexity of the systems development effort.

The DOL OCIO has also developed a standard PMP template to assist and support IT PMs and IPTs in the development and maintenance of a PMP document. A copy of the DOL OCIO PMP template can be found in the DOL OCIO Resource Library on LaborNet.

1.3 Directing and Managing the Execution of the IT investment

DOL PMs and IPTs are responsible for directing and managing the execution of an IT investment as per the approved PMP. Successful execution of the work activities is essential to ensure the successful implementation and operation of the IT investment (i.e., such that the IT investment is managed on schedule, within budget, and is performing as planned or desired).

As described in Section 4.1 and in Section 3.3, executing an IT investment requires directing and managing in a coordinated fashion the integrated work activities associated with each of the 15 interrelated IT business management areas including the four IT investment management (i.e., SBM, CPIC, SDLCM, and IT Security) life cycles.

See Section 4.11 for details on how to execute the specific DOL IT investment management life cycles including the associated activities and deliverables, since all DOL IT investments are required to follow the principles, processes, and procedures described in each of these life cycles.

Also, it is important to understand that the general principles and practices for directing and managing the execution of a project as described in the PMBOK apply to DOL IT investments. Therefore, see the PMBOK Guide for further details on the principles and practices for directing and managing the execution of an DOL IT investment.

1.4 Monitoring and Controlling the Work of the IT investment

DOL PMs and IPTs are responsible for monitoring and controlling the execution of an IT investment as per the approved PMP. Monitoring and controlling activities ensures the successful execution of the work activities, which in turns ensures the successful implementation and operation of the IT investment (i.e., it is managed on schedule, within budget, and is performing as planned or desired).

As described in Section 3.4, monitoring and controlling the work activities associated with an IT investment requires monitoring the status, progress and/or performance of the IT investment and generating reports and conducting reviews including various internal DOL process and management, and even OCIO reviews as well as external (i.e., OMB, GAO, and/or Congressional) status reporting and possible reviews. The monitoring and controlling reviews will be based on the performance against the PMP and the 15 interrelated IT business management areas including the four IT investment management (i.e., SBM, CPIC, SDLCM, and IT Security) life cycles.

See Section 4.11 for details on how to execute the specific DOL IT investment management life cycles including the associated activities and deliverables, since all DOL IT investments are required to follow the principles, processes, and procedures described in each of these life cycles.

Also, it is important to understand that the general principles and practices for monitoring and controlling a project as described in the PMBOK apply to DOL IT investments. Therefore, see the PMBOK Guide for the details. DOL internal and external reporting requirements are identified and described in the various sections and/or applicable subject areas within this document or in the associated referenced documents. See Appendix E for a complete list of references.

1.5 Performing Integrated Change Control

DOL PMs and IPTs are responsible for performing integrated change control activities the for an IT investment as described in the PMBOK Guide. See the PMBOK Guide for details on performing integrated change control work for an IT investment.

1.6 Closing the Life Cycle Phase of the IT investment or the Entire IT investment

DOL PMs and IPTs are responsible for closing life cycle phases of the IT investment or the entire IT investment as described in the PMBOK Guide.

DOL IT investment management practices and process are consistent with the PMBOK Guide for this section. See the PMBOK Guide for details on closing life cycle phase of an IT investment or an entire IT investment.

In addition, see the DOL SDLCM Manual to understand the DOL phase gate review requirements for an IT investment. Also, see the SDLCM Disposition Plan requirements and template for understanding the closing (i.e., end of life cycle shutdown and decommissioning) requirements for an IT investment.

2. Scope Management

Scope Management, as described in the PMBOK Guide, involves defining, defending, and controlling the boundaries associated with an IT investment. Scope Management involves completing the following processes:

- Defining the scope of the IT investment including for instance the core features, functions and/or characteristics of the IT investment; the users and/or the community that will be utilizing the IT investment solution; the funding associated with the investment, the timeframe to develop and implement the investment; the performance characteristics and/or requirements; and
- Identifying and documenting the business needs and/or performance gaps to be addressed by an IT investment.

- Identifying and documenting the work activities to address the business need and/or close the performance gap(s); at a high level in the Project Charter and in greater detail (i.e., a or Work Breakdown Structure (WBS)) within the PMP.
- Validating the scope by acquiring senior management acceptance of the Project Charter and PMP.
- Managing, monitoring, and controlling the IT investment PMO and/or IPT members to execute the IT investment within the approved scope
- Validating and controlling the scope through the completion and acceptance of project/program related deliverables

The scope is also validated, monitored, and controlled throughout the life cycle of an IT investment through the completion and acceptance of project/program related deliverables, the completion of phase gate reviews, as well as through periodic (i.e., weekly, monthly, quarterly, and/or yearly) management reporting including DOL IT governance reporting.

See the DOL OCIO Project Charter and PMP templates for details on how to complete these documents and to capture the scope of the IT investment. A copy of the Project Charter template can be found at on LaborNet. A copy of the DOL OCIO PMP template can be found on LaborNet. A copy of the DOL phase gate review templates can be found in Appendix C.

Also see the DOL OCIO Baseline Management Guide for details and requirements on baselining (i.e., locking in and acquiring management approval of the scope) through the implementation and approval of an integrated baseline review at the beginning of an IT investment. A copy of the OCIO Baseline Management Guide can be found on LaborNet

In addition, see Chapter 5, *Project Scope Management* of the PMBOK Guide for a detailed review of the scope management processes including defining, validating, and controlling the scope as well as the associated inputs, tools & techniques, and outputs for each process.

3. Time Management

Time Management, as described in the PMBOK Guide, involves developing, managing, and maintaining a realistic schedule of work activities associated with an IT investment. Time Management involves completing the following processes:

- Identifying the work activities, the sequencing of the work activities or WBS, and the available resources associated with an IT investment
- Developing and documenting the schedule (i.e., sequencing, duration, and resources) of activities in the Project Charter and PMP
- Controlling the schedule by directing and managing the IT resources to execute the IT investment according to the defined schedule

See the DOL OCIO PMP and WBS templates for details on how to complete these documents. A copy of the DOL OCIO PMP template can be found on LaborNet. A copy of the DOL WBS template can also be found on LaborNet.

In addition, see Chapter 6, *Project Time Management* of the PMBOK Guide for a detailed review of the time management processes and the associated inputs, tools & techniques, and outputs for each process.

4. Cost Management

Cost Management, as described in the PMBOK Guide, involves planning, estimating, budgeting, financing, funding, managing, and controlling the costs throughout the life cycle of an IT investment. Cost Management involves completing the following processes:

- Planning the costs and the associated cost management activities throughout the life cycle of an IT investment
- Estimating costs
- Developing and documenting the budget
- Controlling the costs by closely monitoring and managing the costs including changes in costs

At DOL, IT investment cost management activities begin by leveraging and utilizing the detailed estimated life cycle costs included in the CBA document that was produced during the Initiate phase of the IT investment. (If a CBA was not developed, then a CBA should be developed per this guide, the SDLCM manual, CPIC process, and the CBA template.) The life cycle costs in the CBA document form the basis of the IT investment costs that are used by the PM and/or IPT during the Capital Planning and Investment Control (CPIC) process for planning and acquiring the annual budget for the IT investment. The CBA costs for the selected IT investment solution will likely need to be updated and/or refined to reflect the actual contract labor rates and other costs for all contracts awarded after the CBA document for the IT investment was completed.

Once the IT investment's annual budget has been approved through the DOL CPIC process and funding has been approved and contractually obligated, IT investment PMs and IPTs are required to actively manage, monitor, and control the IT investment's costs to ensure the successful execution of the IT investment in accordance with the management approved IT investment Charter and PMP.

DOL's IT investment cost management monitoring and control activities occur during the execution phase of an IT investment and will likely include implementing Earned Value Management (EVM) principles and processes, as applicable, as well as tracking and managing contractor invoices for work performed and/or completed per the contracts. In addition, cost management activities will include reporting the status of actual costs versus planned costs on a periodic basis to senior management, the OCIO CPIC team, other the DOL IT governance structure bodies, and/or as required by OCIO management and/or DOL or OMB IT investment management practices and guidelines. External cost reporting may include reporting actual costs on a monthly basis via the OMB IT Dashboard or quarterly via the OMB Integrated Data Collection (IDC) cost/benefit reporting process, and via the annual Exhibit 300 budget submission process.

See the DOL OCIO CBA template for more information regarding the DOL CBA and alternatives analysis process. A copy of the DOL CBA template can be found on LaborNet.

See the DOL OCIO CPIC Guide for more information regarding the DOL CPIC process and the annual budget development and reporting process. A copy of the DOL CPIC Guide can be found on LaborNet.

See the DOL OCIO SDLCM Manual for more information regarding the DOL SDLCM phases and associated deliverable requirements. A copy of the SDLCM Manual can be found on LaborNet.

In addition, see Chapter 7, *Project Cost Management* of the PMBOK Guide for a detailed review of the generally accepted good cost management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

5. Quality Management

Quality Management, as described in the PMBOK Guide, involves various life cycle activities to ensure quality is a priority and actively managed to meet or exceed specified and/or defined requirements and standards as well as achieve or exceed desired results or outcomes throughout all aspects of an IT investment's life cycle. Quality Management involves completing the following processes:

- Planning and documenting the quality management standards
- Performing quality assurance activities including audits
- Monitoring and controlling quality by recording quality audit results, assessing the results, and implementing any necessary corrective actions

At DOL, IT quality management is consistent with the PMBOK processes and it encompasses the implementation of a four step, "Plan", "Do", "Check", and "Act," quality process. The four steps and the associated activities within each step are summarized below.

1. Quality Planning (Plan)

    - Identifying, defining, and documenting in measurable terms the quality objectives, requirements, and standards for the IT investment processes and products in a Quality Management Plan (QMP)
    - Defining and documenting in the QMP the roles and responsibilities associated with the quality management activities including how quality will be measured
    - Planning and executing Independent Verification and Validation (IV&V) activities, as necessary or applicable to the IT investment

2. Quality Assurance (Do)

- Objectively evaluating the quality requirements including the results from quality control measurements that ensure appropriate quality standards are achieved
- Conducting process and product quality reviews in compliance with the QMP and this document (i.e., the DOL IT IMLC)
- Conducting process and product quality audits

3. Quality Control (Check)

- Communicating and reporting on performance
- Reviewing quality assurance activities and results with senior management and stakeholders
- Monitoring, documenting, and controlling execution of quality activities to assess performance and if necessary identify changes
- Placing work products under configuration management

4. Quality Improvement (Act)

- Collecting improvement information
- Implementing preventive or corrective action to avoid and/or resolve quality deficiencies with processes and/or products and to prevent recurrences
- Maintaining a "lessons learned" repository
- Updating the Quality Management Plan and/or policies and processes, as needed

The four quality management steps described above are directly applicable to improving the quality of IT business and/or management processes as well as in the development of quality IT products. Each of these quality areas is described in the following subsections.

5.1 Process Quality

Process quality focuses on the processes associated with the 15 Business Management areas in Figure 1 and the processes used to create the IT investment deliverables in each area. Process quality ensures that the processes are being implemented correctly and producing the intended results. PMs and IPTs should develop IT investment process quality success criteria as part of the QMP document. The following represent process quality success criteria that should be applied to most DOL IT investments:

- To apply, implement, and complete the IT IMLC, as illustrated in Figure 1, including the 15 IT investment business management area processes for an IT investment in accordance and/or compliance with this DOL IT IMLC Guide and the PMBOK Guide

- To implement and complete the DOL IT IMLC commensurate with the size, scope, and complexity of the IT investment

- To ensure implemented business and technical management processes are within scope and support and/or comply with planned cost, schedule, and allocated resource requirements

- To ensure required process quality requirements and/or standards are established, clear, and documented in the QMP.

- To ensure the implemented processes meet or exceed the process quality standards in the QMP. This includes monitoring and controlling the implemented processes, as necessary, to ensure process quality standards are met as described in the IT Investment QMP.

5.2 Product Quality

Product quality focuses on IT investment related deliverables and/or artifacts including for example documentation (i.e., written and/or electronic) as well as physical systems and/or services, which may include hardware, software, applications, data, information, interfaces, and other tangible elements and/or components. Product quality ensures deliverables are acceptable and meet or exceed requirements, standards, and/or customer expectations. For example, deliverable documentation is complete and correct – in that it contains the required information and the information is contextually accurate. Likewise, system and/or service deliverables meet or exceed required functional and/or performance expectations, as well as comply with required contractual and/or industry standards. PMs and IPTs should define and develop IT investment product quality success criteria as part of the QMP document. The following represent product quality success criteria that should be applied to most DOL IT investments:

- To develop clear, achievable, and complete IT investment documentation that is within scope and complies with planned cost, schedule, and allocated resource requirements

- To produce clear, accurate, and complete documents for business, functional and technical requirements

- To develop traceable IT investment artifacts that meet best practices and industry standards

- To develop and complete required standards, within acceptable quality standards, as established by the contract and the Quality Management Plan.

- To produce clear, accurate, and complete documents for business, functional and technical requirements

At DOL, quality management begins with the development of a sound Quality Management Plan (QMP), which describes the quality planning, assurance, control, and improvement processes and associated requirements and/or standards. The QMP describes the roles and responsibilities of the various quality management players and stakeholders and in particular describes how the PM and/or IPT will execute the quality management processes to meet or exceed the specified quality requirements and standards in order to achieve the goals and/or intended results of the IT investment. As described above, the QMP will also describe the process and product success criteria.

The DOL OCIO has developed a standard QMP template to assist and support IT PMs and IPTs in the development and maintenance of a QMP document. The OCIO requires PMs and/or IPTs to develop, implement, and actively manage an approved QMP. A copy of the DOL OCIO QMP template can be found in the DOL OCIO Resource Library on LaborNet .

In addition, see Chapter 8, *Project Quality Management* of the PMBOK Guide for a detailed review of the generally accepted good quality management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

6. Human Resources (HR) Management

At DOL, IT HR management activities are consistent with the PMBOK HR processes and encompass (like the quality management area HR management) a four step, "Plan", "Do", "Check", and "Act," process. The four HR steps and the associated activities within each step are summarized below.

1. HR Planning (Plan)

    - Identifying, defining, and documenting in measurable terms the quality objectives, requirements, and standards for the IT investment processes and products in a HR Plan (HRP)
    - Defining and documenting in the HRP the roles and responsibilities associated with the HR management activities including how HR will be measured

2. HR Execution (Do)

    - Objectively evaluating the quality requirements including the results from quality control measurements that ensure appropriate quality standards are achieved
    - Conducting HR reviews in compliance with the HRP and this document (i.e., the DOL IT IMLC)
    - Conducting HR audits

3. HR Control (Check)

    - Communicating and reporting on HR performance
    - Reviewing HR activities and results with senior management and stakeholders
    - Monitoring, documenting, and controlling execution of HR activities to assess performance and if necessary identify changes

4. HR Improvement (Act)

    - Collecting improvement information
    - Implementing preventive or corrective HR action to avoid and/or resolve issues and/or performance deficiencies and to prevent recurrences

- Maintaining a "lessons learned" repository
- Updating the HRP and/or policies and processes, as needed

At DOL, HR management begins with the development of a sound Human Resources Plan (HRP), which describes the resource planning, execution, control, and improvement processes and associated requirements and/or standards. The HRP describes the roles and responsibilities of the various players and stakeholders and in particular describes how the PM and/or IPT will execute the HR management processes to ensure the IT investment achieves its goals and/or intended cost, schedule, and performance results.

In addition, see Chapter 9, *Project HR Management* of the PMBOK Guide to review the generally accepted good HR management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should follow and/or implement.

7. Communications Management

At DOL, IT communications management activities begin with the development of a sound Communication Plan. The Communication Plan describes the processes in which communication will flow into and out of the IT investment. It will identify significant communication, frequency, and audience. It is a proactive plan to ensure accurate, timely, and appropriate communication. It should include a sufficient level of detail to establish and maintain control of the internal and external communication channels and activities necessary to effectively manage customers, end user, and/or stakeholder expectations.

In addition, see Chapter 10, *Project Communications Management* of the PMBOK Guide for a detailed review of the generally accepted good quality management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

8. Risk Management

Risk Management activities include documenting and identifying risks to the successful completion of the investment on time and under budget. This includes investment risks; analysis, assessment, and prioritization of those investment risks, and laying out plans to implement actions to reduce the investment risks throughout the investment's life cycle. Risk Management planning provides a control mechanism to monitor, report, and direct all risk mitigation activities. It is during the Conceptual Planning Phase that risk management is initiated and continues until the investment is operational. While security risks can appear in this phase, only the security risks related to the successful implementation of the investment. Security risks inherent in operation of the system are covered is the System Security Plan.

The DOL OCIO has created a standard Risk Management Plan template and a Risk Register that all DOL IT investments are required to implement. A copy of the Risk Management Plan template and associated Risk Register template can be found on LaborNet.

For IT security related risks, see the DOL Computer Security Handbook (CSH) for information. A copy can be found in the DOL OCIO Resource Library on LaborNet.

In addition, see Chapter 11, *Project Risk Management* of the PMBOK Guide for a detailed review of the generally accepted risk management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

9. Procurement Management

Procurement management is a critical IT investment management business area as it includes the various acquisition and procurement activities associated with acquiring and implementing the life cycle management activities associated with an IT investment.

This section covers the following procurement management related activities:

- IT Investment Acquisition Plan
- ITARB and the ITARB request/approval process
- IT Spend Plan process (i.e., annual Agency acquisition plans

In addition, see Chapter 12, *Project Procurement Management* of the PMBOK Guide for a detailed review of the generally accepted procurement management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

IT Investment Acquisition Plan Overview

An IT Investment Acquisition Plan (AP) is a document that describes the acquisition and procurement strategy and plan for how all hardware, software, and telecommunications capabilities, along with contractor support services, are acquired during the life of an IT investment. The AP helps ensure that resources are available at the time they are needed. The plan includes a milestone schedule that lists activities for completion and deliverables to be produced with appropriate estimated completion dates.

The DOL OCIO has developed a detailed AP template as well as a guide to developing the Acquisition Plan to assist and support IT Investment PMs, PMOs, and/or IPTs in completing an Acquisition Plan for the IT investment. The AP template has been developed in accordance with the Federal Acquisition Regulations (FAR), Part 7, *Acquisition Planning;* the Office of Management and Budget (OMB) Capital Planning Guide, Version 2.0, Supplement to the OMB Circular No. A-11, Part 7, *Planning, Budgeting, Acquisition , and Management of Capital Assets;* and DOL SDLCM and Capital Planning and Investment Control (CPIC) guidelines. The AP supports the requirements of the OMB Exhibit 300, *Capital Asset Plan and Business Case Summary,* as well as the tenets of Performance-Based Acquisition.

A copy of the *DOL Acquisition Plan* template can be found in the DOL OCIO Resource Library on LaborNet. A copy of the *DOL Guide to Developing the Acquisition Plan for IT Investments* can also be found on LaborNet.

ITARB Overview

In July 2011, the DOL OCIO established the IT Acquisition Review Board (ITARB) to utilize strategic sourcing of IT acquisitions and ensure that IT acquisitions are aligned with the Department's strategic business and the IT modernization program. Specifically, the ITARB:

- Oversees & manages IT acquisitions as strategic business resources
- Eliminates duplicate enterprise IT initiatives; approves IT expenditures
- Supports Federal and DOL Compliance

The ITARB makes strategic IT recommendations via the CIO to the Deputy Secretary based on results and outcomes from EIC meetings.

DOL's ITARB is led by the CIO to ensure DOL's IT acquisitions are managed as strategic business resources and adhere to DOL acquisition and strategic sourcing policies. The ITARB works in conjunction with the Strategic Business Management PMO (SBM) and other IT governance bodies to manage all of DOL's IT spending. The ITARB was further strengthened in 2013 by including formalized OCIO review of Agency IT Spend Plans as part of the Department budget formulation process.

IT Spend Plan Process Overview

The DOL IT spend plan process is used to capture all planned agency IT acquisitions for the upcoming year. Identifying and documenting agency IT acquisition information as part of the IT spend plan process reduces the need for additional DOL agency IT data calls. The IT spend plan documents also assist DOL agencies in making IT expenditure decisions and make it easier for agencies to plan and manage their IT acquisition requests. The IT spend plan also allows agencies to identify and categorize their planned IT acquisitions consistent with the commodity IT services identified in the OMB PortfolioStat process as either Business Systems (i.e., Agency Mission Support Systems), Enterprise IT Systems (e.g., email, collaboration, Identify and Access Management, etc.), or IT infrastructure systems or services (e.g., desktop systems, mobile devices, mainframes, servers, etc.). The DOL OCIO created an IT Spend Plan template for DOL agencies to use and complete their annual acquisition plans. Completed Agency IT Spend Plan documents are submitted to the OCIO for review and approval.

A copy of the *DOL IT Spend Plan* template can be found in the DOL OCIO Resource Library on LaborNet.

Additionally, agency submitted IT spend plans are also leveraged by the ITARB as part of the DOL IT Governance process. The IT spend plan process has increased the efficiency and reduce the burden of individual agency ITARB requests.

10. Stakeholder Management

At DOL, stakeholder management begins by conducting a stakeholder analysis for the IT Investment. This is a systematic process for identifying and analyzing the stakeholders associated with an IT investment including identifying their needs, goals and objectives, their sphere of influence, expectations, and strategies and actions for communicating and ensuring the stakeholder are involved as appropriate throughout the IT investment life cycle.

See Chapter 13, *Project Stakeholder Management* of the PMBOK Guide for a detailed review of the generally accepted stakeholder management principles and processes and the associated inputs, tools & techniques, and outputs that DOL PMs and IPTs should followed and/or implement for each process.

11. IT Investment Management

See Figure 3 for an illustration of the entire DOL IT IMLC framework including the four interrelated and standard IT investment management life cycles. Each of the standard IT investment management life cycles, including their phases as well as the processes and activities performed in each phase, are described in detail in Section 4.

12. Change Management

DOL standard change management principles, processes, practices, and tools (i.e. references to applicable and/or useful templates), requirements, and/or management techniques will be incorporated here in a future version of this document. Until that time, DOL PMs and IPT members are encouraged to employ industry standard change management principles, processes, and practices in accordance with existing DOL and federal policies, regulations, and/or requirements, as appropriate and applicable to ensure IT investment management success, for current and/or planned DOL IT investments.

13. Performance Management

DOL standard performance management principles, processes, practices, and tools (i.e. references to applicable and/or useful templates), requirements, and/or management techniques will be incorporated here in a future version of this document. Until that time, DOL PMs and IPT members are encouraged to employ industry standard performance management principles, processes, and practices in accordance with existing DOL and federal policies, regulations, and/or requirements, as appropriate and applicable to ensure IT investment management success, for current and/or planned DOL IT investments.

14. Information Management

DOL standard information management principles, processes, practices, and tools (i.e. references to applicable and/or useful templates), requirements, and/or management techniques will be incorporated here in a future version of this document. Until that time, DOL PMs and IPT members are encouraged to employ industry standard information management principles, processes, and practices in accordance with existing DOL and federal policies, regulations, and/or requirements, as appropriate and applicable to ensure IT investment management success, for current and/or planned DOL IT investments.

15. Records Management

DOL standard records management principles, processes, practices, and tools (i.e. references to applicable and/or useful templates), requirements, and/or management techniques will be incorporated here in a future version of this document. Until that time, DOL PMs and IPT members are encouraged to employ industry standard records management principles, processes, and practices in accordance with existing DOL and federal policies, regulations, and/or requirements, as appropriate and applicable to ensure IT investment management success, for current and/or planned DOL IT investments.

Appendix B – DOL IT Governance Structure

This appendix describes the entities comprising DOL's IT Governance structure as shown in Figure 3. The sections below also describe the role and the responsibilities of the various governance entities.

B.1 DOL IT Governance Structure

Each of the entities, shown in Figure 3, are described in greater detail in the following subsections.

B.1.1 Secretary and Deputy Secretary

The DOL IT governance structure, by hierarchical organizational design, shows the Secretary of Labor and the Deputy Secretary at the top of the structure. The Secretary and/or Deputy Secretary make strategic IT governance management decisions, as necessary and/or applicable, based on information, communications, and/or recommendations received from the Assistant Secretary for Administration and Management (OASAM) Chief Information Officer (CIO). Outcomes from the Enterprise Implementation Committee (EIC), which is led by the CIO, will also be communicated, as necessary and/or applicable to the Deputy Secretary and/or Secretary. The Office of Public Affairs (OPA) coordinates and communicates DOL digital government strategy information regarding DOL websites, social media sites, and/or mobile applications as necessary and/or applicable to the CIO/DCIO and the Deputy Secretary and/or Secretary.

B.1.2 Enterprise Implementation Committee (EIC)

In May 2011, the Enterprise Implementation Committee (EIC) was established to facilitate the implementation of Department-wide and cross agency IT Modernization and customer service initiatives. Specifically, the EIC:

- Provides enterprise-wide, business-led support for business-and IT-related initiatives
- Undertakes implementation planning, prioritization, resource assignment, progress monitoring, evaluation, re-allocation and termination of initiatives
- Reviews IT performance and evaluation criteria, measures and targets
- Supports development and sharing of innovation and best practices between agencies

The EIC makes strategic IT recommendations via the CIO to the Deputy Secretary based on results and outcomes from EIC meetings. The DOL CIO chairs the EIC.

B.1.3 Chief Information Officer (CIO)/Office of the Chief Information Officer (OCIO)

The Secretary's Order (03-2003, dated May 16,2003) Update of Delegation of Authority and Assignment of Responsibility to the Chief Information Officer for Implementation of the Paperwork Reduction Act of 1995 (P. L. 104-13) and the Clinger-Cohen Act of 1996 (Information Technology Management Reform Act of 1996) (Division E of P. L. 104-106) delegates authority and assigns responsibility for implementation of the Paperwork Reduction

Act of 1995 (P. L.104-13) and the Information Technology Management Reform Act (ITMRA) of 1996 (Division E of P. L.104-106) and formally establishes within the Department of Labor the position of the Chief Information Officer (CIO). The Secretary's Order (03-2003) states that the CIO provides advice and other assistance to the Secretary of Labor and other senior management personnel of DOL to ensure that IT is acquired and information resources are managed for the Department in a manner that implements the policies and procedures of the ITMRA. In accordance with the duties assigned to the CIO by the ITMRA, the CIO:

- Is responsible for presenting proposed IT portfolios,
- Serves as the senior IT advisor to the Deputy Secretary,
- Promotes the effective and efficient design and operation of all major information management processes for the Department and provides final portfolio enhancement, and
- Designs, implements and maintains in DOL a process for maximizing the value and managing the risks of IT acquisitions. This is accomplished by providing a means for senior management personnel to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.
- The CIO shall chair and manage EIC.

B.1.4 IT Acquisition Review Board (ITARB)

In July 2011, the IT Acquisition Review Board (ITARB) was established to utilize strategic sourcing of IT acquisitions and ensure that IT acquisitions are aligned with the Department's strategic business and the IT modernization program. Specifically, the ITARB:

- Oversees & manages IT acquisitions as strategic business resources
- Eliminates duplicate enterprise IT initiatives; approves IT expenditures
- Supports Federal and DOL Compliance

The ITARB makes strategic IT recommendations via the CIO to the Deputy Secretary based on results and outcomes from EIC meetings. The DOL CIO chairs the ITARB.

B.1.5 Strategic Business Alignment Committee (SBAC)

The focus of the Strategic Business Alignment Committee is to:

- Provide strategic direction, coordination, support, and guidance to enterprise IT solutions
- Ensure compliance with Clinger-Cohen and other Federal and DOL regulations
- Facilitate IT strategic planning and EA activities

B.1.6 IT Capital Planning Committee (CPC)

The focus of the IT Capital Planning Committee is to:

- Understand IT drivers and requirements
- Ensure compliance with federal, OMB and DOL policy, regulations and controls
- Provide management guidance on policy
- Ensure IT investments achieve their intended purposes on time and within budget

B.1.7 IT Security Committee (ITSC)

The focus of the IT Security Committee is to:

- Implement and communicate IT security policies, procedures, issues and best practices
- Facilitate cross-agency support of IT security initiatives, training
- Provide feedback/ analysis on policy, procedures, standards and guidelines
- Research and collaborate on emerging security issues

B.1.8 IT Service Management Committee (ITSM)

The IT Service Management Committee (ITSM) will be established to help standardize and mature enterprise change management processes. The ITSM mission is to define, implement and oversee IT service management and change management processes, and manage risks to ensure the integrity of DOL enterprise systems shared across two or more agencies. The ITSM roles and responsibilities include:

- Overseeing DOL's transition from configuration-focused IT processes to an expanded change management and service management role supporting enterprise and infrastructure systems and applications
- Managing all changes to enterprise systems shared by two or more agencies; analyze the risks of adverse change effects and interruption to critical business processes
- Developing/enforcing System Development Life Cycle Management (SDLCM) and Information Technology Infrastructure Library (ITIL) standardization and change management technical policies, procedures and products (BMC/remedy) mandated for use by DOL agencies prior to change management and release processes
- Facilitating resolution of SDLC, ITIL and change management issues that are common across agencies and business missions
- Collaborating with appropriate Federal government and DOL administrative and agency offices to address SDLCM and ITIL processes; as required collaborate with OMB and DOL OASAM on issues related to Continuity of Operations (COOP) and Homeland Security
- Identifying working groups to address specialty areas, e.g., Configuration Control
- Participating in DOL-wide initiatives that have change management implications

B.1.9 Technology and Innovation Forum (T&IF)

The focus of the Technology and Innovation Forum is to:

- Look for new ways to use IT to enable or support the business and create value; areas of interest include:
    - Mobile Apps
    - Social media
    - Data Visualization,
    - Data Analytics
    - Open Source
    - Emergent Technologies

B.1.10 Field IT Forum (FITF)

The Field IT Forum leverages the knowledge and experience of DOLs IT field operations personnel in assessing, analyzing, managing, and/or resolving and identifying IT issues and solutions in support of DOL IT operations as well as strategic business and IT modernization program initiatives.

B.1.11 OPA's Enterprise Communications Management Group

The DOL Office of Public Affairs (OPA), Division of Enterprise Communications, oversees and manages the Enterprise Communication Management Group (ECMG), which includes DOL agency representatives that govern DOL's websites, social media sites, and mobile application development activities including creating associated policies, business processes, and guidance documents.

Appendix C – SDLCM Phase Gate Review Checklists

This appendix includes seven System Development Life Cycle Management (SDLCM) phase gate review checklists for each of the seven phases of the Department of Labor (DOL) SDLCM process. As required by the DOL SDLCM manual, version 2.3 dated May 2012 and version 2.4 dated July 2014, IT investment Project Manager's (PMs) and Integrated Project Teams (IPTs) are required to conduct reviews at the end of each SDLCM phase. These reviews require, at a minimum, the completion and sign-off of the checklists provided in this appendix.

Background

At the end of each SDLCM phase, PMs and IPTs are required to conduct a gate review to determine whether all required phase exit criteria, i.e., deliverables, Work Breakdown Structure (WBS) tasks, and any other items required by the contract Statement of Work (SOW) have been completed successfully and whether the IT Investment should continue to the next SDLCM phase.

A phase gate review begins with a complete review and assessment of the deliverables required by the phase (in accordance with the DOL SDLCM manual) as well as the WBS tasks. In addition, the PM/IPT needs to determine whether the IT investment has met the goals for the phase. If not, then the PM/IPT will need to identify what tasks need to be accomplished to complete the goals of the phase. Any cost, schedule, and/or performance delays resulting from an incomplete phase will need to be communicated to the IT Investment stakeholders, sponsors, and to the OCIO.

Once the IPT has determined that the goals of the current phase have been met, a go or no-go decision is made for proceeding to the next phase.

It is important to note that there may be reasons why a no-go decision to the next phase may be required even if all deliverables have been completed successfully and all the tasks associated with the phase have been completed. For example, based on the tasks completed during a phase it may be determined that there are complexities or issues that were not apparent at the beginning of the phase that may warrant delaying or halting work on the IT investment. Another example may be the lack of or a change in resources or funding cuts associated with the IT investment. Thus, the phase gate review may result in a no-go decision for non-performance related issue – an issue that might prevent an IT investment from being developed and deployed successfully.

Phase gate reviews should be viewed as a proactive management tool as they can be used to identify, in advance or as early as possible, activities or issues that need or will need to be addressed and/or completed in the current phase or in succeeding phases. Thus, avoiding any show stoppers in later phases of the IT investment life cycle.

SDLCM Phase Gate Review Checklist for the Conceptual Planning Phase

Project Name:							
	SDLCM - Conceptual Planning Phase					***Level of Integrity 4 3 2 1 - Circle***	
						CPIC Threshold	
						Non-Major	Major
						SDLCM Work Pattern	
						Non-Major	Major
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Conceptual Planning phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.					**Review – Enter a check next to each completed and approved item below. ✓**	
Deliverables	Request for Information Technology Services (RITS) or Statement of Concept		C			C	
	Feasibility Study					O	
	Cost Benefit Analysis (CBA) and Cost Model		C			C	
	Project Management Plan		I			C	
	Work Breakdown Structure (WBS) and WBS Dictionary		C			C	
	Risk Management Plan and Risk Register		I			C	
	Investment Target Architecture – Business Architecture & Performance Architecture		I			C	
	Investment Transition Strategy		I			C	
	FIPS 199 System Categorization Report		C			C	
	Privacy Impact Assessment		C			C	
	Statement of Work (SOW)		O			O	
	Other (please specify below … add rows as necessary)						
Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							
Signatures	Project Manager	Name					
		Signature					
		Date					
	COR	Name					
		Signature					
		Date					

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Planning and Requirements Phase

Project Name:						
	SDLCM - Planning and Requirements Phase	***Level of Integrity 4 3 2 1 - Circle***				
		CPIC Threshold				
		Non-Major		Major		
		SDLCM Work Pattern				
		Non-Major		Major		
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Planning and Requirements phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.	**Review – Enter a check next to each completed and approved item below. ✓**				
Deliverable	Investment Target Architecture - Data Architecture (DA)	C		C		
	Acquisition Plan	C		C		
	Functional Requirements Document	C		C		
	Security Risk Assessment	C		C		
	System Security Plan	C		C		
	Security Plan of Action and Milestones (POA&M)	C		C		
	Test Plans	O		O		
	Configuration Management Plan	O		O		
	Legacy Data Plan	O		O		
	Other (please specify below … add rows as necessary)					
Findings:						
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…						
Signatures	Project Manager	Name				
		Signature				
		Date				
	COR	Name				
		Signature				
		Date				

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Design Phase

Project Name:							
	SDLCM - Design Phase						***Level of Integrity 4 3 2 1 - Circle***
							CPIC Threshold
							Non-Major / Major
							SDLCM Work Pattern
							Non-Major / Major
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Design phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.						**Review – Enter a check next to each completed and approved item below.** ✓
Deliverables	Investment Target Architecture - Application Architecture (AA)	I		C			
	Investment Target Architecture - Technical Architecture (TA)	I		C			
	Test Plans			O			
	Configuration Management Plan	I		C			
	Detailed Design			C			
	Contingency Plan	I		C			
	Implementation Plan			O			
	Other (please specify below … add rows as necessary)						
Other Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							

Signatures	Project Manager	Name	
		Signature	
		Date	
	COR	Name	
		Signature	
		Date	

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Development and Test Phase

Project Name:							
	SDLCM - Development and Test Phase				***Level of Integrity 4 3 2 1 - Circle***		
					CPIC Threshold		
					Non-Major		Major
					SDLCM Work Pattern		
					Non-Major		Major
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Development and Test phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.				**Review – Enter a check next to each completed and approved item below. ✓**		
Deliverables	Test Plans	C			C		
	Implementation Plan				C		
	Acceptance Test Plan				C		
	Security Control Assessment Aid (SCAA) / Security Test & Evaluation (ST&E) Report	I			C		
	Acceptance Test Report and Approval	C			C		
	Training Plan				C		
	System Manuals				C		
	User Manuals				C		
	Security Certification and Accreditation Package	I			C		
	Other (please specify below … add rows as necessary)						
Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							

Signatures	Project Manager	Name	
		Signature	
		Date	
	COR	Name	
		Signature	
		Date	

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Implementation Phase

Project Name:							
	SDLCM - Implementation Phase	***Level of Integrity 4 3 2 1 - Circle***					
		CPIC Threshold					
		Non-Major		Major			
		SDLCM Work Pattern					
		Non-Major		Major			
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Implementation phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.	**Review – Enter a check next to each completed and approved item below. ✓**					
Deliverables	Contingency Plan Test Report	I		C			
	Security Accreditation Letter	I		C			
	System Acceptance Letter	I		C			
	Other (please specify below … add rows as necessary)						
Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							

Signatures	Project Manager	Name	
		Signature	
		Date	
	COR	Name	
		Signature	
		Date	

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Operations and Maintenance Phase

Project Name:							
	SDLCM - Operations and Maintenance Phase	***Level of Integrity 4 3 2 1 - Circle***					
		CPIC Threshold					
		Non-Major		Major			
		SDLCM Work Pattern					
		Non-Major		Major			
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Operations and Maintenance phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.	**Review – Enter a check next to each completed and approved item below. ✓**					
Deliverables	Security Controls Test Report / Continuous Monitoring Annual Report	I		C			
	Security Re-certification and Accreditation Package	O		O			
	Security Self-Assessment (Annual)	I		C			
	Disposition Plan	I		C			
	Other (please specify below … add rows as necessary)						
Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							

Signatures	Project Manager	Name	
		Signature	
		Date	
	COR	Name	
		Signature	
		Date	

Legend:

C – Core, O – Optional, I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

SDLCM Phase Gate Review Checklist for the Disposition Phase

Project Name:							
	SDLCM – Disposition Phase	***Level of Integrity 4 3 2 1 - Circle***					
		CPIC Threshold					
		Non-Major		Major			
		SDLCM Work Pattern					
		Non-Major		Major			
Objective	Verify that the IT investment IPT/PMO completed the required DOL SDLCM Disposition phase deliverables and any other required activities or deliverables as specified in the IT investment contract SOW and/or in the WBS.	**Review – Enter a check next to each completed and approved item below. ✓**					
Deliverables	Disposition Plan			C			
	Other (please specify below … add rows as necessary)						
Findings:							
Outcome: ✓ ( ) Approved, ( ) Not Approved – See Findings, ( ) Conditional Approval – See Findings, ( ) Other – explain…							
Signatures	Project Manager	Name					
		Signature					
		Date					
	COR	Name					
		Signature					
		Date					

Legend:

C – Core
O – Optional
I – Core, unless it is integrated into a parent deliverable. If not integrated, then it should be reviewed independently

Appendix D – Software Life Cycle Models

One designed purpose of the SDLCM approach is to provide a mechanism that ensures developing systems meet established user requirements and support critical DOL success factors. The SDLCM sets forth a standard and logical process for managing system development activities in a controlled, measured and documented manner (in-line with both legislative and industry standards). Seven sequential life cycle phases have been defined as part of this standard and logical process (referred to as the full-sequential life cycle process, most similar to the Waterfall model described below).

The importance of a software life cycle model is that it depicts the significant phases or activities of a software investment from conception until the product is retired. It specifies the relationships between investment phases, including transition criteria, feedback mechanisms, milestones, baselines, reviews, and deliverables. For the delivery of large and complex IT systems, it is a critical element for the overall success of an investment, incorporating all aspects of system engineering influences on an investment from management to design.

Considering the benefits provided by the incremental/iterative life cycle development approach, both Departmental IT and EA policy guidance states investments should follow a phased and modular incremental approach. Many advantages are realized by delivering large and complex IT investments in useful increments or iterations, including reduced complexity, reduced risk, earlier user feedback, and earlier implementation for subsets of the system. To achieve this, the full-sequential phases of the SDLCM should be utilized in combination with desirable iteration based aspects of other common software life cycle models utilized in industry and across the Federal Government.

Project Managers are encouraged to diagram the specific adaptation of a life cycle model being utilized for an investment, and detail its alignment with the SDLCM as part of their planning effort. This model will contribute to the control review process by providing a vehicle to easily convey the phase location of an investment, allowing easy cross-reference to the required state of core document deliverables and updates. Much of the motivation behind utilizing a life cycle model is to provide structure and a mechanism for ensuring that quality is built into a system development investment. This helps avoid the substantial problems that can result from the activities of an "undisciplined hacker" during investment development.

Types of Models

Life cycle models specifically describe the interrelationships between software development phases. Some common life cycle models are:

- **Spiral** - The spiral development model is a risk-driven process model that is used to guide multi-stakeholder concurrent engineering of software-intensive systems. It has two main distinguishing features. One is a cyclical approach for incrementally growing a system’s degree of definition and implementation while decreasing its degree of risk. The

other is a set of anchor point milestones for ensuring stakeholder commitment (funding allocation) to feasible and mutually satisfactory system solutions.

- **Waterfall** - Well suited to investments that have low risk in the areas of user interface and performance requirements, but high risk in budget and schedule predictability and control. The waterfall model describes a development method that is linear and sequential. Development moves from concept, through all phases of development and ends up at operation and maintenance. Each phase of development proceeds in strict order, without any overlapping or iterative steps. The disadvantage of this approach is that it does not allow for much reflection or revision. Once an application is in the testing stage, it is very difficult to go back and change something that was not well thought out in the concept stage. The least flexible and most obsolete of the life cycle models.
- **Throwaway Prototyping** - Useful in "proof of concept" or situations where requirements and user's needs are unclear or poorly specified. The approach is to construct a quick and dirty partial implementation of the system during or before the requirements phase. The developer creates a prototype for requirements that are under-specified or ambiguous, demonstrating a part of or the entire requirement in question. This creates a channel of communication with the end-user. The basis of the newfound communication is derived from the understanding of how the prototype functions.
- **Evolutionary Prototyping** - Use in investments that have low risk in such areas as budget, schedule predictability and control, or large-system integration problems, but high risk in user interface design. The evolutionary prototyping rationale is one where the prototype is grown and refined into the final product.
- **Incremental/Iterative Development** - This process is for constructing several partial deliverables, each having incrementally more functionality. An iterative life-cycle is based on successive enlargement and refinement of a system through multiple development cycles of planning, design, development, testing and implementation. The system grows by adding new functions within each development cycle. After a preliminary conceptual planning phase, development proceeds through a series of development cycles. Each cycle tackles a relatively small set of requirements with the system growing incrementally as each cycle is completed.
- **Reusable Software Model** - The objective of the Reusable Software Model is to improve investment cycle time, system quality and system maintainability through a formal understanding of the features and structure of a system family. It is also achieved through the development and maintenance of reusable software resources that simplify the development of new investments in the family.
- **Automated Software Synthesis** - This process relies on tools to transform requirements into operational code. Formal requirements are created and maintained using specification tools. This is an active research area and is one technique that can be utilized as part of a rapid application development approach.

Because the life cycle steps are described in very general terms for most of these standardized models, they are adaptable and their implementation details will vary among the different organizations that use them. Organizations generally mix and match the approach of different life

cycle models, incorporating the relationship between phases of some of the common models, to specific organizational guidelines or approaches tailored to development products or capabilities (investments). The point is that the SDLCM approach specifies the sequential phases involved with the Department's model, executed in sequence this is the waterfall approach. It also specifies the format for required deliverables, including the schedule of deliverable creation and update based upon the work pattern being utilized.

A very critical responsibility and aspect of oversight for the project manager is ensuring both internal and contract staffs utilize the appropriate interrelationships between phases for the specific type of system being developed. Whatever approach is used should meet the compliance standards within the SDLCM (i.e. templates and deliverables) and deliver the benefits of the specific life cycle model being utilized (i.e. the modular benefits provided by aspects of the incremental/iterative development approach).

Figure 7**,** on the next page, demonstrates how the SDLCM phases are implemented in conjunction with an incremental/iterative software development model. In the diagram, the investment team moves from the SDLCM planning phases into developing useful iterations of the system in the form of a pilot and prototype; followed by several releases of the system, each adding increased functionality with each useful iteration delivered. Each useful increment of the system moves into operations and maintenance before being superseded and archived.

The initial planning iteration of the incremental/iterative development model aligns with the select phase of capital planning and the conceptual planning and planning and requirements definition phases of the SDLCM. The prototype, pilot, and release iterations of the incremental/iterative model align with the control phase of capital planning; and the design, development/test, and implement phases of the SDLCM. Finally, the SDLCM's operations and maintenance phase of each iteration in the incremental/iterative development model matches up with both the control and evaluate phases of capital planning.

Figure 7: Iterative/Incremental SW Development Model Integrated with DOL SDLCM and CPIC Life Cycles

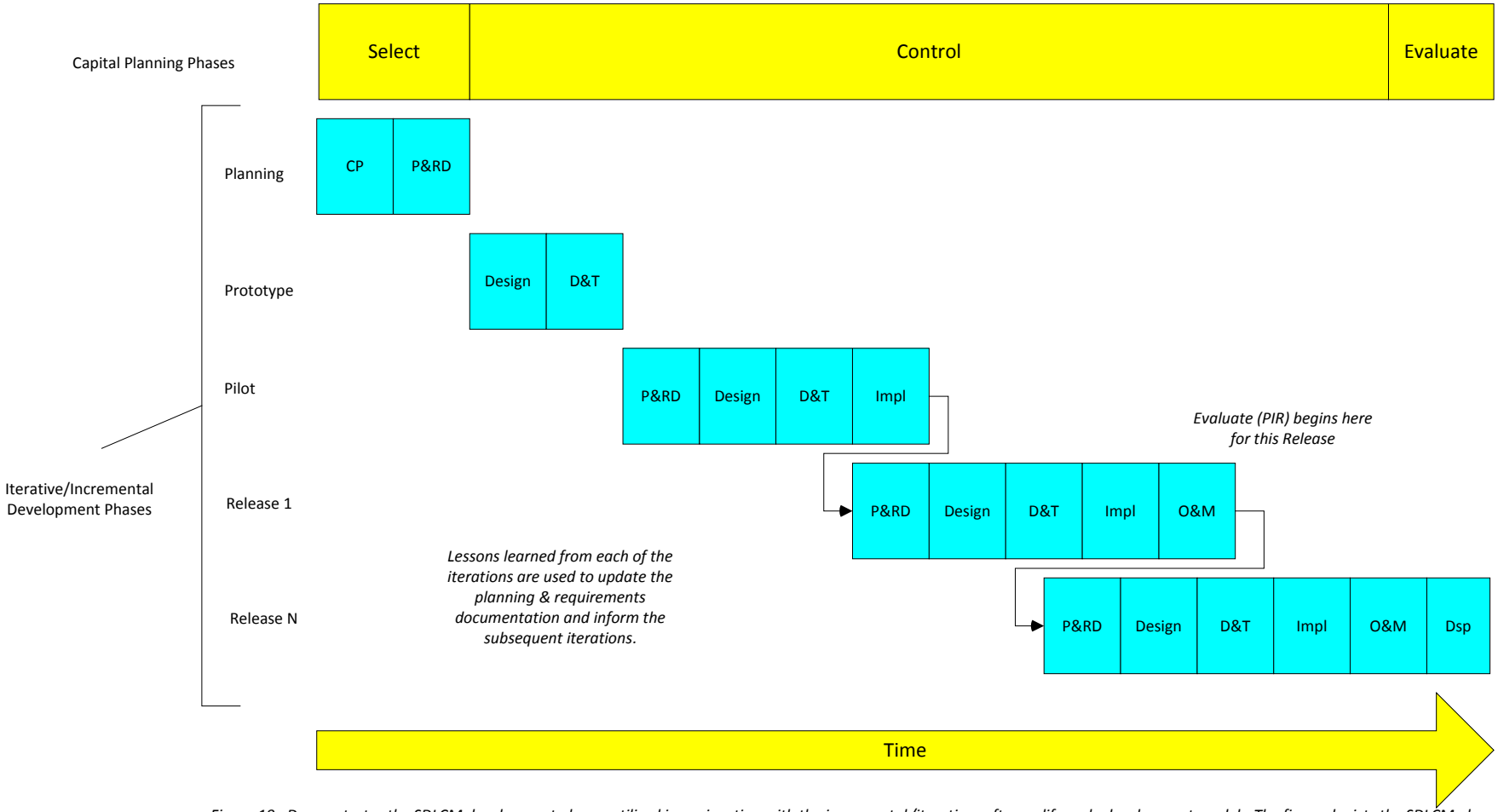


Figure 10: Demonstrates the SDLCM development phases utilized in conjunction with the incremental/iterative software life cycle development model. The figure depicts the SDLCM phases addressed during each iteration of the approach and shows how each iteration should contribute to updates of previously produ ced SDLCM deliverables produced in earlier phases (i.e. Lessons learned from the Prototype & Pilot and should be incorporated into Release 1). Capital Planning phase alignment is also demonstrated.

Key: Conceptual Planning = CP; Planning & Requirements Definition = P&RD; Design = Design; Development & Test = D&T; Implementation = Impl; Operations & Maintenance = O&M; Disposition = Dsp

Appendix E – List of Acronyms

Acronym	Definition
AA	Alternative Analysis
AP	Acquisition Plan
ASAM	Assistant Secretary for Administration and Management
BPR	Business Process Reengineering
BRM	Business Reference Architecture
C/DRP	Contingency/Disaster Recovery Plan
CBA	Cost Benefit Analysis
CCA	Clinger Cohen Act
CIO	Chief Information Officer
CO	Contracting Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COR	Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
CM	Configuration Management
CPIC	Capital Planning and Investment Control
CPC	IT Capital Planning Committee
CPM	Collaborative Planning Methodology
CSH	Computer Security Handbook
CSSPP	Cyber Security Strategic Program Plan
CSO	Computer Security Officer
CTO	Chief Technology Officer
DBC	Departmental Budget Center
DGS	Digital Government Strategy
DLMS	Department of Labor Manual Series
DP	Disposition Plan
DOL	Department of Labor
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
EIC	Enterprise Implementation Committee
ER	Enterprise Roadmap
EVM	Earned Value Management
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FITF	Field IT Forum
FISMA	Federal Information Security Management Act
FOIA/PA	Freedom of Information Act/Privacy Act
GAO	General Accountability Office
GOTS	Government-Of-The-Shelf
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act

Acronym	Definition
GSS	General Support System
HR	Human Resources
HRP	Human Resources Plan
IAD	Information Assurance Division
IDC	Integrated Data Collection
IPT	Integrated Project Team
IMLC	Investment Management Life Cycle
IRM SP	Information Resource Management Strategic Plan
IT	Information Technology
ITARB	Information Technology Acquisition Review Board
ITMRA	Information Technology Management Reform Act
ITIM	Information Technology Investment Management
ITSM	Information Technology Service Management Committee
ITSC	IT Security Committee
IV&V	Independent Verification and Validation
MA	Major Application
MOU	Memoranda of Understanding
MOU/A	Memoranda of Understanding/Agreement
NPV	Net Present Value
NIST	National Institute for Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPA	Office of Public Affairs
PBIP	Performance Budget Issue Paper
PM	Project Manager
PMA	President's Management Agenda
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
POC	Point of Contact
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
PRM	Performance Reference Architecture
QMP	Quality Management Plan
RA	Risk Assessment
RITS	Request for Information Technology Services
RMP	Risk Management Plan
ROI	Return On Investment
RR	Risk Register
SBA	Strategic Business Alignment
SBAC	Strategic Business Alignment Committee
SBM	Strategic Business Management
SDLCM	System Development Life Cycle Management

Acronym	Definition
SLA	Service Level Agreement
SOW	Statement of Work
T&IF	Technology & Innovation Forum
TA	Target Architecture
TS&SP	Transition Strategy and Sequencing Plan
WBS	Work Breakdown Structure (WBS)

Appendix F – Glossary of Terms

The following are key terms and definitions applicable to this disposition plan.

Agency - any executive department, military department, bureau, government corporation, government-controlled corporation, independent regulatory agency, or other organization in the Executive Branch of the United States Federal Government.

Alignment - conformance to a policy, standard, and/or goal.

Artifact - a documentation product, such as a text document, diagram, spreadsheet, briefing slides, or video clip.

Capital Planning and Investment Control (CPIC) - the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues. CPIC includes a management process for ongoing identification, selection, control, and evaluation of investments in IT. The CPIC process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

Change Management - the process of setting expectations and involving stakeholders in how a process or activity will be changed, so that the stakeholders have some control over the change and therefore may be more accepting of the change.

Configuration Management - the process of managing updates to business and technology resources (e.g., processes, systems, applications, and networks) to ensure that security controls are operating effectively and that standards are being followed.

Culture - the beliefs, customs, values, structure, normative rules, and material traits of a social organization. Culture is evident in many aspects of how an organization functions.

Current View - means a collection of artifacts that represent processes and technologies that currently exist in the enterprise.

Data - refers to an elementary description of things, events, activities, and transactions that are recorded, classified, and stored, but not organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds, or images. A database consists of stored data items organized for retrieval.

Enterprise - an area of common activity and goals within an organization or between several organizations, where information and other resources are exchanged.

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

Governance - a group of policies, decision-making procedures, and management processes that work together to enable the effective planning and oversight of activities and resources.

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

Information Security - involves all functions necessary to meet federal Information Security policy requirements. It includes the development, implementation and maintenance of security policies, procedures and controls across the entire information lifecycle. This includes implementation and activities associated with NIST SP-800-37, Security Awareness training, SP-800-39 regarding the implementation of a Risk Management Framework and continuous monitoring, SP-800-53A security controls, and FISMA compliance reporting, development of security policy, and security audits and testing.

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

Information Technology (IT) - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an executive agency. IT is related to the terms Capital Asset, IT Investment, Program, Project, Sub-project, Service, and System.

Information Technology Investment - the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality and the subsequent operation of those assets in a production environment. While each asset or project would have a defined life-cycle, an investment that covers a collection of assets intended to support an ongoing business mission may not.

Methodology (sometimes called “approach”) - refers to the repeatable process by which architecture documentation will be developed, archived, and used; including the selection of principles, a framework, modeling tools, artifacts, repository, reporting, and auditing.

Operations - the day-to-day management of an asset in the production environment and include activities to operate data centers, help desks, data centers, telecommunication centers, and end user support services. Operational activities for major IT investments are reported through Section C of the Exhibit 300B. Operational costs include the expenses associated with an IT asset that is in the production environment to sustain an IT asset at the current capability and performance levels including Federal and contracted labor costs; and costs for the disposal of an asset.

Operations and Maintenance (O&M) - the phase of an asset in which the asset is in operations and produces the same product or provides a repetitive service. O&M is the same as "steady state."

Program - an ongoing set of activities and projects managed in a coordinated way.

Project - a temporary activity to create a unique product, service, or result.

Records - all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included.

Records Management - the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

Risk - any factor that may potentially interfere with the successful completion of an investment.

Stakeholder - those who are or will be affected by a program, activity, or resource.

System - a tangible IT asset that is comprised of hardware devices, software applications, databases, users, processes, and security controls.

Systems Development Life Cycle (SDLC) - guidance, policies, and procedures, for developing systems throughout their life cycle, including requirements, design, implementation testing, deployment, operations, and maintenance.

Appendix G – List of References

Departmental Guidance

- Department of Labor, Systems Development Life Cycle Management (SDLCM) manual, Version 2.4, July 2014
- Department of Labor, IT Capital Planning Guide and Investment Control (CPIC) Guide: "Managing IT Projects," Version 2.1, October 2011,
- Volume 1, Introduction to the Department of Labor Computer Security Handbook, Version 4.0, August 2011.
- Department of Labor Manual Series (DLMS) 1 – Records Management; DLMS 9 - Information Technology.

Federal Guidance

- OMB Circular A-11, Part 7, Planning, Budgeting, Acquisition and Management of Capital Assets (Includes OMB Exhibit 300 information)

Legislative Guidance

- Information Technology Management Reform Act of 1996 – ITMRA (Clinger-Cohen Act)

DOL Resources

- Department of Labor, OCIO Resources Library on LaborNet – includes valuable IT project management resources, guides, and templates for over a dozen IT Governance and IT Investment Management Life Cycle Framework areas.