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

System Development Life Cycle Management (SDLCM) Manual

Version 2.4
July 2014

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

PREFACE

This document represents Version 2.4 of the Department of Labor's (DOL) System Development Life Cycle Management (SDLCM) Manual. The SDLCM Manual was last updated in May 2012. This version includes the following updates:

- The DOL Information Technology (IT) investment life cycle management framework including the Strategic Business Management (SBM) and Capital Planning and Investment Control (CPIC), IT security life cycles have been removed from this document. This document describes the SDLC management methodology, phases, deliverables, and associated supporting activities. The SBM, CPIC, and IT Security life cycles are still an integral part of DOL's IT Investment Life Cycle Management framework and DOL IT investment Project Manager's (PMs) and Integrated Project Teams are still required to complete these important life cycle management activities. (For more information, see DOL's new *IT Investment Management Life Cycle (IMLC) Guide,* v1.0, dated July 2014 for a complete and integrated view of DOL's IT investment management life cycle processes. A copy of the guide can be found in the OCIO Resource Library on LaborNet under the Investment Management topic area.)
- A figure illustrating the seven SDLCM was added to the introduction section.
- The *DOL IT Governance Model* diagram was updated to reflect the requirements associated with OMB's Digital Government Strategy published in May 2012.
- References to the three IT investment threshold levels (i.e., threshold 1, threshold 2, and threshold 3) were replaced with the terms non-Major or Major to be consistent with the OCIO CPIC Guide and OMB Circular A-11.
- References to the "Life Cycle Cost/Benefit (LCC/B) Management" process were removed from the CBA requirements due to agency and OCIO higher priorities.
- Renamed "End of phase review" language to "phase gate reviews" to align with industry standard phase/stage gate terminology. In addition, the phase gate review checklists were incorporated into an appendix, i.e., Appendix VII, for reference.
- The figures, tables, and exhibits throughout the document were relabeled accordingly to ensure clarity.
- The figures in the document were updated to ensure accessibility and compliance with Section 508 requirements.

The "Document Revision History" in Section 1.3 includes a complete list of changes that have been made to this document since its inception. This document 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 or new information that becomes known or available.

This updated version of the SDLCM Manual takes precedence over prior versions. DOL IT PMs are required to impl
ement this version going forward. DOL IT investments are required to follow the life cycle process presented in this manual as well as the *DOL IT Investment Management Life Cycle (IMLC) Guide*.

If you have any questions, please contact the OCIO, Room N1301, 200 Constitution Avenue, NW, Washington, DC 20210 or via email at OCIO@dol.gov.

EXECUTIVE SUMMARY

The United States Department of Labor (DOL) invests hundreds of millions of dollars annually on information technology (IT) systems. These IT systems are vital to day-to-day operations of the Department as well as to the overall success of the Department's mission programs and in achieving the Secretary's vision. DOL relies on IT systems and advances in technology to ensure a safe, secure, and a dependable method to provide its mission program services, develop products, administer daily activities, and perform short- and long-term management functions. DOL must continue to ensure data privacy and security when developing and implementing information systems as well as establish uniform privacy and protection practices.

To efficiently and effectively develop, implement, operation and manage the Department's IT investments, DOL developed this standardized System Development Life Cycle Management (SDLCM) Manual. This manual serves as the life cycle mechanism to assure developing, modifying, and/or enhancing DOL systems fulfill identified business needs, established customer requirements, and supports DOLs business mission and critical success factors. It sets forth a standard and logical methodology and associated life cycle processes for managing IT system development activities and approvals that are controlled, measured, documented, and ultimately improved. At the same time, this manual responds to the following current legislation mandating the use of industry standards in the development and management of IT systems:

- 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)

This DOL SDLCM manual is a key component of DOL's *IT Investment Management Life Cycle (IMLC) Guide*, which describes the IT investment life cycle phases and how they are interrelated with the Strategic Business Management, Capital Planning and Investment Control (CPIC), and IT Security life cycles. Each of these IT life cycles need to be managed in a coordinated fashion to ensure the successful planning, implementation, and ongoing operations and maintenance of IT systems at DOL. Other related and important IT management functional areas include, but are not limited to, software management, information management, quality management, performance management, records management, and Section 508 accessibility management. Each of these IT management areas is described in greater detail in the DOL IMLC Guide. The Department's IMLC represents a comprehensive integrated approach to IT investment management. A copy of the guide can be found in the OCIO Resource Library on LaborNet under the Investment Management topic area.

This SDLCM manual represents many years of systems development and engineering experience by information systems professionals, including the incorporation of lessons learned from prior implementation versions. The purpose of this manual is to disseminate standardized and proven practices for use throughout DOL. The specific benefits expected include the following:

- Increased likelihood of system planning, development, implementation, and operational success
- Reduced risk of IT system investment failure
- Greater IT system monitoring and control integrity, openness, awareness, and management performance accountability
- Promotes greater communications between IT system business owners and the technical Integrated Project Team (IPT) throughout the entire life of the system
- Supports enhanced critical business management and IT system management decision making capability
- Promotes the early identification and resolution of technical and management issues including avoiding investing in features or functions not benefiting end users or the business owners/stakeholders
- Formalizes the IT system planning, acquisition, development, implementation, operation & maintenance, and the decommissioning processes including the associated incremental management approval process for each milestone and phase
- Is consistent with industry standards in the life cycle management of IT systems
- Supports disclosure of all life cycle costs to guide business management decision-making
- Fosters realistic expectations of what the system will and will not provide, through active user involvement
- Provides information enabling consideration of all aspects -- programmatic, technical, management, and cost -- of a proposed system development or modification effort
- Provides periodic IT system evaluations to identify systems needing enhancements or are no longer effective and need to be replaced
- Measurements of progress and status to enable effective corrective action before proceeding to the next phase
- Essential information that supports effective resource management and budget planning.

The Department’s SDLCM divides an IT system's life cycle into seven phases starting with Conceptual Planning and ending with the Disposition Phase. It describes the inputs, activities and deliverables associated with each phase. Further, it presents guidance on how the approach can be tailored to suit the various types of systems development and maintenance projects that exist within DOL today.

The use of the SDLCM manual applies to all DOL and contractor personnel who are developing, acquiring (i.e. Commercial Off-The-Shelf (COTS)), or managing new systems, including making modifications or enhancements to existing systems. Adherence to the SDLCM by program officials, PMs, IPTs, integrators, system developers, employees, and contractors performing systems work for the Department is crucial to delivering cost effective information systems. DOL Agencies are responsible for ensuring that the SDLCM methodology and practices described in this SDLCM are implemented accordingly throughout the life cycle of an IT investment. The Chief Information Officer/Office of the Chief Information Officer (CIO/OCIO) is the authority for this SDLCM manual.

On September 27, 2004, the DOL Office of the Assistant Secretary for Administration and Management (OASAM) issued a memorandum titled “Guidance for the DOL Earned Value Management System (EVMS) Methodology” which established the requirements and timeline for submission of earned value data by specific IT investments within the Department of Labor (DOL), pursuant to directives from the Office of Management and Budget (OMB) and applicable legislation. As a result of this memorandum, Earned Value Management (EVM) has become a mandatory requirement for major DOL IT investments. As such, EVM information and guidance is contained within this SDLCM manual to assist and support IT PM's in understanding the EVM requirements in the context of the SDLCM. A more detailed explanation of EVM and of the DOL EVM requirements can be found in the DOL EVM Operational Guide which can be found in the DOL OCIO Resource Library on LaborNet under the CPIC subject area. In addition, the DOL OCIO has prepared an EVM Quick Reference Guide which can also be found on LaborNet under the CPIC subject area.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EXHIBITS

1 INTRODUCTION

1.1 Purpose

This manual describes the U.S. Department of Labor's (DOL's) System Development Life Cycle Management (SDLCM) methodology including the procedures, practices, and guidelines for engineering and managing DOL IT investments (e.g., an IT project, system, application, service, program, or initiative) through the seven SDLCM life cycle phases. As illustrated in Figure 1, the seven DOL SDLCM phases include the Conceptual Planning, Requirements Definition, Design, Development & Test, Implementation, Operations & Maintenance, and Disposition phase.

This SDLCM Manual has been created to assist and support DOL Agencies in successfully managing their IT investments throughout the entire life cycle of the investment. This manual applies to all new or existing IT investments including, for example, IT hardware and/or software solutions, software development systems, COTS/GOTS software deployments, existing system development, modernization, and/or enhancement and integration activities, interface development activities, infrastructure changes or enhancements, as well as new IT services, and/or projects. This SDLCM manual sets forth a proven, standard, repeatable, reliable, flexible, and adaptable life cycle management methodology applicable to all DOL IT investments. When followed and implemented correctly by IT PMs and IPTs the life cycle methodology will lead to sound and consistent IT investment management practices across the Department and result in higher quality and successfully managed IT investments – delivered on budget, schedule, and with promised functionality.

The SDLCM concepts presented in this manual are a part of DOL's IT life cycle management framework to improve the quality of Departmental IT investments. See the *DOL IT Investment Management Life Cycle (IMLC) Guide* for more details on the complete and integrated life cycle management framework. A copy of the guide can be found in the OCIO Resource Library on LaborNet under the Investment Management topic area.

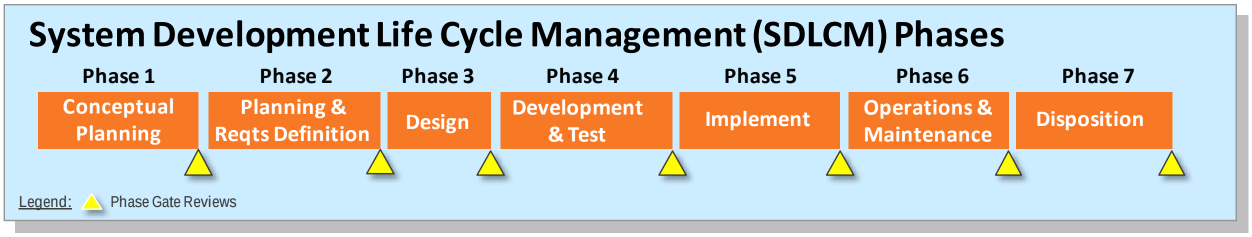

Figure 1: DOL's Seven SDLCM Phases

1.2 Document Overview

This chapter provides an overview of the general concepts that are relevant to the SDLCM, including project management roles and responsibilities, and quality assurance. Subsequent chapters present details regarding the Department's seven defined phases of the SDLCM.

Finally, the appendices provide additional information on several of the areas highlighted in the main document as well as detailed descriptions and templates for the SDLCM deliverables. Appendix II, in particular, contains hyperlinks and relevant references for Departmental, Federal and legislative guidance that relates to and/or impacts SDLCM activities.

1.3 Document Revision History

The following table describes the revision history of this document including the version number, the version date, the person who made the modification(s), and a description of the changes.

Version No.	Version Date	Modified By	Description of Changes
1.0	01/2000		• Initial draft developed
2.0	06/2000		•
2.1	12/2002	DOL OCIO	Administrative update including the following changes: • Addition of Frequently Asked Questions (FAQs) • Addition of a business process, integrating the SDLCM with Capital Planning, Security and Privacy, and other functional areas under CIO oversight • Update of security requirements • Addition of enterprise architecture material • Addition of quality assurance material • Addition of information quality material • Addition of software life cycle models • Addition of a Waiver/Exception process • Legislative update for the E-Government Act of 2002, Public Law 107-347
2.2	08/2006	DOL OCIO	• Replaced/updated I-TIPS references and information with eCPIC information throughout the entire document since I-TIPS is no longer used by the Department. • Added section “1.14 Document Revision History”. • Updated the FAQ section to clarify answers to previous questions and to add several new questions and answers. • Combined the Figure 3 and 4 Large and Medium System Work Patterns • Updated the deliverables in the Large/Medium and small work patterns (and the associated text in Chapters 2 through 8 supporting these Figures), • Eliminated the threshold 3i investment category in Section 1.4.1 and removed Figure 5 the Maintenance and Enhancement Effort Work Pattern • Updated the threshold 1, 2, and 3 descriptions to be consistent with the OCIO Capital Planning Guide and increased the minimum annual investment cost from $100K to $250K for threshold 1 and 2 investments. Also, added the text “with annual investment costs of $500K or above” to the financial management system bullet in the threshold 3 section

			and language clarifying whether the threshold level was considered an Major or Non-Major investment as defined by Circular A-11. • Deleted References to OMB Director's Policy Memorandum M-97-02 (Raines Rules) • Replaced the word "project" with "investment" accept when referencing the Project Manager or Project Management Plan (PMP). • Updated Figure 1 the DOL IT Investment Management Framework • Deleted References to the following six deliverables: ➢ Data Sensitivity Assessment ➢ Acceptance Test Approval ➢ Delivered System ➢ System Fielding Authorization ➢ Trained Personnel ➢ Implemented System • Added six new deliverables including a description of each in Figure 7 ➢ Investment Target Architecture ➢ Investment Transition Strategy ➢ FIPS 199 System Categorization ➢ Contingency Plan Test Report ➢ Security Controls Testing/ Continuous Monitoring ➢ Re-certification and Accreditation • The following changes were made to the list of existing deliverables in the Figure 3 work pattern: ➢ "Security "Security Test & Evaluation" was changed to "Security Control Assessment Aid (SCAA) / Security Test & Evaluation (ST&E)" ➢ "Acceptance Test Report" was combined with "Acceptance Test Approval" to form "Acceptance Test Report and Approval" ➢ "Implementation Certification Statement" was changed to "System Acceptance Letter" ➢ "Archived System" is now integrated into the "Disposition Plan" ➢ Updates to the CBA are now indicated for Phase 4 and 5, and 6. Updates in Phase 6 are driven by the results of the Operational Analysis (OA). ➢ The PMP and RMP are required to be updated in Phase 6 ➢ The WBS is a core requirement in Phase 1 and is updated for each of the remaining phases. ➢ The Acquisition Plan is a core requirement in Phase 2 ➢ Deleted Implemented System, Acceptance Test Approval, Delivered System, System Fielding Authorization, and Trained Personnel ➢ A Records Management Plan has been

			added to the Project Management Plan (PMP) – a description of what is expected by implementing a Records Management is also described in the document. • Deleted Section 1.8 entitled "Certificate Based Services" which described the Departments intention to create a PKI certificate based service since the Department is no longer pursuing this service. • Added text throughout the document describing EVM and Operational Analysis requirements including for example an FAQ question/answer and Section 1.12 Performance Management • Added text to Section 2.1, Step 1 indicating an Agency should use its EA to identify the need for new or modified IT investments as well as consolidation, business optimization, and collaboration opportunities. • Replaced text in Section 2.1, Step 2, in the EA section of the table that states "the Departments enterprise target architecture and standards" with "the Departments enterprise architecture and IT standards." • Added a "Note" to Figure 5 in Section 1.9 to the definition of the Investment Target Architecture and Investment Transition Strategy to clarify that these EA deliverables are required to be incorporated into the Agency Target Architecture and Transition Strategy, respectively. Otherwise, an IT Investment PM may choose to create and maintain an IT Investment Target Architecture and Transition Strategy document that is separate from the Agency Target Architecture document. • The Cost Benefit Analysis (CBA) outline in Appendix V has been updated and well as the CBA text in Chapter 2 and 3. • A description of the OCIO Cost Model has been incorporated in the CBA sections. • The Project Management Plan (PMP) text has been updated to clarify the WBS and several other existing requirements. • The Risk Management sections have been updated to reflect the new OCIO Risk Management Plan template and associated Risk Register (RR). • The References section has been updated including the URLs. • The Acronyms List has been updated to reflect current acronyms
2.3	05/2012	DOL OCIO	• An updated description of the OCIO Cost Model has been incorporated in the CBA sections. • The Risk Management sections have been updated to reflect the latest updates to the OCIO Risk Management Plan template and associated Risk Register. • A description of the end of phase review process was

			added to the document. • A description of the Performance Measurement Baseline (PMB) and the Integrated Baseline Review (IBR) was added to document. • A description of Release Management and the associated Release Management process that is to be implemented by IT investments was added to the document. • A description of the relationship between the SDLCM and the PMBOK Guide was added to the Q&A section of this document. • A description of how the Federal Acquisition Certification for Program and Project Managers (FAC P/PM) requirements relate to the SDLCM was added to the Q&A section of this document. • A description of how the Cyber Security Assessment and Management (CSAM) Internet-based tool relates to the SDLCM was added to the Security section of this document. • A description of the Initial Investment Post Implementation Review (PIR) was added as an activity in the beginning of Phase 6. • A description of the Independent Verification and Validation (IV&V) activities that will need to be performed by an IT investment has been added to the Quality Assurance (QA) section of the document. • References have been incorporated in applicable sections throughout the manual to the following OCIO templates: CBA template, Acquisition Plan template, Project Charter, IT Rebaseline Guide, Initial Investment PIR template, EVM Operational Guide, and the EVM Quick Reference Guide. • The word “initiative” was replaced with the words “IT investment” throughout the document to be consistent with Office of Management and Budget (OMB) A-11, Part 7 terminology. • References to the OCIO FAQ website on LaborNet have been removed. • The URLs throughout the document have been tested, updated or removed as necessary, and/or verified as being active. • The Acronyms List has been updated to reflect current acronyms. • The IT Investment Management Framework diagram in Figure 1 was updated to reflect changes (i.e., SDLCM end of phase reviews, CPIC Control phase starting during the SDLCM phase 2, EA shift to Strategic Business Management and the associated phases being updates, and updates to the Security life cycle phases. • The DOL IT Governance Model was updated to reflect the changes made and announced by the DOL Assistant Secretary for Administration and Management in the memo dated July 26, 2011. • Deleted Appendix I – Enterprise Architecture as the

			information was duplicative and dated • Deleted Appendix II – Security Roles, Activities, and Deliverables as the information is duplicative to the DOL Computer Security Handbook.
2.3.1	09/2013	DOL OCIO	• The DOL IT Governance Model was updated to comply with the requirements of the OMB Digital Government Strategy published in May 2012. • Relabeled the Figures, Tables, and Exhibits accordingly. • Added alternative text to each of the figures to make them Section 508 compliant.
2.4	01/2014	DOL OCIO	• See the "Preface" for a summary of changes made to this document.

1.4 Frequently Asked Questions (FAQ) about the SDLCM

What is the SDLCM Manual?

This 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. This 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.). This manual provides a proven, structured, and standardized life cycle management approach to all DOL IT investments.

Why do I have to use the SDLCM methodology?

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 presented in this manual 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.

When do I use the SDLCM?

Agency PMs and IPTs will need to follow the SDLCM for applicable IT investments throughout the entire life cycle of the investment from conceptual planning to disposition. The SDLCM should be utilized as a reference and guide throughout the life cycle of an IT investment. The SDLCM should be used in conjunction with other existing DOL IT investment management framework processes including the Capital Planning and Investment Control (CPIC), Security, and Strategic Business Management (SBM) life cycle processes. (See the DOL IT Investment Management Life Cycle (IMLC) Guide for further details on DOL's integrated IT investment management life cycle processes. A copy of the guide can be found in the OCIO Resource Library on LaborNet under the Investment Management topic area.)

What is a work pattern and how do I know which one to use?

A "work pattern" refers to the activities performed and products or deliverables produced as part of the life cycle phases associated with the development and life cycle of a system. There are two work patterns associated with this SDLCM Manual: one for major IT investments and one for non-major IT investments. See the DOL CPIC Guide for information on determining whether a system is considered a major or non-major IT investment. PMs will need to work with the OCIO CPIC team during the early conceptual planning phase to determine whether a system is consider major or non-major and ensure the determination is clearly identified and included within the IT investment Project Charter document. In general, the more costly, technically complex, or risky an IT investment is, the more likely it's considered a major system and as such will require completing the major system work pattern. All major systems are required to follow the major work pattern. Please refer to the major and non-major work patterns in Section 1.6 of this manual for a list of required deliverables to be completed, for each pattern, throughout the system's life cycle. DOL PMs and/or IPTs are highly encouraged to work with the OCIO CPIC team in determining the correct work pattern for an IT investment as soon as possible during the early conceptual planning phase. Ideally, PMs and/or IPT members should seek OCIO CPIC team review and approval of the correct work pattern prior to signature approval of the Project Charter. For more information on the DOL CPIC process, see the latest DOL Capital Planning and Investment Control (CPIC) Guide. A copy of the CPIC Guide can be found in the OCIO Resource Library on the DOL LaborNet under the CPIC topic area.

How do I know what the security requirements for my system will be?

Security requirements should be discussed with Departmental security staff during the beginning of the conceptual planning phase. Sponsoring Agency security authorities should, if possible, review the requirements referenced in the Computer Security Handbook prior to these discussions. While this SDLCM describes security requirements in each phase of the life cycle, there are numerous other regulations and guidelines that drive security requirements into the SDLCM. Thus, Project Managers (PMs) and Integrated Project Team (IPT) members are encourage to review the DOL OCIO Computer Security Handbook (CSH) for all the Department-wide IT security policies, procedures, standards, requirements, and templates. A copy of the DOL CSH can be found in the OCIO Resource Library on LaborNet under the Security subject area.

Where do I go to get help when I have questions?

The OCIO IT capital planning and system development personnel are the primary resources for providing SDLCM assistance. If you have questions about the SDLCM, please contact Peter Sullivan in the OCIO at 202-693-4211 or sullivan-peter@dol.gov. Additional SDLCM information can be found in the OCIO Resource Library on the DOL LaborNet under the System Development Life Cycle Management (SDLCM) topic area.

What if the DOL SDLCM process does not suit the needs of my IT investment?

PMs and IPTs are required to follow the SDLCM for applicable IT investments throughout the entire life cycle of the investment from conceptual planning to disposition. The OCIO requires any deviations or exceptions to implementing and/or utilizing this standard SDLCM methodology to be justified and submitted in writing and approved by OCIO leadership prior to the initiation or funding of an IT investment. Exception requests will be handled on a case-by-case basis, taking into consideration the complexity of the investment and the applicability/reason for the specific request. Please refer to the Waiver/Exception Process section of this manual, and direct exception requests to the OCIO's IT Governance staff. In addition, please refer to Appendix I for more information on Software Life Cycle Models.

What if my IT investment is considered Software Development or an Application?

This 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. This 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 I for more information on various Software Life Cycle Models that may be implemented. Figure 11 in the appendix illustrates, as an example, an iterative/incremental software development approach implemented utilizing the SDLCM life cycle phases.

This 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.

How does the SDLCM relate to other OCIO requirements for IT investments?

The SDLCM is one component of DOL's IT Investment Management Framework. This Framework is described as the activities necessary to ensure that an IT investment progresses toward the achievement of its objectives in accordance with planned or revised cost, schedule and technical baselines, as well as performance outcomes. The other components of the framework include the Capital Planning and Investment Control (CPIC) process, the Security Life Cycle phases, and the Strategic Business Management life cycle phases. Other related functional areas within the OCIO include Information Quality, Quality Assurance, Performance Measurement, E-Government and Records Management. All of these components must work together in an integrated manner to ensure compliance with statutory and regulatory requirements and to lead to successful investment outcomes. In formulating a lifecycle development process, it is essential that requirements documentation, work efforts and system specifications reflect the Department's guidance on these topics. Reference materials on these topics are listed in the appendices.

How does the SDLCM manual relate to Office of Management and Budget (OMB) requirements for IT investments?

The DOL SDLCM manual is a DOL IT Investment life cycle management process that is implemented by Project Managers and/or Program Managers and associated Integrated Project Teams (IPTs). DOL IT investments (e.g., an IT projects, systems, or services,) are implemented in accordance and compliance with DOL policies, orders, memorandum, procedures, standards, and guidelines, as well as in accordance and compliance with applicable Federal laws, legislation, policies, standards, regulations, rules, procedures and processes. This includes OMB requirements as documented in OMB circulars, memorandum, guidance, and presidential directives and orders. As such, DOL Project Managers, Program Managers, and IPTs are expected to manage, implement, and/or operate and maintain IT investments using the SDLCM manual processes to achieve Department, Agency, as well as OMB goals and objectives as is applicable to the specific IT investment. Project Manager, Program Managers, and IPT members are encouraged to monitor, review, implement, and/or abide by OMB circulars, memorandum, directives, and guidance as applicable to DOL IT investments in order to achieve

OMB goals including, for example, but not limited to, Transparency and Open Government, IT Cloud-Computing, Shared Services, Consolidation, Virtualization, Standardization, and other Federal IT modernization and cost cutting initiatives. DOL agencies are encouraged to contact and work with the DOL OCIO Capital Planning and Investment Control (CPIC) group to understand OMBs requirements and how to plan and implement OMBs requirements.

How does DOL's and OMB's Baseline Management policy requirements for IT investments relate to the DOL SDLCM manual?

On September 9, 2010, the DOL OCIO CPIC Program Office published DOL specific Baseline Management policy in accordance and compliance with OMB Memorandum M-10-27, "Information Technology Investment Baseline Management Policy," issued to Federal Agencies on June 28, 2010. In addition, the OCIO Program Office created the "IT Baseline Management Guide" to assist and support DOL agencies, IT Project Manager, Program Managers, and IPT member in understanding DOL's IT baseline management policy, processes and requirements.

In order to comply with DOL and OMB Baseline Management policy, DOL Agency IT Project Managers, Program Managers, and IPT members are required to establish, manage, and report on (OCIO approved) IT investment baselines for all new and current IT investments to ensure that the investments meet their specified cost, schedule and performance goals and achieve intended results. In order to achieve IT investment baseline approval from the OCIO, Agency IT Project Managers, Program Managers, and IPT members will need to complete and acquire OCIO approval of fundamental SDLCM deliverables described in this manual including for example, the Project Charter, Cost Benefit Analysis (CBA), Project Management Plan (PMP), Work Breakdown Structure (WBS), Functional Requirements document, etc. Thus, this SDCLM manual and the DOL IT Baseline Management Guide are critical resources to help Agencies be successful and comply with DOL's IT baseline management policy and the associated Federal laws and OMB requirements. A copy of the DOL IT Baseline Management Guide can be found in the OCIO Resource Library on the DOL LaborNet under the Baseline Management topic area.

For further information about the Guide or DOL's baseline management policy or processes, please contact the DOL OCIO via email at OCIOCapitalPlanning@dol.gov.

How does the Project Management Body of Knowledge (PMBOK) Guide relate to the SDLCM?

The PMBOK Guide is an internationally recognized project management methodology established by the Project Management Institute (PMI). The PMBOK Guide is an important reference document 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. The SDLCM, on the other hand, is a specialized and proven information technology life cycle management methodology. It is flexible, adaptable, and scalable methodology, which has been successfully implemented and utilized to plan, develop, test, integrate, deploy, operate, and manage a wide variety of IT investments (i.e., applications, systems, services, programs, initiatives) at DOL; and similar SDLC methodologies have been successfully used throughout the Federal Government and in private industry for decades.

Since the SDLCM is IT focused, DOL IT investments are managed using the SDLCM methodology as represented in this document. DOL IT PMs and IPTs are highly encourage to apply PMBOK principles, processes, and practices as applicable, while implementing and executing the life cycle phases in this SDLCM Manual. One of the benefits of the good practices established by the PMBOK principles and processes is that they can be applied at various levels and to various degrees throughout the SDLCM methodology. For example, work activities and individual SDLCM deliverables within each of the phases of the SDLCM can be managed using PMBOK principles and processes. In addition, each of the seven phases of the SDLCM can also be managed using the PMBOK principles, processes, and practices.

An IT investment may have one or more vendors and/or contractor teams including for instance an IV&V team supporting the investment. Each of these entities should manage their individual contracts and associated tasks as independent projects using PMBOK principles. Thus, the DOL OCIO encourages all IT investment PMs and IPTs to apply PMBOK principles and processes, as applicable and appropriate, to ensure the success of individual IT investment tasks and deliverables as well as individual phases and the IT investment as a whole.

The PMBOK Guide should be used as a reference to support IT Investment PMs/IPTs in implementing and executing the SDLCM methodology. In the unlikely event that the SDLCM and PMBOK principles and practices should conflict or if there is a perception of conflict, then the principles and practices described in this DOL specific manual outweigh the general practices in the PMBOK Guide. This version of the SDLCM continues to include/adopt PMBOK Guide terminology were applicable and appropriate and as long as it does not conflict with standard SDCLM terminology.

How does the Federal Acquisition Certification for Program and Project Managers (FAC P/PM) requirements relate to the SDLCM?

DOL Program and Project Managers of Major IT investments must be certified at the FAC-P/PM Level 3 – Senior/Expert level. This requirement will ensure that DOL Program and Project Managers (P/PMs) are experienced in managing IT investments, including managing them through the SDLCM phases. To maintain FAC-P/PM Level 3 certification, P/PMs are required to earn 80 continuous learning points (CLPs) every two years. Thus, P/PMs will need to review and follow DOL FAC-P/PM Program and policy requirements in order to be certified and maintain compliance going forward.

The FAC P/PM requirements were established on April 25, 2007 when OMB issued a Memorandum for Chief Acquisition Officers entitled "The Federal Acquisition Certification for Program and Project Managers (FAC P/PM)". The FAC P/PM requirements were based on the recommendations from a Federal Acquisition Institute working group.

As a result of OMBs memo, the DOL established a FAC-P/PM Program within the Department and published DOL specific FAC-P/PM policy. In accordance with the OMB memo, the DOL FAC-P/PM Program and requirements represent general training and experience requirements *for certifying DOL program and project managers. As stated in DOL's FAC-P/PM policy document, the DOL FAC-P/PM Program and requirements focus on defining and establishing essential competencies needed for program and project managers. The DOL FAC-P/PM requirements describe three levels of certification based on the number of years of experience. The three levels include:*

1. *Entry or Apprentice level – This level requires at least one year of on the job training defining and assisting a program/project manager. A baccalaureate degree in Engineering, Systems Management, or Business Admin is desirable at this level.*

2. *Mid-level/Journeyman level – This level requires at least two years of on the job training. A Masters degree in Engineering, Systems Management, or Business Admin is desirable at this level.*

3. *Senior or Expert level – This level requires at least four years of on the job training - Manage and Evaluate. Senior/Expert-Level FAC-P/PM required for all investments defined as "Major Investments" by OMB. A Masters degree in Engineering, Systems Management, or Business Admin is desirable at this level.*

No additional information regarding the DOL FAC-P/PM Program is included in this SDLCM manual. For additional information, please see the Department of Labor's Federal Acquisition Certification in Project/Program Management (FAC-P/PM) Program policy document.

What is Earned Value Management (EVM) and do I have to implement it for my IT investment?

EVM is a Department of Labor and OMB mandated IT investment performance based management process that integrates cost, schedule, and technical performance, to provide decision makers timely and accurate information on the overall performance or health of an IT investment. The EVM process measures the cost and schedule performance of an IT investment by comparing planned, budgeted, and scheduled work activities (which are laid-out in a time-phased manner) against actual work accomplished. As work is accomplished on an IT investment, IT investment value is "earned." The EVM process is also used as a predictive tool that, when used effectively, can highlight investment risks, identify opportunities to manage or control the performance of the IT investment, and estimate the future (near-term) cost and schedule performance of the investment.

EVM is applicable to Major IT investments and Mixed Lifecycle investments when the annual cost of Development, Modernization, and Enhancement (DME) exceeds $1,000,000. These exemptions are not applicable to an investment that warrants special attention because of other factors as delineated in OMB Circular A-11, such as significant importance to an agency's mission, high management visibility, or high risk.

IT investments that are required to perform EVM are required to develop a Performance Measurement Baseline (PMB), which is an integrated scope-schedule-cost plan for the work that *will be performed. It will be used to measure and manage the actual work performed, i.e., to measure work performance. The PMB will need to be approved as part of the Integrated Baseline Review (IBR), which is a meeting typically performed shortly after the IT investment vendor/integrator contract is awarded. The PMB includes the vendor/integrator activities as well as the federal PM and Project Management Office (PMO) personnel and activities including for example CPIC, Security, EA, and any IV&V activities. Once the PMB is approved, it becomes the integrated scope-schedule-cost plan for the work that will be performed. It will be used to measure and manage the actual work performed, i.e., to measure work performance.*

See Section 1.11 of this document for more information regarding the PMB and the IBR.

IT investments in the Operational and Maintenance (O&M) or "steady state" phase are not required by OMB to perform EVM. These investments will conduct an Operational Analysis on an annual basis to determine how they are performing relative to operational cost, schedule, and performance goals.

For more information on EVM and the DOL Earned Value Management System (EVMS) please see the DOL EVM Operational Guide which can be found in the DOL OCIO Resource Library on LaborNet under the CPIC EVM subject area . The DOL OCIO has also developed a handy EVM Quick Reference Guide to assist and support DOL IT Investment PM and IPTs in understanding and implementing EVM activities. The DOL EVM Quick Reference Guide can also be found in the DOL OCIO Resource Library on LaborNet under the CPIC EVM subject area.

Where can I find more information about the DOL's IT Investment Management Framework, specifically, the Capital Planning and Investment Control (CPIC) process, the Security life cycle phases, and the Strategic Business Management (SBM) phases.

A description of the DOL IT Investment Management Framework can be found in the DOL IT Investment Management Life Cycle (IMLC) Guide. This guide can be found in the OCIO Resource Library on the DOL LaborNet under the Investment Management topic area.

A detailed description of the DOL Capital Planning and Investment Control (CPIC) process can be found in the DOL Capital Planning and Investment Control (CPIC) Guide, which can be found in the OCIO Resource Library on the DOL LaborNet under the Capital Planning and Investment Control (CPIC) topic area.

A detailed description of the DOL IT Security Life Cycle phases can be found in the DOL Computer Security Handbook, which can be found in the OCIO Resource Library on the DOL LaborNet under the Security topic area.

A description of the DOL Strategic Business Management phases can be found in the DOL IT Investment Management Life Cycle (IMLC) Guide. SBM related resources can be found in the OCIO Resource Library on the DOL LaborNet under the SBM topic area.

1.5 IT System Roles and Responsibilities

1.5.1 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.

1.5.2 IT System Owner

The System Owner is located within the DOL organization benefiting from or requesting the work on an IT investment and is frequently thought of as the “customer” for that investment. The 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.

1.5.3 Users

Active 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.

1.5.4 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.

1.5.5 IT Investment Governance Structure

As part of the DOL IT investment management process, DOL has established an IT investment governance structure for senior DOL management to have over see, coordinate, and/or guide the Department's implementation and modernization of information technology investments. In 2013, as required by the OMB Digital Government Strategy (DGS), DOL updated its IT governance structure, which is shown in Figure 2, on the next page, to accommodate the DGS requirements.

All of the entities and the associated governance activities are coordinated and/or guided by the Deputy Secretary of Labor, and the Chief Information Officer. The IT governance structure allows for more aggressive decision-making and greater alignment between the Department's planning activities, operations, and strategic business, mission and goals — thus ensuring IT is used strategically to enhance and modernize the Department. Additionally, the CIO is directly integrated into the Department's budget formulation and execution processes to make sure information technology priorities and equities are represented.

Furthermore, the OCIO is working 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.

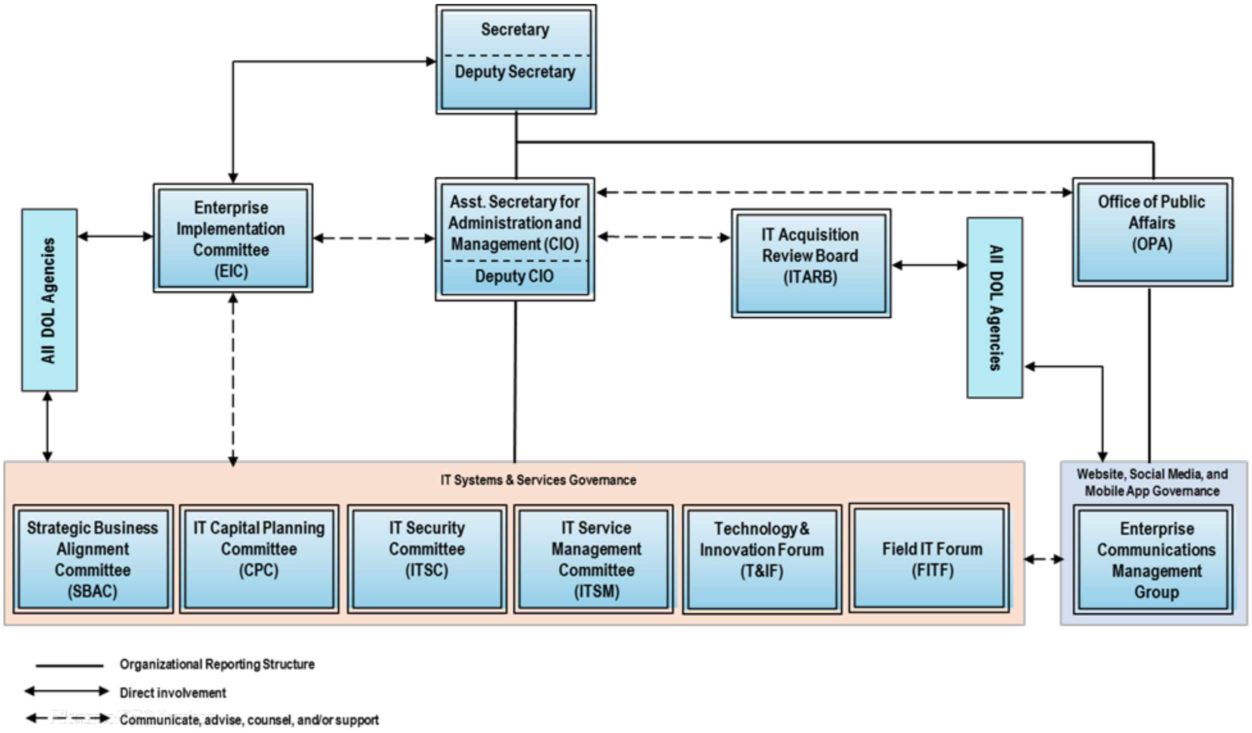
Secretary
Deputy Secretary
Enterprise Implementation Committee (EIC)
Asst. Secretary for Administration and Management (CIO)
Deputy CIO
IT Acquisition Review Board (ITARB)
Office of Public Affairs (OPA)
All DOL Agencies
All DOL Agencies
IT Systems & Services Governance
Strategic Business Alignment Committee (SBAC)
IT Capital Planning Committee (CPC)
IT Security Committee (ITSC)
IT Service Management Committee (ITSM)
Technology & Innovation Forum (T&IF)
Field IT Forum (FITF)
Website, Social Media, and Mobile App Governance
Enterprise Communications Management Group
Organizational Reporting Structure
Direct involvement
Communicate, advise, counsel, and/or support

Figure 2: DOL's IT Governance Structure (as of May 15, 2013)

Each of the entities, shown in Figure 2, is described in greater detail in the following subsections.

1.5.5.1 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.

1.5.5.2 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.

1.5.5.3 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.

1.5.5.4 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.

1.5.5.5 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

1.5.5.6 IT Capital Planning Committee (CPC)

The focus of the IT Capital Planning Committee is to:

- Understand IT drivers and requirements
- Ensure complianc
- e 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

1.5.5.7 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

1.5.5.8 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

1.5.5.9 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

1.5.5.10 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.

1.5.5.11 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.

1.5.6 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 Paperwork Reduction Act (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 Clinger-Cohen 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.

1.6 SDLCM Work Patterns and Associated Deliverables

An important objective of the SDLCM is to provide flexibility that allows tailoring to suit the characteristics of a particular IT system being developed, implemented, and/or maintained. One methodology does not necessarily fit all sizes and/or types of system development and/or enhancement efforts. This section describes the work patterns (i.e., activities and deliverables) required for a system that is categorized as either a major IT investment or a non-major IT investment. See the DOL CPIC Guide for information on determining whether a system is considered a major or non-major IT investment. DOL PMs and/or IPTs are highly encouraged to work with the OCIO CPIC team in determining the correct work pattern for an IT investment as soon as possible during the early conceptual planning phase. Ideally, PMs and/or IPT members should seek OCIO CPIC team review and approval of the correct work pattern prior to signature approval of the Project Charter. For more information on the DOL CPIC process, see the latest DOL Capital Planning and Investment Control (CPIC) Guide. A copy of the CPIC Guide can be found in the OCIO Resource Library on the DOL LaborNet under the CPIC topic area.

It is important to note that the IT investment documentation developed in accordance with this SDLCM should be commensurate with the size (i.e., funding level), scope, and/or complexity of the IT investment.

Major IT Investment Work Pattern

The major IT investment work pattern is shown in Table 1 on the next page.

The table shows the core (C), optional (O) and updated (U) deliverables for each life cycle phase. See section 1.7 for a detailed explanation of each deliverable in this work pattern.

Table 1: Major IT Investment Work Pattern

		SDLCM Phase						
SDLCM Deliverables	**Type**	**Phase 1**	**Phase 2**	**Phase 3**	**Phase 4**	**Phase 5**	**Phase 6**	**Phase 7**
Project Charter	PM	C						
Cost Benefit Analysis (CBA) [1]	PM	C	U	→	→	U	2	
Project Management Plan (PMP)	PM	C	U	→	→	→	U	
Work Breakdown Structure (WBS)	PM	C	U	→	→	→	→	U
Risk Management Plan and Risk Register	PM	C	U	→	→	→	U	
Investment Target Architecture	PM	C	U	→	→	→	→	U
Investment Transition Strategy & Sequencing Plan (TS&SP)	PM	C	U	→	→	→	→	U
FIPS 199 System Categorization Report	Sec	C	U	→	→	→	→	U
Privacy Impact Assessment	Sec	C	U	→	→	→	→	U
Acquisition Plan	PM	O	C	U	→	U		
SOW	Acq	O	O	O	O	O	O	O
Functional Requirements Document	Sys		C	U	U			
Security Risk Assessment	Sec		C	U	→	→	U	
System Security Plan	Sec		C	U	→	→	U	
Security Plan of Action and Milestones (POA&M)	Sec		C	U	→	→	U	
Test Plans	Sys		O	O	C			
Configuration Management Plan	Sys		O	C	U	→	U	
Legacy Data Plan	Sys		O					
Detailed Design	Sys			C				
Contingency Plan	Sys			C	U	→	U	
Implementation Plan	Sys			O	C			
Acceptance Test Plan	Sys				C			
Security Control Assessment/Continuous Monitoring	Sec				C		U	
Acceptance Test Report and Approval	Sys				C			
Training Plan	Sys				C			
System Manuals	Sys				C	U	U	
User Manuals	Sys				C	U	U	
Security Accreditation Package	Sec				C	U	U	
Contingency Plan Test Report	Sec					C	U	
Security Accreditation Letter	Sec					C	U	
System Acceptance Letter	Sec					C		
Security Controls Test Report / Continuous Monitoring Annual Report	Sec						C U	
Security Re-certification and Accreditation Package	Sec						U	
Security Self-Assessment (Annual)	Sec						C U	
Disposition Plan	Sys						C	U

Legend

SDLCM Phases

Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

Type

PM = Project Management
Sys = System
Sec = Security
Acq = Acquisition

C = Core
O = Optional
U = Updated

Table 1 Footnotes:

[1] The DOL OCIO has developed a CBA template and cost model to aid IT PMs and IPTs in the development of their CBA. A copy of the CBA template and cost model can be found in the OCIO Resource Library on the DOL LaborNet under the System Development Life Cycle Management (SDLCM) topic area.

[2] An Operational Analysis is a CPIC activity that is performed annually during the O&M or Steady State Phase of an IT investment to determine whether there are any performance gaps with the investment. Depending on the results of the Operational Analysis, an updated or new investment CBA may need to be completed in the O&M Phase. (See Section 7.3.3 for more information on an Operational Analysis.)

Non-Major IT Investment Work Pattern

The work pattern for non-major IT investments is shown in Table 2 below.

As was the case with the major IT investments, the table shows the core (C), optional (O) and updated (U) deliverables for each life cycle phase for a non-major IT investment. See section 1.7 for a detailed explanation of each deliverable in this work pattern.

Table 2: Non-Major IT Investment Work Pattern

SDLCM Deliverables	Type	SDLCM Phase						
		Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
Project Charter	PM	C						
Cost Benefit Analysis (CBA) [1]	PM	C	U	→	→	U	2	
Project Management Plan (PMP)	PM	I	U	→	→	→	U	
Work Breakdown Structure (WBS)	PM	C	U	→	→	→	→	U
Risk Management Plan and Risk Register	PM	I						
Investment Target Architecture	PM	I	U	→	→	→	→	U
Investment Transition Strategy & Sequencing Plan (TS&SP)	PM	I	U	→	→	→	→	U
FIPS 199 System Categorization Report	Sec	C	U	→	→	→	→	U
Privacy Impact Assessment	Sec	C	U	→	→	→	→	U
Acquisition Plan	PM	O	I					
SOW	Acq	O						
Functional Requirements Document	Sys		C	U	U			
Security Risk Assessment	Sec		I	U	→	→	U	
System Security Plan	Sec		I	U	→	→	U	
Security Plan of Action and Milestones (POA&M)	Sec		I	U	→	→	U	
Test Plans	Sys				C			
Configuration Management Plan	Sys			I	U	→	U	
Legacy Data Plan	Sys		O					
Detailed Design	Sys			O				
Contingency Plan	Sys			I				
Implementation Plan	Sys				O			
Acceptance Test Plan	Sys				O			
Security Control Assessment/Continuous Monitoring	Sec				I			
Acceptance Test Report and Approval	Sys				C			
Training Plan	Sys				O			
System Manuals	Sys				O			
User Manuals	Sys				O			
Security Accreditation Package	Sec				I			
Contingency Plan Test Report	Sec					I		
Security Accreditation Letter	Sec					I		
System Acceptance Letter	Sec					I		
Security Controls Test Report / Continuous Monitoring Annual Report	Sec						I U	
Security Re-certification and Accreditation Package	Sec						U	
Security Self-Assessment (Annual)	Sec						I U	
Disposition Plan	Sys						I	

Legend
SDLCM Phases
Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

Type
PM = Project Management
Sys = System
Sec = Security
Acq = Acquisition

C = Core

O = Optional

U = Updated

I = Core unless it can be integrated into a parent investment. If integrated, the it is updated as the parent investment is updated. If not integrated, then the core deliverable is created and reviewed during each subsequent life cycle phase and updated as necessary.

Table 2 Footnotes:

[1] The DOL OCIO has developed a cost model to aid IT investments in the development of their CBA. A copy of the cost model can be found in the OCIO Resource Library on the DOL LaborNet under the SDLCM subject area.

[2] An Operational Analysis is a CPIC activity that is performed annually during the O&M or Steady State Phase of an investment to determine whether there are any performance gaps with the investment. Depending on the results of the Operational Analysis, an updated or new investment CBA may need to be completed in the O&M Phase. (See Section 8.3.3 for more information on an Operational Analysis.)

A Portfolio IT Investment (What work pattern do I use in this case?)

A Portfolio IT Investment is an IT investment that includes at least two or more major and/or non-major IT investments. From a work pattern perspective, a portfolio IT investment may be considered major or non-major depending on the component IT investments comprising the portfolio IT investment. If any component IT investment of a portfolio IT investment is considered a major IT investment, then the IT portfolio investment is considered major. In this case, it may be possible to included non-major IT investment deliverable reporting requirements into the deliverable documents of the parent or associated major IT investment. This only makes sense if the IT investments are related in some manner (e.g., organizationally or functionally). Otherwise, it would not make sense to combine the two investments in the same documentation materials.

If a portfolio IT investment is comprised of two or more non-major IT investments then the overarching IT portfolio investment may be considered a major IT investment depending on the major/non-major criteria described in the DOL OCIO CPIC Guide. When combining non-major IT investments together to form a single portfolio IT investment, PMs and IPT members should coordinate with the DOL OCIO CPIC team to review, discuss, and agree upon the bundling and classification of the portfolio IT investment as either major or non-major. In some cases, it may be desirable to create a portfolio IT investment and in other cases it may not work or be desirable. It depends on the nature of the IT investments be combined.

Deviations from the Major or Non-Major Work Patterns

PMs and/or IPT members should endeavor to follow and complete either the major or non-major standard SDLCM work patterns as shown in Table 1 and 2, respectively. However, it is possible that a new investment or system may not require one or more of the standard deliverables identified in Table 1 or 2. In this situation, the PM will need to arrange through appropriate Agency representatives and the System Owner to coordinate with the designated OCIO representative, to develop and document a waiver/exception to a deliverable(s) in the standard set of deliverables in Table 1 or 2. Please refer to the section on the Waiver/Exception Process.

1.7 Deliverable Description By Life Cycle Phase

This section describes the deliverables required for either major or non-major IT investments in each of the seven SDLCM phases. What you will find below in Table 3 is a summary of all SDLCM deliverables, identifying whether a document is core or optional, including the description of the deliverable in the phase in which it becomes a core document. Each deliverable appears only once, in the SDLCM phase that the deliverable first appears. In many cases, a deliverable is required to be updated in later phases. These updates are not reflected in the Table 3. Information on when each deliverable is required to be produced and updated was presented in Table 1 and 2, depending on the work pattern being followed.

Table 3: SDCLM Deliverable Description By Phase

Deliverable	Type*	Description
Phase 1 - Conceptual Planning Phase		
Project Charter	Core	An agreement between the requesting organization and the IT organization reviewing the request is reached. Decisions are made as to when the investment will be initiated, the target completion date and resources needed from both the user community and the IT organization to ensure a successful implementation. The Project Charter document describes the business need or performance gap that must be corrected or addressed and the proposed high level business and IT concept that will be implemented. This document identifies the intended business goals and objectives that are to be achieved as well as the key stakeholders, funding concept, high-level schedule, and critical success factors that must be met to ensure the desired outcomes (i.e., the business goals and objectives) are achieved. The document will need to be signed by the key business and technical stakeholders to ensure proper approvals and management support of the new IT investment. The DOL OCIO has developed a Project Charter document template to assist and support Agencies in developing a Project Charter for their specific IT investments. A copy of the template can be found in the DOL OCIO Resource Library on LaborNet at http://labornet.dol.gov/OCIO/resource-lib.htm under the SDLCM subject area.
Cost Benefit Analysis (CBA) and Cost Model	Core	Provides the results of the financial analysis of the projected life cycle costs and benefits of at least three viable investment alternative solutions to fulfill a business need or performance gap. A CBA supports management in making business decisions about initiating or continuing the life cycle of an IT investment. A CBA includes an Alternative Analysis section which describes the process in which three viable alternatives were selected, as a result of identifying first the feasible alternatives and then the most viable alternatives. The three most viable alternatives used in the CBA are required to be similar or comparable in size/scope and close the same business need or performance gap. For Major IT investments, the CBA life cycle period is required to be 10 years. For Non-Major IT Investments, the life cycle period should be at least 5 years. An investment CBA document should be no more than 5 years old and it is required be reviewed and "refreshed" annually in preparation for the annual CPIC Exhibit 300 budget process. "Refreshed" means the document is reviewed and updated as necessary to reflect any investment changes especially cost and/or benefit changes that could result in a change to the Net Present Value (NPV), Return on

Deliverable	Type*	Description
		Investment (ROI), and/or the chosen alternative. PMs of Major IT investments are required to actively manage the life cycle costs and benefits of the chosen investment on an annual basis. While "sunk" costs (i.e., costs that have already been incurred in prior fiscal years by the existing investment) are not included in a full CBA update, the reuse and/or portability of existing capital assets for the current investment must be leveraged and factored into the life cycle costs/benefits of the other viable alternatives, as applicable. The DOL OCIO has developed a detailed Cost Model to assist and support IT PMs in the development and maintenance of the investment CBA. The Cost Model alone does not represent a CBA as the content and results of a specific investment's Cost Model must be explained and justified in narrative form in a CBA document. A copy of the DOL OCIO Cost Model can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area. In addition, the DOL OCIO has prepared a detailed CBA template to assist and support PMs in completing their CBA documents. The CBA template can also be found in the DOL OCIO Resource Library on LaborNet at under the SDLCM subject area.
Project Management Plan	Core	A key IT investment planning and management document that uses a building block approach to planning and managing an IT investment. It includes a description of all the essential information associated with an IT investment and how an Agency, PM, and/or PMO will manage the IT investment through the SDLCM life cycle phases. For example, the PMP will include a description of the investment, the investment scope, the roles and responsibilities of individuals, teams, and/or Agencies involved in the development, deployment, and/or operation and maintenance of the IT investment. It will also include a description of the Work Breakdown Structure (WBS), a schedule of activities and milestones, resource estimates, and the relationship with other investments. It will include details regarding the Agencies and/or Agency units involved, required job tasks, milestone and review schedules. The PMP will also include a description of various documents that will be developed to support the IT investment including for example a Communication Plan, Records Management Plan, Risk Management Plan, Release Management Plan, and a Security Plan. Security and privacy requirements will be addresses in the PMP to ensure senior management that the system will meet all security and privacy issue concerns. The DOL OCIO has developed a PMP template to assist and support PMs and/or PMOs in developing a PMP. A copy of the DOL OCIO PMP template can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area.
Work Breakdown Structure (WBS) and WBS Dictionary	Core	A proven successful IT investment management planning tool that identifies in a hierarchical structure with numerous levels the life cycle work activities (i.e., work elements, sub-elements, packages, sub-packages, tasks, or subtasks) to be completed in order to achieve the investment mission, goals, and/or performance objectives. An investment WBS needs to be well planned and it should define, as much as possible, all of the work activities associated with an investment for each phase of its life cycle. While all the forthcoming work activities may not be known, the lower levels of the WBS are reviewed and expanded upon on a routine basis (i.e., at least annually as part of the investments budget preparation and approval process). Each of the elements in the WBS is uniquely numbered in a hierarchical fashion so they can be identified,

Deliverable	Type*	Description
		tracked, and related to the other work elements. It is important to note that once an investment WBS has become "baselined" the WBS elements and numbering cannot be changed without rebaselining the investment. Thus, PMs should plan and define as much of the investment WBS up front before it is baselined. A WBS is typically included in an MS Project schedule along with the start and end dates and resources for each WBS element. A WBS is deliverable oriented. That is, the output of each WBS element or sub-element results in a deliverable. In addition to creating a WBS, PMs are also required to create a WBS Dictionary that defines each work activity in the WBS as well as the resulting deliverable(s), and the estimated number of FTEs needed to complete the work activity.
Risk Management Plan and Risk Register	Core	The Risk Management Plan documents the risk management process that will be implemented by the Investment PM and/or Integrated Project Team (IPT) to identify, manage, and control the risks associated with successfully implementing the investment on time and within budget. The risk management process includes the 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. The Risk Register (RR) is a risk management tool for actively managing risks (i.e., logging, tracking, and documenting the current status of the risks including the status of the mitigating strategies associated with each investment risk). The DOL OCIO has created a standard Risk Management Plan template and a RR that all DOL IT investments are required to implement. A copy of the Risk Management Plan and associated RR can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area.
Investment Target Architecture	Core	The Investment Target Architecture is "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 the changing mission needs." An Investment Target Architecture is the explicit description and documentation of the desired (or "To Be") relationships among business and management processes and information technology. It is a framework for managing and connecting all aspects of an organization, from its business objectives and information needs to its data, supporting data systems and technological infrastructure. Business Architecture (BA) - Identifies broad high-level business processes that are core to supporting the IT investment, including mappings to the Business Reference Model, identification of stakeholders and Investment goals. The Business component is an analysis of the work the IT Investment intends to perform to support the organization's mission vision, and goals, and is the foundation Enterprise Architecture. Performance Architecture (PA) - Identifies quantifiable and outcome-based performance metrics (mapped to the Performance Reference Model) that will drive the IT Investment towards its target vision. These metrics should be tied to all layers of the Architecture. The DOL OCIO has created an "Investment Target Architecture" template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area.

Deliverable	Type*	Description
Investment Transition Strategy and Sequencing Plan	Core	Describes the overall plan for an organization to achieve its target Investment “to-be” vision within a specified timeframe, providing a clear link to the Investment Target Architecture. The Transition Strategy and Sequencing Plan helps to define logical dependencies between transition activities, helps to define the relative priority of these activities, and defines specific and meaningful milestones that can be used to track the IT investment’s progress towards achieving its “Target State” as it evolves through the investment life cycle. Milestones should be outcome-based and updated quarterly. The DOL OCIO has created an “Investment Transition Strategy and Sequencing Plan” template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area.
FIPS 199 System Categorization Report	Core	The FIPS 199 Security Categorization Report describes the results of the FIPS 199 Security Categorization process which identifies the sensitivity of the data contained in federal information systems. The categorization process is necessary to determine the controls required to adequately protect the information contained in the system. The FIPS 199 security categorization report is evaluated with each submission for certification and accreditation (C&A) of the system. Deliverable: Security Control Assessment Aid (SCAA) FIPS 199 Categorization Report (Sources: Computer Security Handbook (CSH) Volumes 4 and 14.)
Privacy Impact Assessment	Core	Reviews information maintained on the system, categorizes that information based on Privacy Act criteria and evaluates requirements for security as mandated by the Privacy Act.
Statement of Work (SOW)	Optional	A SOW is a document that is used for contractual purposes to describe the work or tasks to be performed and the products or services to be delivered by a contractor.
Phase 1 - Phase Gate Review Checklist	Core	A Phase 1 - Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 1 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
Phase 2 - Planning & Requirements Definition Phase		
Investment Target Architecture – Application Architecture,	Core	The Investment Target Architecture is updated in this phase to include the Application Data Architecture (DA). Data Architecture (DA) - Identifies the information needed to support the business, including mapping to the Data Reference Model. This component defines data

Deliverable	Type*	Description
Data Architecture, and Technical Architecture		entities, attributes, assets, taxonomy, and relationships in support of the target IT investment business functions. This component should define data exchanges between stakeholders (internal and external) and the associated data exchange mechanisms. Information flows should indicate where the information is needed and how information is shared to support mission functions.
Acquisition Plan	Core	Describes the investment acquisition strategy and procurement plan including the associated methods to be used for acquiring necessary hardware, software, and/or support services. The DOL OCIO has developed a detailed Acquisition Plan template as well as a guide to developing the Acquisition Plan to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the Acquisition Plan. A copy of the Acquisition Plan template can be found in the DOL OCIO Resource Library under the SDLCM subject area.
Functional Requirements Document	Core	A formal statement of an application's business requirements, and serves the same purpose as a contract. The developers agree to provide the capability specified and the client agrees to find the product satisfactory if it provides the specified capabilities. This document addresses the activities that need to be performed to analyze, understand, and review the overall architecture of the proposed system, the extent of interfaces with other existing internal/external systems or systems currently under development.
Security Risk Assessment	Core	Determines the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Security risk management is the process of identifying risk, assessing risk, and identifying the steps to reduce risk to an acceptable level.
System Security Plan	Core	A formal plan detailing the types of computer security is required for any new system based on the type of information being processed and the degree of sensitivity. The system security plan should directly address any vulnerability identified in the security risk assessment.
Security Plan of Action & Milestones (POA&M)	Core	Deliverable used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Major security efforts can be tracked within a investment and subsequently updated in the Operations and Maintenance Phase.
Legacy Data Plan	Optional	Identifies the time period covered by the data, volume of data, and where it resides. If some or all legacy data have already been converted to a new format, the approach to testing the converted data must be discussed. Requirements for processing legacy data in the future and plans for meeting those requirements are provided, and include a discussion of resource requirements for doing the conversion and potential problems that would need to be overcome.
Phase 2 – Phase Gate Review Checklist	Core	A Phase 2 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 2 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software

Deliverable	Type*	Description
		development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
Phase 3 - Design Phase		
Investment Target Architecture – Application Architecture, Data Architecture, and Technical Architecture	Core	The Investment Target Architecture is updated in this phase to include the Application Architecture (AA) and Technical Architecture (TA). Application Architecture (AA) - Defines the types of application(s) that supports the IT investment target business architecture and handle the data defined in the target data architecture. This architectural layer includes mapping to the Service Reference Model, specifies internal/external interface requirements, and illustrates architectural patterns that support functional requirements (examples include layered architecture, pipes and filters, batch processing, service oriented architecture). This information should be use to identify redundancies and define component reuse opportunities and associated cost savings/avoidance. Technical Architecture (TA) - Defines the technological infrastructure (the hardware, software, and communications network technologies) that support the applications identified in the Application Architecture, including mapping to the Technical Reference Model. The Technology Infrastructure component describes and identifies the physical layer including, the functional characteristics, capabilities, and interconnections of the hardware, software and communications.
Configuration Management Plan	Core	Systematic control of revisions is necessary to enable reproduction of past results from a team effort. This plan identifies the automated CM system to be used for software development, and other items to be placed under control, with methods of control. Locations where items are stored are specified and plans for audits are specified.
Detailed Design	Core	The preliminary system design clarifies the general characteristics of the system. It specifies the operating system, architecture components, their timing and sizing, external and internal interfaces, inputs and outputs of each subsystem, administrative activities, and security and auditing needs. The preliminary design is the foundation for the detailed design. System components are further specified into modules, processes, data, and interfaces and are defined to a level of detail that will enable a smooth transition to the Development and Test Phase.
Contingency Plan	Core	Used to ensure that a system can continue to operate and perform its function as needed during and after a localized emergency or large-scale disaster. Contingency planning ensures that DOL systems can recover from processing disruptions, no matter what the source.
Phase 3 – Phase Gate Review Checklist	Core	A Phase 3 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 3 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on

Deliverable	Type*	Description
		the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
Phase 4 - Development and Test Phase		
Test Plans	Core	The test plans document the test environment, resources, training, methods, schedules, evaluation, and test descriptions for unit, integration and system test activities as appropriate.
Implementation Plan	Core	Describes a plan for implementing the system in the operational environment. It translates business needs into key activities (i.e. installation, training, verification, monitoring); specifies an implementation schedule; and identifies specific personnel, hardware, software, and site requirements. It includes back-out plans for use when necessary.
Acceptance Test Plan	Core	This plan documents the scope, content, methodology, sequence, management of, and responsibilities for acceptance test activities. It ensures that all aspects of the system are adequately tested against requirements.
Security Control Assessment Aid/ Security Test & Evaluation (ST&E) Report	Core	The security controls assessment (SCA) of the full set of security controls performed in support of certification and accreditation (C&A) is an important step in ensuring the security of an information system. This assessment occurs at a single point in time. Deliverable: (1) Security Test and Evaluation (ST&E) Report; Computer Security Handbook (CSH) Volume 6 and (2) Security Self- Assessment, Security Control Assessment Aid (SCAA). (Source: Computer Security Handbook (CSH) Volume 4.)
Acceptance Test Report and Approval	Core	Documents software testing as defined in the Acceptance Test Plan. A summary of test results documenting problems encountered during testing, are attached to this report, as appropriate. In addition, this is also an approval checkpoint where a confirmation is reached that the IT system satisfies the intent of the investment and is ready to be released for implementation. The report documents that the acceptance test results have been reviewed and acceptance testing was completed successfully. Acceptance of the Acceptance Test Report by the designated approval authority indicates approval to move forward.
Training Plan	Core	Outlines the objectives, needs, strategy, and curriculum to be addressed for training users on the new or enhanced information system. The plan presents the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks.
System manuals	Core	Includes documents providing information to describe the design, development, production, distribution, operation, maintenance, and management of the system and are produced as needed to meet specific investment needs.
User Manuals	Core	Document instructions, guidance, and reference information relating to user execution of the system.
Security Certification and Accreditation Package	Core	The security certification process includes completing a Risk Assessment, System Security Plan, Security Test and Evaluation (ST&E), and Certification Statements. Only when these items have been completed can the system be accredited. ST&E involves determining a system's security mechanisms adequacy for completeness and correctness, and the degree of consistency between system documentation and actual implementation. This is accomplished through a variety of assurance methods such as analysis of system design documentation, inspection of test documentation, and independent execution of function testing and penetration testing.

Deliverable	Type*	Description
Phase 4 – Phase Gate Review Checklist	Core	A Phase 4 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 4 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
Phase 5 - Implementation Phase		
Contingency Plan Test Report	Core	The Contingency Plan Test Report documents the results of the contingency plan testing, which utilizes a variety of test elements, to include notification drills, component tests of the backup process, tabletop (scenario) exercises, and functional exercises to include testing of hot/warm/cold sites. These test elements are designed to deliver a complete contingency plan test comprised of several reports over a number of reporting cycles. Contingency plan testing must be coordinated with agency elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan). Deliverable: Contingency Plan Test Report (Source: Computer Security Handbook (CSH) Volume 6.)
Security Accreditation Letter	Core	The certification process includes completing a Risk Assessment, System Security Plan, Security Test and Evaluation, and Certification Statements. Only when these items have been completed can the system be accredited.
System Acceptance Letter	Core	This letter is signed by the Project Manager and the System Owner and verifies that the system has been successfully implemented and accepted according to documented plans and procedures.
Phase 5 – Phase Gate Review Checklist	Core	A Phase 5 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 5 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review

Deliverable	Type*	Description
		Checklists can be found in Appendix VII.
Phase 6 - Operations and Maintenance Phase		
Security Controls Test Report / Continuous Monitoring Annual Report	Core	The Continuous Monitoring Report documents the activities associated with the continuous monitoring process, which continually verifies the effectiveness of an information system's security controls. Continual vigilance is necessary to ensure the information system remains in a protected state. Deliverable: (1) Security Self-Assessment, Security Control Assessment Aid (SCAA) and (2) Continuous Monitoring Annual Report. (Source: Computer Security Handbook (CSH) Volume 4.)
Security Recertification and Accreditation Package	Core	Security recertification and accreditation is a process that is performed on an information system at least every 3 years to ensure a higher level of security for an information system and its data. Deliverable: C&A Package, Computer Security Handbook Volume 4.
Security Self-Assessment (Annual)	Core	Ensures that the system is in compliance with the latest requirements and synchronized with the most up-to-date security practices. Furthermore, self-assessments provide a mechanism to ensure that all requisite security documentation has been completed and updated with the latest system changes.
Disposition Plan	Core	States the approach and processes for disposing of a system in a planned orderly manner and to ensure that the system is properly archived or incorporated into other systems.
Phase 6 – Phase Gate Review Checklist	Core	A Phase 6 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment is prepared to continue to the next SDLCM phase. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 6 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
Phase 7 - Disposition Phase		
Updated Disposition Plan (as necessary)		The Disposition Plan is updated (as necessary) and executed in this phase. The result of the implementation of the Disposition plan is the archived system. The archived system is comprised of the packaged set of software, data, procedures, and documentation associated with the archived application.
Phase 7 – Phase Gate Review Checklist		A Phase 7 – Phase Gate Review is required to determine whether all required phase deliverables and activities (i.e., exit criteria) have been completed satisfactorily and whether the IT investment has be properly shutdown and decommissioned. The phase gate review is conducted by the IT Investment PM, PMO, and/or and involves all contractor teams supporting the IT investment. The DOL OCIO has developed a Phase 7 - Phase Gate Review Checklist to assist and

Deliverable	Type*	Description
		support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.
* Deliverable Types:	Core	Deliverable is required for this phase
	Optional	Deliverable may or may not be produced for this phase (depending on discussions with OCIO)

1.8 Capital Planning and Investment Control (CPIC)

CPIC is a critical budget planning and system development and implementation activity that must be successfully implemented throughout the life cycle of an IT system. See the *DOL Capital Planning and Investment Control (CPIC) Guide*, for details regarding the implementation of the DOL CPIC process. A copy of the CPIC Guide can be found in the OCIO Resource Library on the DOL LaborNet under the CPIC topic area.

1.9 IT Security

Now, more than ever, IT security is a critical element throughout the system development life cycle. Security must be incorporated and addressed from the initial planning and design phases through the disposal of the system. Without proper attention to security, DOL and its component Agencies' IT systems can compromise the ability of DOL to accomplish its mission. Please note that the requirement to complete necessary security documentation and processes is independent of the size or dollar amount of the investment. Security requirements are associated with the sensitivity and criticality of the information processed the relationship of the system to the organization's mission, and the economic value of the system's components. While all of the security documentation called out in this manual is required, system owners should work with OCIO and make risk adjusted evaluations of the content and level of detail required.

All DOL systems and applications require some level of protection. The appropriate level of protection is defined by evaluating the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system's components. A variety of Federal laws, regulations, and guidelines provide the requirements for information security. Most of the requirements are addressed by the E-Government Act of 2002, Federal Information Security Management Act (FISMA), the Clinger Cohen Act (CCA) of 1996, the Office of Management and Budget (OMB) Circular A-130, "Security of Federal Automated Information Resources," Homeland Security Presidential Directives HSPD 7, 8 and 12, Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection," and the DOL Cyber Security Program Plan (CSPP). There are numerous other regulations and guidelines that drive security requirements into the SDLCM including the DOL Computer Security Handbook

(CSH), which describes the Department-wide IT security policies, procedures, standards, and templates. The handbook was developed to facilitate commonality in IT security management planning and reporting throughout the Department. A copy of the DOL CSH can be found in the OCIO Resource Library on LaborNet under the Security subject area.

To meet the requirements of Federal mandates, every DOL Agency must certify that their information systems meet an acceptable level of risk in regards to the confidentiality, integrity, and availability and accredit those systems to operate. Each Agency's certification & accreditation program must cover all assets designated "sensitive systems."

For specific information regarding SDLCM security-related roles, responsibilities, and deliverables, please refer to the DOL CSH for more details.

In addition, the DOL CSH provides guidance in implementing the computer security policy outlined in DLMS-9, the DOL Cyber Security Program Plan, the National Institute of Standards and Technology (NIST), and "best practices" from other Federal organizations. These guidance documents will assist Agencies in evaluating and strengthening their IT infrastructure to protect the confidentiality, integrity, and availability of their data and IT systems.

Also, the DOL OCIO utilizes the U.S. Department of Justice Cyber Security Assessment and Management (CSAM) Internet-based tool to document, track, report, and manage the Department's information system security program. CSAM is intended to be used by security personnel of IT Investment responsible for security-related tasks, such as developing system security plans, developing contingency plans, and certifying and accrediting DOL information systems. The CSAM tool supports five IT security related functional areas:

1. Inventory Management
2. Plan of Action and Milestones (POA&M) Management
3. Certification & Accreditation (C&A) Functionality
4. FISMA Reporting
5. Custom Queries

CSAM offers IT Investment security personnel a number of IT security management related capabilities to support and manage their IT investments. For example, CSAM has the ability to:

- Function as a central repository for DOL C&A artifacts
- Generate a standardized System Security Plan (SSP) based on user supplied information
- Manage risk assessments using its Risk Assessment methodology
- Manage Control assessments using its Controls assessment methodology
- Continuously monitor capability
- Generate a host of reports to meet various IT security reporting requirements
- Perform custom queries

As such, IPT personnel responsible for managing and reporting IT security for an IT investment are required to use and leverage the capabilities of CSAM to enhance the IT security management of their IT investments and to comply with Department-wide IT security policy and guidelines documented in the latest version of the DOL OCIO Computer Security Handbook.

DOL IT investment IPT personnel responsible for IT security are required to take the DOL OCIO Security training before receiving a CSAM account. Please contact the DOL OCIO Security team to find out more information regarding CSAM including training, establishing user accounts, and help with using CSAM.

1.10 Strategic Business Management

The OCIO has implemented an Strategic Business Management (SBM) function, which is focused on improving and enhancing the alignment between business and technology across the DOL to improve program performance and contribute to achieving the Secretary's outcome goals. As with most major organizations today, information technology is a key enabler to business mission success and not the business driver. As such, the OCIO continues to strategically and operationally shift its focus towards enhancing DOL's business operations and performance outcomes through implementing IT modernization initiatives, pursuing common or shared business services, and utilizing IT investments to ensure they are tightly aligned, managed, and focused on adding business value and achieving business mission success.

To support this change, the DOL OCIO has realigned its governance structure to ensure alignment between the Departments planning activities, operations, and strategic business, mission and goals —thus ensuring information technology is used strategically to enhance and modernize the Department.

The SBM function is engaging agency business managers/stakeholders as well as IT managers on how best to meet and align the business mission goals/objectives of the organization. This function is ensuring existing and future IT initiatives are planned for, and support organizational business mission goals, operating plans, and associated high priority imperatives. The SBM function is also encouraging and supporting DOL agencies in taking a long-term view of technology across DOL to leverage economies of scale (e.g., standardization, 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. This functional group is responsible for coordinating with DOL Agencies in the development and maintenance of agency and Department-level as-is and to-be architectures and the associated transition plans.

1.11 Performance Management

DOL IT investment PMs will need to develop, implement, and manage a Performance Management process throughout the life cycle of the investment. This process includes defining meaningful IT investment performance goals, measures, and metrics as well as measuring, tracking, and reporting out on the actual performance of the investment against an established baseline. PMs will need to first define specific investment performance measures and the associated metrics that will be measured and tracked. PMs will also need to ensure investment performance measures/metrics align with and support the Agency and Department Enterprise Architecture (EA) Performance Reference Model (PRM) as well as the associated Agency and Department Target EA. See your Agency and DOL target EA for more specific information on the PRM.

IT PMs will need to monitor, track, and report out the performance of their IT investment to Agency sponsors, stakeholders, as well as the OCIO, and OMB via various reporting activities and/or documents (e.g., Agency internal performance reviews, OCIO EA Transition Strategy, OCIO Controls Reviews, OMB Exhibit 300 business cases, and/or via the Performance Assessment Rating Tool (PART) process.) PMs will need to use the Agency and Department EA as necessary or required to monitor, track, and report out on the performance of IT investments.

Investment performance is measured, assessed, controlled, and reported out via one of two Performance Based Management techniques (i.e., Earned Value Management (EVM) and Operational Analysis (OA)) depending on what life cycle phase the investment is in. That is, Major IT investments including Development Modernization and Enhancement (DME) investments and DME activities of mixed life cycle investments are required to implement Earned Value Management (EVM) and follow the DOL EVM System (EVMS).

Figure 3 illustrates the types of questions that EVM helps answer regarding the performance status of an IT investment:

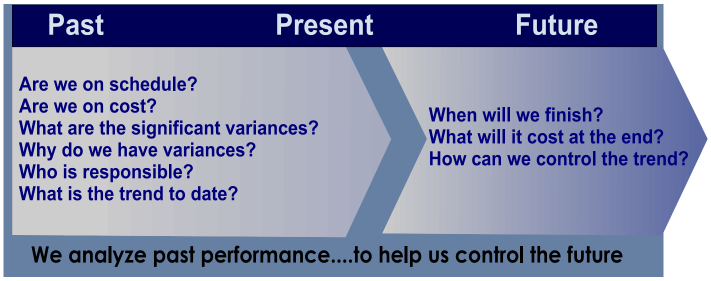
Past
Present
Future
Are we on schedule?
Are we on cost?
What are the significant variances?
Why do we have variances?
Who is responsible?
What is the trend to date?
When will we finish?
What will it cost at the end?
How can we control the trend?
We analyze past performance....to help us control the future

Figure 3: Types of Questions Answered by Earned Value Management (EVM)

EVM is used to assess the health of DME investments or DME activities of mixed life cycle investments by measuring an investment's actual cost and schedule performance against an approved Performance Measurement Baseline (PMB).

A PMB is required of all DOL IT investments that are implementing or are required to perform EVM. In accordance with the PMBOK, a PMB is an approved integrated scope-schedule-cost plan for the work that will be performed. It will be used to measure and manage the actual work performed, i.e., to measure work performance. The PMB includes the integration of a time-phased schedule of all the work to be performed, the budget cost for the work, and the organizational elements that will perform the work and produce the required deliverables.

All DOL IT investments are required to follow PMBOK practices and guidelines for developing and implementing a PMB. As shown in the OCIO PMB training presentation (which can be found in the OCIO Resource Library on LaborNet, the four steps for developing a PMB are as follows:

Step 1: Define what will be performed (Scope): Statement of Work
Step 2: Determine what work needs to be done (to the best of your ability) to complete the project's Statement of Work/Scope
Step 3: Assign Responsibility for elements of work: Organizational Breakdown Structure & Responsibility Assignment Matrix
Step 4: Integrate the Organizational Breakdown Structure & Responsibility Assignment Matrix with the WBS to create the Control Accounts

In addition to reflecting the contractors' work, a PMB also reflects Program Management Office (PMO) activities, Independent Validation and Verification (IV&V) activities, IT security activities, Strategic Business Management (SBM) activities, capital planning activities, and all other activities required for the investment to achieve the desired results.

The PMB is typically developed following vendor/integrator contract award. Once the PMB is developed, it will need to be approved during the Integrated Baseline Review (IBR). The IBR is a critical initial IT investment meeting as it is an opportunity for the government PM/IPT and vendor/integrator to discuss in detail the scope of work to be completed and reach agreement on the PMB including the specific tasks that will be performed, when they will be executed and completed, and by which resource(s). The purpose of the IBR is three-fold: (1) to provide mutual understanding and buy-in of the investment's PMB, (2) to understand the risks involved in executing the investment schedule, and (3) to develop plans to either avoid or mitigate the effects of those risks. The four phases of an IBR process include:

- Developing the PMB or review the current PMB (subsequent IBR cycles)
- Preparing the team for the IBR by reviewing the essential documentation and the risks involved with executing the investment as laid out in the current PMB.
- Conducting IBR sessions to validate the PMB and review risks to actively address and watch.
- Establishing management review processes such as monthly performance measurement reviews to monitor execution of the investment against the PMB

For additional IBR information including details in executing each of the four phases above, see the DOL OCIO *Introduction to the Integrated Baseline Review (IBR)* training presentation dated January 30, 2008. The IBR presentation can be found in the OCIO Resource Library on LaborNet under the 2008 training classes listed in the Training subject area.

Once the PMB is approved as a result of the IBR, its integrity as an integrated measurement tool, relating scope, schedule, and cost, will need to be managed closely and strictly maintained to ensure that the EVM process is sound and the EVM reports are reflecting true performance.

In the event that the PMB needs to change, IT investment PMs, PMOs, and/or IPTs will need to follow the OCIO re-baselining guidelines and procedures as described in the *OCIO IT Investment Rebaseline Guidance* version 1.1, dated April 2009. A copy of the *OCIO IT*

Investment Rebaseline Guidance document can be found in the OCIO Resource Library on LaborNet under the CPIC subject area.

For more information on EVM and the DOL Earned Value Management System (EVMS) please see the *DOL EVM Operational Guide* which can be found in the DOL OCIO Resource Library on LaborNet under the CPIC EVM subject area . The DOL OCIO has also developed a handy *EVM Quick Reference Guide* to assist and support DOL IT Investment PM and IPTs in understanding and implementing EVM activities. The DOL *EVM Quick Reference Guide* can also be found in the DOL OCIO Resource Library on LaborNet under the CPIC EVM subject area.

1.12 Quality Assurance

Quality Assurance (QA) activities are conducted in many ways throughout the SDLCM. Project Managers and other senior leadership within the Agencies are responsible for ensuring quality assurance on their investments through peer reviews, independent validation and verification reviews as described below, and other QA activities.

Conducting an Independent Verification and Validation (IV&V) review of an IT investment has been a long standing and proven practice for improving the quality and performance of an IT investment solution. Thus, DOL IT investments will need to perform IV&V reviews commensurate with the major/non-major status of the IT investment to the business mission of the DOL Agency or the Department. DOL IT PMs will need to coordinate and seek OCIO approval on the IV&V direction it is planning to take in regards to an IT investment. Every DOL IT investment is different and as such the IV&V approach needed will be reviewed and approved by the OCIO on a case-by-case basis.

PMs and/or IPTs will need to assess their IT investments, in the Conceptual Planning phase of the SDLCM, to determine whether a formal/informal Agency or OCIO led IV&V review will be required for the IT investment. The IV&V assessment and resulting formal/informal IV&V review will need to be conducted in accordance with the IV&V methodology, standards, and procedures laid out in detail in the DOL IV&V Manual, v1.0. A copy of the DOL IV&V Manual will be available in the OCIO Resource Library on LaborNet.

As described in the IV&V Manual, the goal of performing an IV&V review is to improve the quality and performance of the IT investment, while the IT investment is progressing through each of the phases of the SDLCM process.

There are numerous benefits associated with implementing a disciplined IV&V review process including:

- Independent assessment – Provides an objective and unbiased evaluation of the system. An IV&V Team assesses the system quality and provides recommendations for improvement that result in:
    - Facilitating early detection and correction of software anomalies

  - Enhancing management insight into development risks
  - Providing an early assessment of software and system performance
  - Improving the software development and maintenance process

- Increased visibility – Performing an IV&V process provides increased visibility into all phases of the SDLCM. This ensures the client and all stakeholders have insight into all phases of the development effort and that independent quality standards are enforced and communicated via the IV&V process.

- Enhanced risk assessment – IV&V activities enhance risk assessments of the system throughout each phase of the SDLCM. The IV&V process identifies risks early in the IT investment system's life-cycle, noting recommendations that improve system quality and reduce potential rework costs. The IV&V Team might uncover risks that would not have been identified or disclosed by the Development Team.

- Verification of deliverables – IV&V activities will assess SDLCM deliverables for standards compliance, making necessary recommendations. This includes ensuring that the required artifacts and deliverables for each phase of the life-cycle are completed and archived appropriately.

- Validation of requirements and solution – IV&V activities will confirm that the software satisfies the user's mission needs, and that requirements are adequately demonstrated and tested. Deliverable reviews focus on technical content, ensuring the system has been well engineered.

Thus, the PMP shall describe the IT Investment PM's plan to assess the level of IV&V review required and then acquire the IV&V support services, as necessary and appropriate for the investment. IV&V support services, if required, shall be procured via a separate contract from the IT investment's integration contract to ensure independence and no contractual conflict of interest.

In addition, the PMP shall also describe how the PM will implement and conduct the IV&V review process as defined in the DOL IV&V Manual to improve the quality and ensure the successful design, development, testing, quality assurance, and deployment of the IT investment solution.

As described in the DOL IV&V Manual, a project specific IV&V Project Plan will be developed describing the organization of the IV&V Team, the scope of IV&V work activities, deliverables, an IV&V Work Breakdown Structure (WBS), and any assumption, constraints, and/or tailoring decisions unique to the IV&V project.

Refer to the DOL IV&V Manual, v1.0, for a detailed description of the IV&V methodology, standards, procedures, and required IV&V related deliverables. A copy of the DOL IV&V Manual can be found in the OCIO Resource Library on LaborNet under the System Development Life Cycle Management (SDLCM) subject area.

The OCIO also provides QA oversight for IT investments through the IT Investment Management Framework process. IT investments will be screened initially before they are approved for IT Crosscut budget funds. In addition, the control phase of capital planning process ensures that investments stay on track in terms of schedule, budget and technical performance. Finally, OCIO security staff must review and approve all security related SDLCM deliverables before an investment is permitted to move forward.

1.13 Information Quality Guidelines

In 2000, Congress passed legislation regarding information quality. The legislation specifically directed all Federal agencies to:

- Issue information quality guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information, including statistical information, disseminated by the Department;
- Establish administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the Department that does not comply with the OMB guidelines; and
- Annually report to the Director of OMB the number and nature of complaints received regarding compliance with the OMB guidelines, including how the complaints were resolved.

The DOL guidelines were effective as of October 1, 2002, and can be found at: http://www.dol.gov/informationquality.htm. Project managers must be cognizant of the guidelines and take them into account when beginning system development investments that perform data analysis or disseminate information.

1.14 Software Life Cycle Models

The DOL SDLCM principles and practices, as described in this manual, is by design and intent provided in sufficient detail as to provide clear guidance and direction for IT PMs and IPTs, yet broad in scope and generalized to cover a wide range of IT investments including software systems and applications that are being developed using standard software development models and any number of standard software languages and tools. The DOL SDLCM does not require or mandate a particular software development life cycle approach. This is left to IT PMs and IPTs to decide which software development life cycle approach is best suited for the IT investment. A software life cycle model 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, the model is a critical element for the overall success of an investment, incorporating all aspects of system engineering influences on an investment from management planning to design.

Considering the benefits provided by the incremental/iterative life cycle development approach, both Departmental IT and EA guidance state 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 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. For further information on software life cycle models, please refer to Appendix I.

1.15 Waiver/Exception Process

If one or more standard SDLCM deliverables are not necessary or required to be generated in conjunction with the development of an IT investment, an exception request needs to be received and approved by the OCIO. Project Managers will need to coordinate with OCIO staff, discuss the exception process prior to the conceptual planning phase, and submit an SDLCM Exception Request Form for approval. Exception requests will be handled on a case-by-case basis, taking into consideration the size, scope, and complexity of the investment and the applicability of the specific request. Please utilize the exception request form located in Appendix IV, directing requests to the OASAM Office of Systems Development and Integration as referenced. The System Development Team and the Capital Planning Team will initially review exception requests and the Deputy CIO will provide final approval.

2 CONCEPTUAL PLANNING PHASE

2.1 Phase 1 Overview

The SDLCM methodology begins with the Conceptual Planning Phase. It is during this phase that a need to develop or significantly enhance a system is identified, its feasibility and costs assessed, and risk and investment-planning approaches defined. Figure 4 identifies key inputs, activities, and deliverables of this phase.

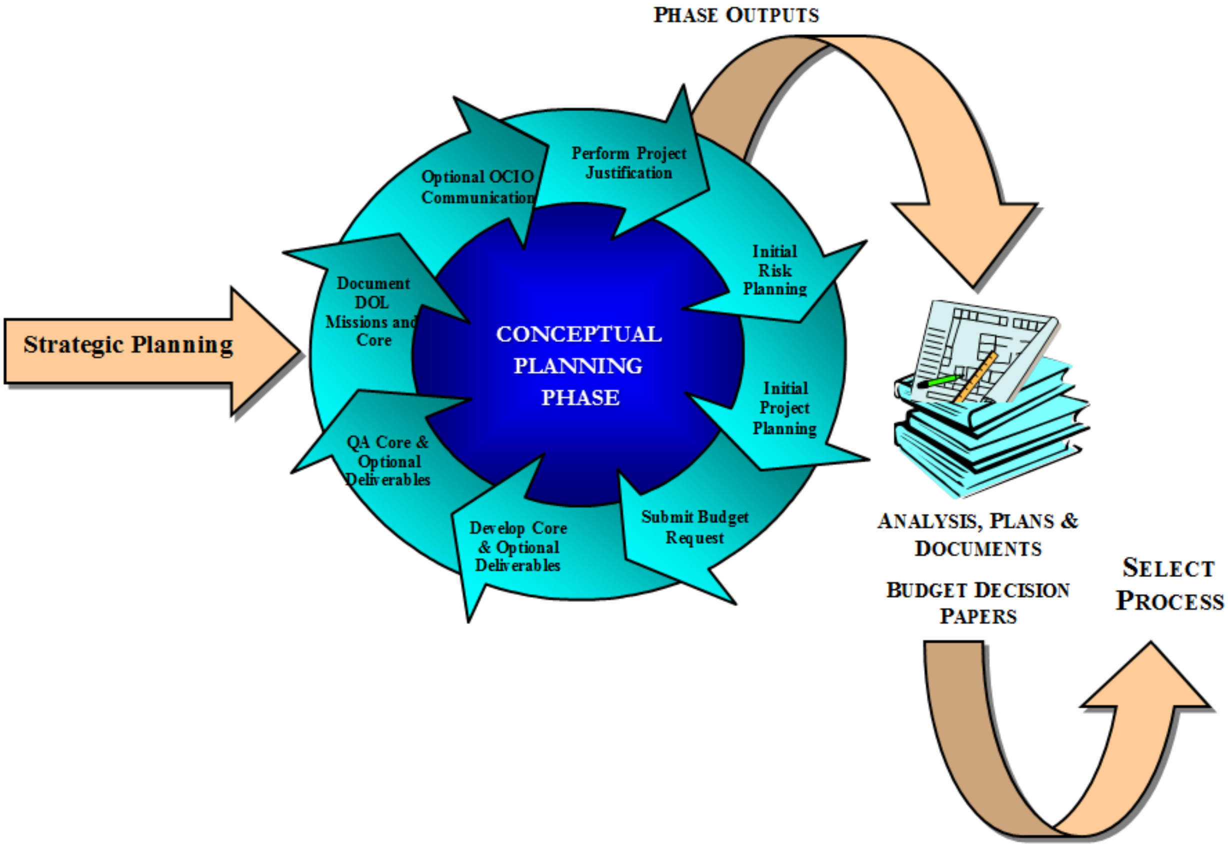
PHASE OUTPUTS
Strategic Planning
Optional OCIO Communication
Perform Project Justification
Initial Risk Planning
Initial Project Planning
Submit Budget Request
Develop Core & Optional Deliverables
QA Core & Optional Deliverables
Document DOL Missions and Core
CONCEPTUAL PLANNING PHASE
ANALYSIS, PLANS & DOCUMENTS
BUDGET DECISION PAPERS
SELECT PROCESS

Figure 4: Conceptual Planning Phase Activities

2.2 Phase Inputs

Conceptual planning begins with a need to develop a new IT system or to enhance an existing one. The identification for a need or opportunity may be communicated formally as part of Agencies' strategic planning process, or informally via telephone, e-mail or a verbal discussion. During the justification process, a functional manager provides the first critical description of the information management concept and secures the resources needed for further examination of the concept and potential approaches. A functional manager may prepare a concept paper (issue paper or decision paper) that identifies and describes the information management concept. Depending on the sensitivity or criticality of the issue, the functional manager may submit the concept paper to program management or executive management for information and/or approval.

2.3 Phase Activities and Deliverables

2.3.1 Document DOL Mission/Core Processes

A review of DOL's mission statement is critical before initiating an IT investment. The following two important points are noted here:

- There is a strong emphasis on defining the information management need or opportunity and linking it to specific U.S. Department of Labor (DOL) missions, strategic goals, and/or core processes, as required by the Clinger-Cohen Act, implemented by the Office of Management and Budget (OMB).

- No assumption can be made that the approach will necessarily result in the development of a new system or the replacement of a manual process with an automated system. A modification to existing manual or automated systems may be the best approach to address the need or opportunity; the determination could be recommended in the Project Charter. In all cases, a manual process should be evaluated for improvement opportunities before considering automation.

2.3.2 OCIO Communication

It is recommended that investment representatives have clarifying discussions with OCIO representatives during the Conceptual Planning phase as necessary or required. Ideally, for every IT investment that an Agency initiates investment representatives will have drafted an IT investment proposal and/or Project Charter that can be used during these discussions. This prepared information should discuss the business problem that has served as the impetus for the investment, alignment with the Department's strategic plan, the contribution of the IT investment to program areas, and any alignment with other investments going on either within DOL or across the Federal Government landscape.

The purpose of a discussion is for the investment team to propose their investment to OCIO staff, receiving in return any required clarifying guidance and feedback. The initial consultation may include discussions regarding whether it is reasonable to pursue the investment, what the investment team needs to be thinking about as it moves forward, what work pattern, deliverable, and security requirements would be appropriate for the investment. A determination at this time is made whether the IT development, modification, or enhancement requires a security classification (see DOL Computer Security Handbook). Sensitive systems must be identified in accordance with the E-Government Act of 2002 and OMB Circular A-130. Coordination between the appropriate Agency officials and the OCIO is required to take place to ensure posting in the Federal Register.

No funding decisions are made at this time – the communication serves simply as an interactive discussion and an opportunity for OCIO to provide guidance to the investment team.

2.3.3 Perform Investment Justification

The Conceptual Planning Phase is where the identification of need is formalized. The need or opportunity identified prior to initiating this phase is formalized into a Project Charter defining what the need is, benefits to the organization, and the proposed solution and approach. The IT investment concept is defined in business terms to enable the successful development of an appropriate solution.

To continue, Agency management must commit resources to explore ways to address the need or opportunity. Management must also determine if staff or other resources will be devoted to defining and evaluating alternative ways to respond to the identified need or opportunity. At this point, the decision to proceed generally is accompanied by a Cost Benefit Analysis (CBA). The Project Charter in conjunction with a CBA could provide information that management needs to make decisions to initiate or continue the development, procurement and modification of proposed investment. The process used is the same process followed under the Departments' IT Capital Planning and Investment Control (CPIC) IT investment selection process.

Deliverables:

Project Charter - An agreement between the requesting organization and the IT organization reviewing the request is reached. Decisions are made as to when the investment will be initiated, the target completion date and resources needed from both the user community and the IT organization to ensure a successful implementation.

Cost-Benefit Analysis (CBA) – Provides the results of the financial analysis of the projected life cycle costs and benefits of at least three viable investment alternative solutions to fulfill a business need or performance gap. A CBA supports management in making business decisions about initiating or continuing the life cycle of an IT investment. A CBA includes an Alternatives Analysis section which describes the process in which three viable alternatives were selected, as a result of identifying first the feasible alternatives and then the most viable alternatives. The three most viable alternatives used in the CBA are required to be similar or comparable in size/scope and close the same business need or performance gap. For Major IT investments, the CBA life cycle period is required to be 10 years. For Non-Major IT Investments, the life cycle period should be at least 5 years. An investment CBA document should be no more than 5 years old and it is required be reviewed and "refreshed" annually in preparation for the annual CPIC Exhibit 300 budget process. "Refreshed" means the document is reviewed and updated as necessary to reflect any investment changes especially cost and/or benefit changes that could result in a change the NPV, ROI, and/or the chosen alternative. PMs of Major IT investments are required to actively manage the life cycle costs and benefits of the chosen investment on an annual basis. While "sunk" costs (i.e., costs that have already been incurred in prior fiscal years by the existing investment) are not included in a full CBA update, the reuse and/or portability of existing capital assets for the current investment must be leveraged and factored into the life cycle costs/benefits of the other viable alternatives, as applicable.

The DOL OCIO has developed a detailed Cost Model to assist and support IT PMs in the development and maintenance of the investment CBA. The Cost Model alone does not represent a CBA as the content and results of a specific investment's Cost Model must be explained and justified in narrative form in a CBA document. A copy of the DOL OCIO Cost Model can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area. In addition, the DOL OCIO has prepared a detailed CBA template to assist and support PMs in completing their CBA documents. The CBA template can also be found in the DOL OCIO Resource Library on LaborNet.

Conceptual Planning Phase Gate Review – A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 1 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

2.3.4 Initial Investment Planning

During the Conceptual Planning phase, the individuals sponsoring the IT investment will need to complete the initial investment planning activities, including identifying essential investment personnel. A key first step in this process, is to designate a Project Manager having the appropriate skills, experience, credibility, and availability to lead the effort and identify the System Owner point of contact and the Integrated Project Team (IPT) members which includes support personnel from key organizations. Once the IPT has been created, they will need to draft a Project Management Plan (PMP). This document, described below, will also get updated regularly during the lifecycle of the investment.

Deliverables:

Project Management Plan (PMP) - The PMP is the single most critical initial investment management and planning document that is created for any investment. It lays out the detailed plan on how the Project Manager and IPT will manage and follow the DOL IT Investment Management Framework to deliver, operate, and maintain the selected or chosen investment from the CBA. The PMP describes the investment purpose, scope, work activities or tasks, schedule, key milestones, required resources, and interrelationships with other investments. It also provides details on how the PM and IPT will manage the investment through each of the phases of the SDLCM and CPIC processes and complete the required investment management deliverables including the SDLCM, CPIC, Security, and

EA deliverables. It is one of several key planning documents that use a building block approach to investment management and planning.

Work Breakdown Structure (WBS) - A WBS is a proven successful IT investment management planning tool that identifies in a hierarchical structure with numerous levels the life cycle work activities (i.e., work elements, sub-elements, packages, sub-packages, tasks, or subtasks) to be completed in order to achieve the investment mission, goals, and/or performance objectives. An investment WBS needs to be well planned and it should define, as much as possible, all of the work activities associated with an investment for each phase of its life cycle. While all the forthcoming work activities may not be known, the lower levels of the WBS are reviewed and expanded upon on a routine basis (i.e., at least annually as part of the investments budget preparation and approval process). Each of the elements in the WBS is uniquely numbered in a hierarchical fashion so they can be identified, tracked, and related to the other work elements. It is important to note that once an investment WBS has become "baselined" the WBS elements and numbering cannot be changed without rebaselining the investment. Thus, PMs should plan and define as much of the investment WBS up front before it is baselined. A high level WBS is typically included the Project Management Plan (PMP) and a detailed version is included in an MS Project schedule along with the start and end dates and resources for each WBS element. A WBS is deliverable oriented. That is, the output of each WBS element or sub-element results in a deliverable. In addition to creating a WBS, PMs are also required to create a WBS Dictionary that defines each work activity in the WBS as well as the resulting deliverable(s), and the estimated number of FTEs needed to complete the work activity.

Statement of Work (SOW) (optional) - A SOW presents the scope of the work that is to be investigated and the objectives to be accomplished.

2.3.5 Initial Risk Planning

A process for identifying, assessing, monitoring, reporting, and mitigating investment risks – is identified and documented in the Investment Risk Management Plan deliverable. Investment risks are identified and analyzed to determine any negative scope, technical, cost, and schedule risks to the investment. Analysis of investment risks should be coordinated and categorized in alignment with OMB's Exhibit 300 risk planning requirements. Refer to the Appendix II for a reference link to OMB documents.

Frequent review points are identified when the investment is divided into manageable tasks and activities. By authorizing effort to be expended only for the next phase and by requiring approval to proceed beyond that point, senior management can limit exposure to only the cost of the next phase. Further, because confidence in estimates is strongest for the next immediate phase and is less predictable for subsequent phases, management may assume they are authorizing work to be performed against an estimate that is reasonably reliable. To facilitate risk management at the end of each phase, the SDLCM methodology requires a detailed and accurate time and cost projection for the next phase, while permitting a less detailed time and cost estimate for the balance of the investment. This enables management to make decisions in an environment where risks can be managed and controlled.

(Note: The Investment Risk Assessment is no longer a separate required deliverable for the SDLCM, it is now incorporated in the Risk Management Plan. However, the Security Risk Assessment is a separate document covered in the security section.)

Deliverable:

> **Risk Management Plan** - 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 investment risk management is initiated and continues until the investment is operational. While security risks can be identified in the Investment Risk Management Plan, only the security risks related to the successful development and implementation of the investment should appear. This would typically include risks involved with the development and integration of security modules for the IT investment (i.e. levels of control and access). Security risks (vulnerabilities/threats) inherent in the operation of the system are documented and covered in the Security Risk Assessment.

2.3.6 Strategic Business Management

As described in detail in Section 1.10, Strategic Business Management is focused on improving and enhancing the alignment between business and technology across the DOL to improve program performance and contribute to achieving the Secretary’s outcome goals. It is also closely linked to the DOL Systems Development Life Cycle Methodology (SDLCM). As an IT investment progresses through the SDLC, its Target EA must be updated to reflect it’s “to be vision”. Additionally, the Investment Transition Strategy must be updated to clearly describe the evolving plan (including activities, milestones, and dependencies) to achieve the “to-be vision”.

Deliverables:

> **Investment Target Architecture –** The Investment Target Architecture is “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 the changing mission needs.” An Investment Target Architecture is the explicit description and documentation of the desired (or “To Be”) relationships among business and management processes and information technology. It is a framework for managing and connecting all aspects of an organization, from its business objectives and information needs to its data, supporting data systems and technological infrastructure.

The DOL OCIO has created an "Investment Target Architecture" template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area.

Investment Transition Strategy and Sequencing Plan – The Investment Transition Strategy and Sequencing Plan describes the overall plan for an organization to achieve its target Investment "to-be" vision within a specified timeframe, providing a clear link to the Investment Target Architecture. The Transition Strategy helps to define logical dependencies between transition activities, helps to define the relative priority of these activities, and defines specific and meaningful milestones that can be used to track the IT investment's progress towards achieving its "Target State" as it evolves through the investment life cycle. Milestones should be outcome-based and updated quarterly.

The DOL OCIO has created an "Investment Transition Strategy and Sequencing Plan" template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area.

2.3.7 Initial Security Planning

IT Security management and planning is a critical part of IT investment management. .

Deliverable:

FIPS 199 System Categorization Report - The FIPS 199 Security Categorization Report describes the results of the FIPS 199 Security Categorization process which identifies the sensitivity of the data contained in federal information systems. The categorization process is necessary to determine the controls required to adequately protect the information contained in the system. The FIPS 199 security categorization report is evaluated with each submission for certification and accreditation (C&A) of the system. Deliverable: Security Control Assessment Aid (SCAA) FIPS 199 Categorization Report (Sources: Computer Security Handbook (CSH) Volumes 4 and 14.).

Privacy Impact Assessment - Reviews information maintained on the system, categorizes that information based on Privacy Act criteria and evaluates requirements for security as mandated by the Privacy Act.

2.3.8 Submit Budget Request

An initial budget request is prepared and submitted to ensure the availability of funding, personnel, and other resources needed to proceed with the investment.

Note: The budget request is not an SDLCM deliverable but will need to be produced to facilitate securing funding to move the investment forward. Please discuss the budget request and OMB Exhibit 300 reporting requirements with the OCIO Capital Planning staff or DOL Budget staff. Refer to the integrated business process in the executive summary for an overview of funding activities and outcomes.

2.3.9 Develop Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

2.3.10 QA Core & Optional Deliverables

The project manager is required to Quality Assurance check all investment deliverables. In addition, investment deliverables are required to be submitted and maintained in the resource library within the OCIO eCPIC tool. The eCPIC resource library is a central repository for all IT investment SDLCM and CPIC documentation or deliverables.

2.4 Phase Considerations

Key considerations during this phase should address the following questions:

- ➢ Is it feasible to proceed? Is the IT need or opportunity beyond the capabilities of existing systems and is developing a new system a promising approach?

- ➢ Do the projected benefits of the proposed IT investment justify the investment costs and resources needed?

- ➢ Are appropriate funding and other needed resources available to proceed? (At least to the point where the investment funding will be secured in the IT Capital Planning process).

- ➢ Have investment risks been examined and reviewed by all parties concerned and a risk management plan appropriately documented?

- ➢ Have the investment’s purpose, scope, WBS, schedule, key milestones, and resources been planned and documented in the PMP?
- ➢
- ➢ Have security requirements been discussed, and has a security classification been established and confirmed by the OCIO Security Officer?

- ➢ Has a User Group been established (if needed, at the discretion of the Agency)?

3 PLANNING & REQUIREMENTS DEFINITION PHASE

3.1 Phase 2 Overview

The Planning and Requirements Definition Phase begins after the investment has been defined and appropriate resources have been identified through the initial selection process of Capital Planning. There are two essential aspects of this phase: 1) planning, and 2) defining the functional requirements that the system will need to address. It is during this phase that the Project Management Plan is updated to include or provide additional detail regarding the development approach and methods, tools, tasks, resources, and schedules. Functional requirements are defined to address data, system performance, security, and maintainability aspects of the system. In addition, near the end of this phase, the investment completes the final selection process of capital planning, committing funds for the investment for the next year. Figure 5 identifies key inputs, activities, and deliverables of this phase.

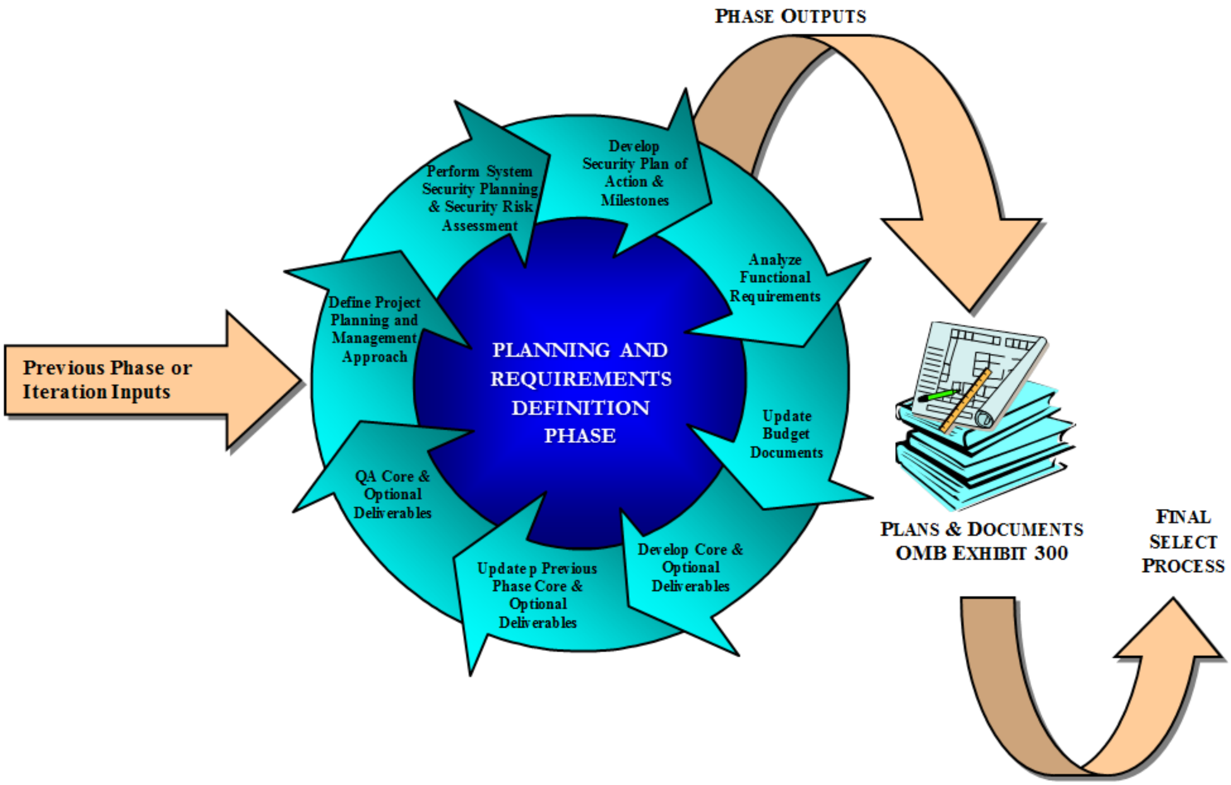
PHASE OUTPUTS
Previous Phase or Iteration Inputs
Perform System Security Planning & Security Risk Assessment
Develop Security Plan of Action & Milestones
Define Project Planning and Management Approach
Analyze Functional Requirements
PLANNING AND REQUIREMENTS DEFINITION PHASE
Update Budget Documents
QA Core & Optional Deliverables
Updatep Previous Phase Core & Optional Deliverables
Develop Core & Optional Deliverables
PLANS & DOCUMENTS OMB EXHIBIT 300
FINAL SELECT PROCESS

Figure 5: Planning & Requirements Phase Activities

3.2 Phase Inputs

The inputs to the Planning and Requirements Definition Phase are the deliverables that were produced during the Conceptual Planning Phase. As a general rule, even if the investment is using an iterative (multiple releases) approach, inputs for each phase will consist of the outputs from the previous phase. Moreover, deliverables first produced in a previous phase may be updated throughout the life cycle of the investment. Requirements for deliverable updates are not called out in these sections – please refer to the work pattern matrices for the specifics.

3.3 Phase Activities and Deliverables

Activities and deliverables produced and/or updated in the Planning and Requirements Definition Phase are described below. Deliverables are to be reviewed and approved in accordance with the integrated business process quality assurance step before moving into the Design Phase.

3.3.1 Define Investment Planning and Management Approach

The methodology to be adopted for the IT effort is defined and customized. For large or complex investments, it may be appropriate to divide the investment into major logical or functional components/subsystems and manage the evolution of each component/subsystem through the life cycle. However, for such investments, proper coordination across the logical/function component/subsystems is necessary to ensure consistency and successful integration. Other factors related to defining the investment planning and management approach include the following:

1. Confirming and finalizing the SDLCM work pattern and any tailoring aspects.

2. Establishing investment schedules. The schedule should allocate time for routine systems maintenance activities such as: conversion/upgrades of hardware and software; removal of defects or minor modifications to reflect changes in the business or technical environment or legislation; alteration, rewriting, or restructuring of a system to reduce the maintenance effort or to make operations more efficient.

3. Planning for emergency maintenance and establishing procedures to address sudden breakdowns due to hardware or software failure.

4. Managing life cycle activities by setting specific milestones for measuring the work completed to the costs incurred during the life cycle.

5. Identify Investment Tools and Methodologies. The organization of the investment and methodologies and tools to be used in this phase and subsequent phases are identified and planned for in this phase. The set of methods and tools may include prototyping and utilization of computer-aided software engineering tools, as well as the needs for linking the tools across all subsequent life cycle phases and activities.

6. Estimating human resource requirements for staffing an investment is a key activity of investment planning and should be done in conjunction with evaluating the scope of the investment, identifying the tasks and deliverables, estimating the required resource hours, distributing resource hours and leveling resources and reviewing the preliminary estimates thoroughly. Another essential activity of investment resource planning is estimating

hardware and software requirements and available resources to determine the availability and suitability for investment applications.

Automated investment scheduling systems facilitate the production of initial investment staffing estimates and permit a regular review of staffing projections throughout the life cycle. Actual-to-estimated comparisons should be made and maintained, and forwarded to estimators to help improve estimating skills. Subsequent work includes refining the requirements, defining the solution, and confirming the investment management approach.

3.3.2 Perform System Security Planning and Security Risk Assessment

All Federal IT systems have some level of sensitivity and require protection from being accessed by unauthorized sources. As such, it is imperative, that System Security Plans (SSP)/Security Risk Assessments be developed to safeguard against any intrusions. The problem becomes even more acute if systems have multiple interfaces to other similar sensitive systems. SSP/Security RAs are living dynamic documents that are initiated in this phase and are updated through the life cycle process. SSP/Security RAs need to be updated every 3 years or when there is a significant change or modification to the system. Other activities that are done as part of the SSP/Security RA are defined in the DOL Computer Security Handbook as part of the SSP/Security RA and include:

- All systems need to be identified by unique DOL Identification Numbers.
- Personnel working on such systems need to be cleared to the appropriate level of the security classification of the system. This applies both to employees and contractor personnel.
- Ongoing regular training on the different aspects of security needs to be planned.
- Each page of the SSP/Security RA should be marked on the bottom, front of each page as Sensitive Information in bold font.
- Audit trails of transactions and documentation need to be established.
- Systems that are interconnected for sharing sensitive data/information need to have signed and approved Memorandums Of Understanding (MOU)/Agreements in place before establishing the interconnection. See OMB Circular A-130.
- A network diagram or schematic to help identify, define and clarify the system boundaries for the system and the interconnections to other networks (LAN/WAN) should be prepared and maintained.

Investment Teams should always refer to the DOL Computer Security Handbook and the OCIO Security Staff as the final say on security-related issues.

Deliverables:

System Security Plan (SSP) - During the Planning and Requirements Definition Phase, a formal plan detailing the types of computer security is required for any new system based on the type of information being processed and the degree of sensitivity. The system security plan should directly address any vulnerability identified in the security risk assessment. Systems that contain Privacy Act, personal and mission critical information will be more closely safeguarded than other systems.

Security Risk Assessment (RA) – Security risk assessment determines the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Security risk management is the process of identifying risk, assessing risk, and identifying the steps to reduce risk to an acceptable level. The objective of performing security risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed security risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management. Security risk assessments are performed early in the design of a system to indicate for what risks the engineers and managers should plan. The plans to counter the risks are identified in the system security plan discussed in the subsequent section. Security risk assessments conducted later in the development lifecycle ensure that the security controls implemented by following the system security plan are sufficient and identify additional potential risk areas.

3.3.3 Develop Security Plan of Action and Milestones (POA&M)

The purpose of the Security POA&M is to assist Agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. These weaknesses come from a variety of sources including, but not limited to, self-assessments, independent reviews, outside audits, and testing. To promote greater attention to security as a fundamental management priority, OMB continues to take steps to integrate security into the capital planning and budget process. This integration has produced tangible benefits by promoting security that comports with the Agency's enterprise architecture, supports business operations, and is funded within each information system over its life-cycle. During the Development and Test Phase, major security efforts can be tracked within a investment and subsequently updated in the Operational and Maintenance Phase.

Deliverable:

Security POA&M – Deliverable that documents security weaknesses, what will be done to correct or resolve them, and a timeline for when they will be resolved. This deliverable is initiated in the Planning & Requirements Phase but is updated throughout the investment life cycle.

3.3.4 Develop Data Architecture

During the Planning & Requirements Definition Phase, the investment team needs to define the data architecture including the data entities, attributes, assets, taxonomy, and relationships in support of the target IT investment business functions. In addition, the date exchanges between stakeholders (internal and external) and the associated data exchange mechanisms should be defined. Information flows should indicate where the information is needed and how information is shared to support mission functions.

Deliverable:

Investment Target Architecture including the Data Architecture – The Investment Target Architecture is updated to include the Data Architecture.

3.3.5 Identify the Acquisition Strategy and Develop the Acquisition Plan

The acquisition strategy describes the methods to be used in acquiring necessary hardware, software, telecommunication capabilities, and contractor support services. It promotes planning and verification that necessary resources will be available when needed. A milestone schedule emphasizes these issues. During this phase, as the details of the system are defined, resources that need to be acquired are identified. Upon completion of the formal budget process, purchase orders for all required hardware, software, and telecommunications equipment are submitted to the Agency's procurement organization.

Deliverable:

Acquisition Plan – The Acquisition Plan documents the acquisition strategy and procurement plan that will be implemented for the IT investment. The DOL OCIO has developed a detailed Acquisition Plan template as well as a guide to developing the Acquisition Plan to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the Acquisition Plan. A copy of the Acquisition Plan template can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area at http://labornet.dol.gov/itc/it/policyoversight/resource-lib.htm.

3.3.6 Analyze Functional Requirements

Requirements analysis and definition during this phase involves an iterative analysis of system-level requirements that are then defined in terms of high-level functional and data requirements. Documentation related to user requirements from the previous phase is used as the basis for further analysis and for the development of functional requirements. The system is defined in terms of functions to be performed. The requirements are defined to a level of detail sufficient for system design to proceed. During the Design Phase, these high-level functional requirements are further analyzed and defined in terms of detailed functional and data requirements that address data, system inputs, processes, outputs, interfaces (both internal and external), security, and maintainability aspects of the system.

In addition to analyzing functional requirements from a system's perspective, planners must be cognizant of additional considerations that must be addressed during the Planning and Requirements Definition Phase. Several references cited below are examples demonstrating that laws, regulations and policies may apply.

The Americans with Disabilities Act and Section 508 of the Rehabilitation Act require, regardless of the system development effort, that electronic and information technology allow individuals with disabilities to have appropriate access and use of information and data that is comparable to access and use of information and data by people who do not have a disability (P. L. 105-220). For additional information, see the Federal IT Accessibility IT investment at www.section508.gov.

Planners are also responsible for ensuring the privacy, confidentiality, integrity, and availability of citizen and employee information. The Department recognizes that privacy protection is both a personal and fundamental right of all citizens and employees. Among the most basic of citizens' and employees' rights is an expectation that DOL will protect the confidentiality of personal, financial, and employment information. Citizens and employees also have the right to expect that DOL will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out mission responsibilities. Several laws that are noted in the reference section of the SDLCM protect citizen and employee information.

Deliverables:

Functional Requirements Document (FRD) — The FRD is a formal statement of an application’s business requirements, and serves the same purpose as a contract. The developers agree to provide the capability specified and the client agrees to find the product satisfactory if it provides the specified capabilities. This document addresses the activities that need to be performed to analyze, understand, and review the overall architecture of the proposed system, the extent of interfaces with other existing internal/external systems or systems currently under development. In addition, activities may also relate to the high-level data and functional requirements, user organization definition, and the ability of existing system or data resources to satisfy system requirements.

Legacy Data Plan (Optional) - Sometimes the upgrading of a system or parts of a system will create legacy data, i.e., old data in a format that cannot be processed by the new system. The Legacy Data Plan identifies the time period covered by the data, volume of data, and where it resides. If some or all legacy data have already been converted to a new format, the approach to testing the converted data must be discussed. Requirements for processing legacy data in the future and plans for meeting those requirements are provided. It is acceptable to say that data will be converted if they are needed in the future, but information about what is required for the conversion process must be provided. This information includes a discussion of resource requirements for doing the conversion and potential problems that would need to be overcome.

3.3.7 Update Budget Documents

The budget request continues through the budget process during this phase. Several planning modifications may be required as part of the Departmental and OMB pass-back processes. Departmental IT Capital Planning approvals are required before proceeding with the Design phase. Contact OCIO Capital Planning Staff or the DOL Budget Office for specific guidance; refer to the integrated business process model for an overview of funding activities and outcomes.

3.3.8 Develop Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern and above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

3.3.9 Update Previous Phase Core & Optional Deliverables

As the IT investment progresses, active investment management results invariably in new product information (i.e. requirements creep, scope modifications, etc.). Any potential IT investment alterations require the update of relevant previous phase core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern) to reflect the new information. Deliverables are living documents that evolve throughout the life cycle and are updated, as needed, to reflect the current level of maturity of the investment.

3.3.10 QA Core & Optional Deliverables

The project manager is required to Quality Assurance check all investment deliverables. This includes maintaining an investment document library, utilizing eCPIC' resource library as the central repository for all appropriate investment planning and documentation deliverables.

3.3.11 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 2 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

3.4 Phase Considerations

The end of this phase is a critical juncture for the investment; it is the point at which agreements between the Project Manager and System Owner are made, to procure and scope the resources required for accomplishment of the remaining phases of the investment life cycle. These topics can be addressed by answering the following questions:

- What resources are needed for completion of the remaining phases of the Life Cycle?
- Are the requirements complete?
- Have the requirements been scoped accordingly and approved by the system owner?

4 DESIGN PHASE

4.1 Phase 3 Overview

Upon completion of the Planning and Requirements Definition Phase, the system progresses to the Design Phase. During this phase, functional requirements are translated into preliminary and detailed designs. Decisions are made to address how the system will meet functional, physical, interface, and data requirements. A preliminary (general) system design emphasizing the functional features of the system is produced as a high level guide. Then a final (detailed) system design is produced which expands the design by specifying all the technical detail needed to develop the system. Figure 6 identifies key activities and deliverables of this phase.

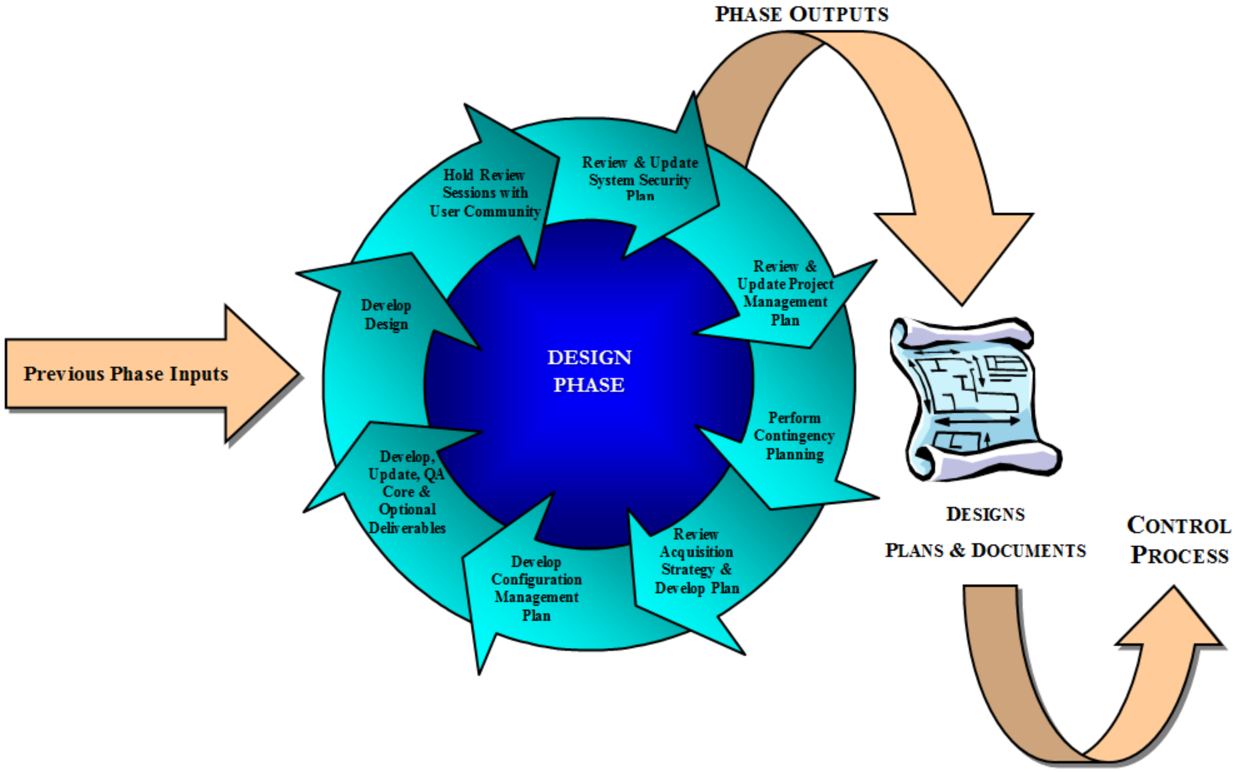
PHASE OUTPUTS
Hold Review Sessions with User Community
Review & Update System Security Plan
Develop Design
Review & Update Project Management Plan
Previous Phase Inputs
DESIGN PHASE
Perform Contingency Planning
Develop, Update, QA Core & Optional Deliverables
Develop Configuration Management Plan
Review Acquisition Strategy & Develop Plan
DESIGNS
PLANS & DOCUMENTS
CONTROL PROCESS

Figure 6: Design Phase Activities

4.2 Phase Inputs

The key inputs to the Design Phase are the core deliverables that were produced during the Planning and Requirements Definition Phase.

4.3 Phase Activities and Deliverables

4.3.1 Develop Application and Technical Architecture

The preliminary system design clarifies the general characteristics of the system. It specifies the operating system, architecture components, their timing and sizing, external and internal interfaces, subsystem inputs and outputs, administrative activities, security and auditing needs.

Deliverable:

> **Investment Target Architecture including the Application and Technical Architectures** – The Investment Target Architecture is updated to include the Application and Technical Architectures.

4.3.2 Develop Design

The preliminary system design clarifies the general characteristics of the system. It specifies the operating system, architecture components, their timing and sizing, external and internal interfaces, subsystem inputs and outputs, administrative activities, security and auditing needs.

The preliminary design is the foundation for the detailed design. System components are further specified into modules, processes, data, and interfaces and are defined to a level of detail that will enable a smooth transition to the Development and Test Phase. This top-down approach follows the structure previously set and adds substructure so that developers need minimal additional guidance. After the design review is completed, statutory or additional requirements may be identified that necessitate a revision to prior phase decisions or documents. Alternatively, these may lead to a new investment.

Deliverable:

> **Detailed Design –** The Detailed Design is documented in this deliverable. Subsystems may be further subdivided and described using charts and pseudo code. Logic specifications are given and data usage is defined in detail. User input and user approvals are spelled out. It includes detailed system requirements used to develop the system. Changes to the detailed design due to changes in the preliminary design may create additional costs and delays that may require revisions to the schedules set in the Project Management Plan.

4.3.3 Hold Review Sessions with User Community

As the design is initiated, participation from the user community through review sessions is essential to ensure that the requirements and the design will be consistent with the new or enhanced business requirements.

4.3.4 Review and Update System Security Plan

The application/system developer should identify specific security requirements, allocate them to specific modules in the design, and update the System Security Plan, as needed to reflect any changes. For example, if a requirement exists to audit a specific set of user actions, the developer may have to add a workflow module into the design to accomplish the auditing.

4.3.5 Review and Update Project Management Plan

As tasks are completed in this phase, the investment manager will update the Project Management Plan as needed. Investment planning information, such as the WBS, schedules, resources, and investment tools and methodologies are updated to reflect changes in approaches and decisions. The WBS is a key component of the investment PMP. It is a core requirement in the first phase, Conceptual Planning, and is required to be reviewed and expanded as necessary at least annually, as part of the annual budget preparation and approval process, for the remaining SDLCM phases.

4.3.6 Perform Contingency Planning

The objective of contingency planning is to ensure that DOL systems are able to recover from processing disruptions in case of localized emergencies or large-scale disasters. An emergency response plan, developed in conjunction with the System Owner and maintained at the primary and backup computer installations, ensures that reasonable continuity of support is provided if events occur that prohibit normal operations. Contingency Plans must be routinely reviewed, updated, and tested through subsequent phases to ensure vital operations and resources can be restored as quickly as possible keeping system downtime to an absolute minimum.

Deliverable:

> **Contingency Plan –** The contingency plan is developed in conjunction with application owners and maintained at the primary and backup computer installation. Developed during the Design Phase, contingency planning ensures that DOL systems can recover from processing disruptions, no matter what the source.

4.3.7 Develop Configuration Management Plan

Systematic control of revisions is necessary to enable reproduction of past results from a version control effort. This deliverable is optional in the prior Planning and Requirements Definition Phase and becomes a core deliverable in the Design Phase.

Deliverable:

> **Configuration Management (CM) Plan –** This plan identifies the automated CM system to be used for software development (version control) and documents other items to be placed under control, with methods of control. Locations where items are stored (the library) are specified and plans for audits are specified.

4.3.8 Develop, Update, QA Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern and above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

As the IT investment progresses, active investment management results invariably in new product information (i.e. requirements creep, scope modifications, etc.). Any potential IT investment alterations require the update of relevant previous phase core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern) to reflect the new information. Deliverables are living documents that evolve throughout the life cycle and are updated, as needed, to reflect the current level of maturity of the investment.

The project manager is required to Quality Assurance check all investment deliverables. This includes maintaining a investment document library, utilizing eCPIC' resource library as the central repository for all appropriate investment planning and documentation deliverables.

4.3.9 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 3 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

4.4 Phase Considerations

Key considerations during this phase may address the following questions:

- Has a sufficient dialog occurred with the designated future users to document their needs before writing the preliminary design?
- Have all investment stakeholders reviewed the final design to ensure incorporation of all requirements and design considerations?
- Has a investment team Peer Review been conducted for both the preliminary and detailed designs?

- Has proper funding been allocated to continue the implementation of the investment?

- Have all significant risks been identified and documented?

- Has a Configuration Management Plan that will track, modify, and update software development entities been developed, including version control procedures and a central library?

- Have new management, risk, and security considerations been documented in light of new understandings flowing from the growth or subsequent iterations of the investment?

- Were statutory requirements (i.e. accessibility) met?

5 DEVELOPMENT AND TEST PHASE

5.1 Phase 4 Overview

During the Development and Test Phase, executable software is developed from detailed design specifications. The system is validated through a sequence of unit, integration, system, and acceptance test activities. The objective is to ensure the system functions as expected and user requirements are satisfied. Large systems are solicited, awarded, and managed in accordance with the Acquisition Plan. All hardware, system software, communications, applications, procedures, and associated documentation are developed/acquired, tested, and integrated. This phase requires strong user participation in order to verify that all requirements have been thoroughly tested and meet all business needs. Figure 7 identifies key activities and deliverables of this phase.

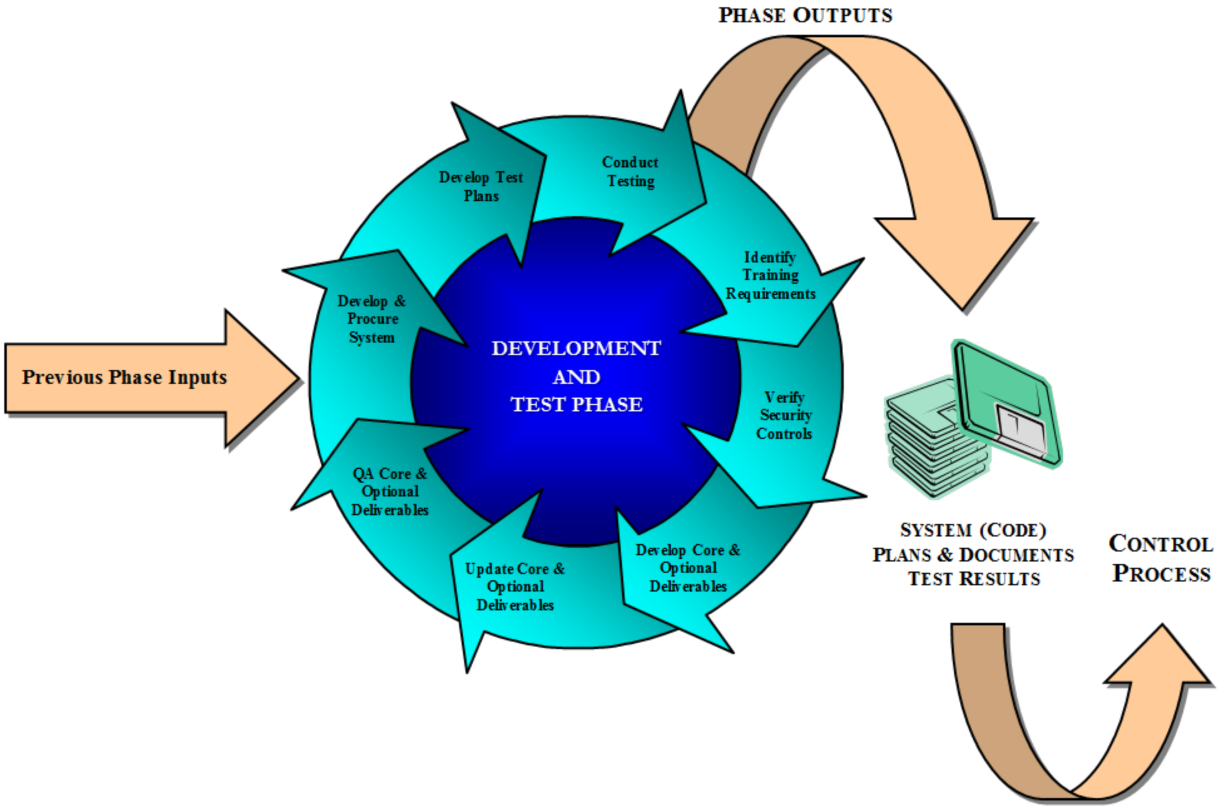

Figure 7: Development and Test Phase Activities

5.2 Phase Inputs

The key inputs to the Development and Test Phase are the core deliverables produced during the Design Phase.

5.3 Phase Activities and Deliverables

5.3.1 Develop and Procure System

Obtain hardware, software and other required resources. Develop the system. Identifying personnel assigned to the investment, generate code, compile and link it, perform unit testing in accordance with the development approach and standards defined in the Project Management Plan. Methods specified in the Configuration Management Plan are utilized to ensure system versions and changes are managed and tracked. Items to be procured include those for both the development and production environment. They are procured, as needed in accordance with the process defined in the Acquisition Plan.

Deliverables:

Implementation Plan - Drawing on prior documents, this plan describes a plan for implementing the system in the operational environment. It translates business needs into key activities (i.e. installation, training, verification, monitoring); specifies an implementation schedule; and identifies specific personnel, hardware, software and site requirements. It includes back-off plans for use when necessary. If a preliminary Implementation has already been produced in prior phases, it is finalized in this as the implementation details become better defined.

5.3.2 Develop Test Plans and Conduct Testing

Testing activities are planned and documented and may include test cases, test scripts, and test scenarios. Test Plans are documented at varying levels, as appropriate, to validate the detailed requirements defined in the Design Phase and functional requirements defined in the Planning and Requirements Definition Phase. Test Plans are the basis for performing integration, system, and acceptance testing activities that occur later in this phase. Test Plans must be kept consistent with the methods and schedules specified in the Project Management Plan and Implementation Plan.

Unit testing usually occurs in conjunction with module development. Individual software modules are executed and tested in a controlled environment (i.e. test data and simulated software). The software modules are validated to ensure they yield the correct results given a range of valid and invalid inputs. Upon successful completion of unit testing, testing activities advance to the next stage - integration tests.

Integration testing is conducted in accordance to previously documented integration test plans and procedures. The objective is to validate that integrated program components, or modules, function properly and yield expected results. In a large system, modules are typically combined into logical functional groupings called subsystems and tested at this level. Upon successful completion of integration testing, testing activities advance to the next stage - system testing.

System testing is conducted in accordance to previously documented system test plans. The objective is to combine all the system components (i.e. subsystems), validate that the system functions properly and meets all technical, performance, and interface requirements. Systems are tested in realistic conditions having changing and competing priorities.

Acceptance testing is conducted in accordance with the Acceptance Test Plan finalized earlier in this phase. Users participate in acceptance testing to confirm that the developed system meets all user requirements identified in the Planning Requirements and Definition Phase. Acceptance testing is conducted in a simulated "real" user environment using simulated or real target platforms and infrastructures. Acceptance test results are documented in an Acceptance Test Report. Upon completion of acceptance testing, the approving authority verifies that the test results have been reviewed and that testing was successfully completed.

Deliverables:

Test Plan(s) – This plan documents the test environment, resources, training, methods, schedules, evaluation, and test descriptions for: unit, integration and system test activities. Test plan development is optional for the prior Planning and Requirements and Design Phases. However, in this phase, the Test Plan is a core deliverable because a testing approach is required to be established before test execution can take place.

Acceptance Test Plan - This plan documents the scope, content, methodology, sequence, management, and responsibilities for acceptance test activities. It ensures that all aspects of the system are adequately tested against requirements.

Acceptance Test Report and Approval - Documents software testing as defined in the Acceptance Test Plan. A summary of test results documenting problems encountered during testing is attached to this report as appropriate.

5.3.3 Identify Training Requirements

Training activities are planned and documented and include a training schedule, class outline, class descriptions, training materials, resources and facility requirements, and identification of the target audience. Training materials and classes are planned and coordinated with the System Owner and user community to ensure that appropriate personnel are trained on new systems or capabilities.

Deliverables:

Training Plan - Outlines the objectives, needs, strategy, and curriculum to be addressed for training users on the new or enhanced information system. The plan presents the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks. Training activities are conducted in accordance with the Training Plan to teach users how to operate the system.

System Manuals - Includes documents providing information to describe the design, development, production, distribution, operation, maintenance, and management of the system and are produced as needed to meet specific investment needs. System manuals are produced during this phase and updated as needed during the Operations and Maintenance Phase to reflect changes or enhancements.

User Manuals – Document instructions, guidance, and reference information relating to user execution of the system. User manuals are produced during this phase and updated as needed during the Operations and Maintenance Phase to reflect changes or enhancements to the system.

5.3.4 Verify Security Controls

Before a system can be certified and accredited, security controls are required to be tested to uncover all design and implementation flaws that could violate Departmental security policy. Performing a Security Test and Evaluation (ST&E) involves determining a system's security mechanisms adequacy for completeness and correctness, and the degree of consistency between system documentation and actual implementation. During the Development and Test Phase this is accomplished through a variety of assurance methods such as analysis of system design documentation, inspection of test documentation, and independent execution of function testing and penetration testing. Results of the ST&E effect security activities developed earlier in the life cycle such as the security risk assessment, system security plan, and contingency plan. Each of these activities will be updated in the Development and Test Phase based on the results of the ST&E.

Deliverable:

Security Control Assessment Aid/ Security Test & Evaluation (ST&E) Report - The security controls assessment (SCA) of the full set of security controls performed in support of the certification and accreditation (C&A) process is an important step in ensuring the security of an information system. This assessment occurs at a single point in time. Deliverable: (1) Security Test and Evaluation (ST&E) Report; Computer Security Handbook (CSH) Volume 6 and (2) Security Self- Assessment, Security Control Assessment Aid (SCAA). (Source: Computer Security Handbook (CSH) Volume 4.)

Security Certification Package (prerequisites) - The certification process includes completing a Security Risk Assessment, System Security Plan, Security Test and Evaluation, and Certification Statement. Only when these items have been completed can the system be accredited. The accreditation occurs during the Implementation Phase, and requires preparation and coordination with the OCIO Security Office during the Development and Test Phase. Please refer to the DOL Computer Security Handbook for specific templates and guidance.

5.3.5 Develop Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern and above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

5.3.6 Update Previous Phase Core & Optional Deliverables

As the IT investment progresses, active investment management results invariably in new product information (i.e. requirements creep, scope modifications, etc.). Any potential IT investment alterations require the update of relevant previous phase core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern) to reflect the new information. Deliverables are living documents that evolve throughout the life cycle and are updated, as needed, to reflect the current level of maturity of the investment.

5.3.7 QA Core & Optional Deliverables

The project manager is required to Quality Assurance check all investment deliverables. This includes maintaining a investment document library, utilizing eCPIC' resource library as the central repository for all appropriate investment planning and documentation deliverables.

5.3.8 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 4 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

5.4 Phase Considerations

Key considerations during this phase may address the following questions:

- ➢ Has the newly developed/enhanced system undergone code, testing, peer and/or quality reviews?

- ➢ Have the appropriate parties formally accepted the newly developed system or enhancement?

- Has proper funding been allocated to continue through the remainder of the SDLCM?

- Did the test team document any discrepancies that existed in the original specifications?

Problems or new information identified in this phase may require changes to products developed in earlier phases. If this is the case, is an alternate approach necessary and/or is the investment ready to proceed (i.e. go/no-go decision may be required)?

6 IMPLEMENTATION PHASE

6.1 Phase 5 Overview

During the Implementation Phase, the new or enhanced system is installed in the production environment, users are trained, data is converted (as needed), and the system is turned over to the user. This phase includes efforts required to implement the system as well as to resolve any problems identified during the implementation process. Figure 8 identifies key activities and deliverables of the Implementation Phase.

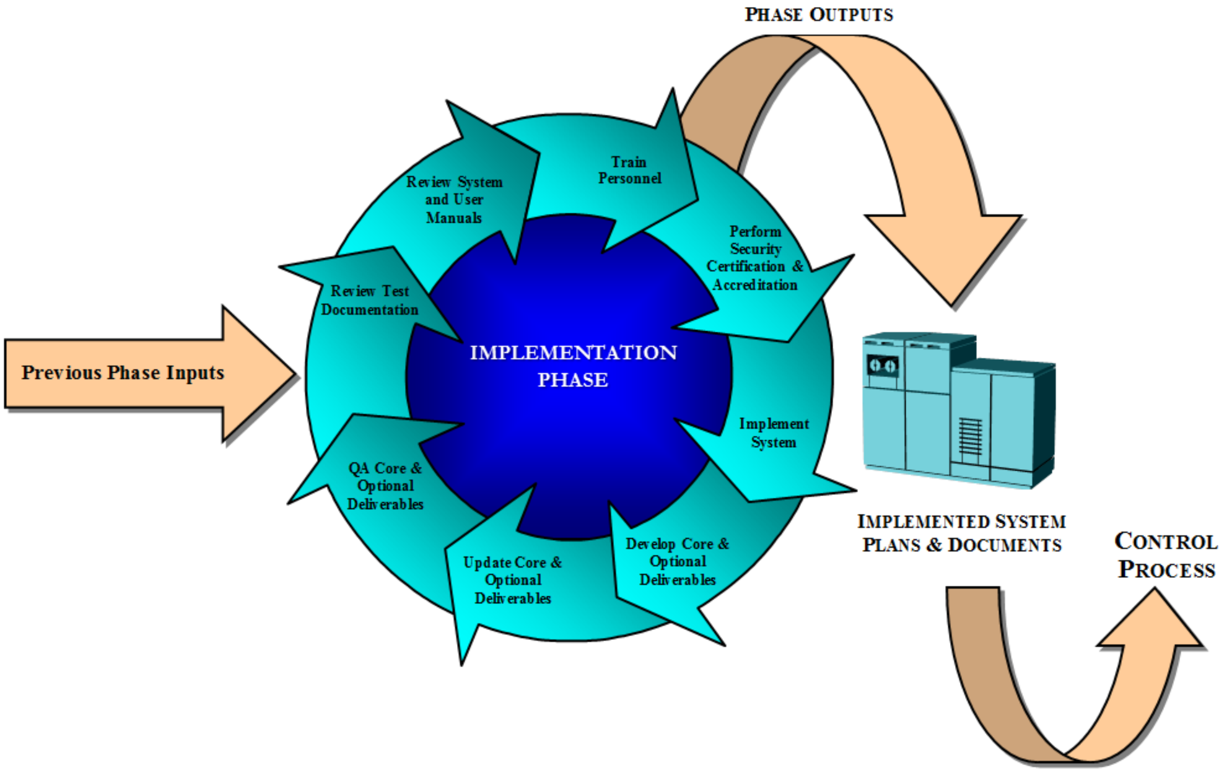
PHASE OUTPUTS
Previous Phase Inputs
IMPLEMENTATION PHASE
Train Personnel
Perform Security Certification & Accreditation
Implement System
Develop Core & Optional Deliverables
Update Core & Optional Deliverables
QA Core & Optional Deliverables
Review Test Documentation
Review System and User Manuals
IMPLEMENTED SYSTEM PLANS & DOCUMENTS
CONTROL PROCESS

Figure 8: Implementation Phase Activities

6.2 Phase Inputs

The essential inputs to the Implementation Phase are the core deliverables that were produced during the Development and Test Phase.

6.3 Phase Activities and Deliverables

6.3.1 Review Test Documentation

All test plans, test cases and test results produced during the Development and Test Phase, including those for acceptance testing, is reviewed for completeness during this phase. Some sample testing of the tests conducted in the previous phase may be conducted for purposes of validating system operability once the system is installed.

6.3.2 Review System and User Manuals

System and user manuals developed or updated during the Development and Test Phase are reviewed for accuracy and completeness and updated, as needed. Changes are incorporated to reflect modifications or enhancements that have been incorporated. Additional detail is incorporated to reflect the availability of new information.

6.3.3 Train Personnel

Users and operations personnel are trained during this phase in accordance with the processes established in the Training Plan. The purpose is to fully acquaint personnel with the system and equip them for operating the system effectively and efficiently. System and user manuals developed during the previous phase are utilized during the training sessions.

6.3.4 Certify and Accredit System

The security certification and accreditation process is intended to provide direct management oversight into the decision to operate a system within a given risk profile. This process gathers together developers, operators, management, and executive leadership to ensure the function and adequacy of security controls and accept responsibility for the system's operation. During the Implementation phase, the system is certified through a process that includes completing and submitting a Security Certification Package. Only when these items have been completed can the system be accredited and move into production.

Computer Security Accreditation is defined as a "formal declaration by an accrediting authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards." The Designated Accrediting Authority (DAA) may be a senior manager of DOL or from within the Agency. The DAA will determine, based on the remaining residual risk, if the system is operating in the best interest of DOL/Agency. After ensuring that all needs have been fulfilled, Computer Security Accreditation or an interim Authority To Operate (ATO) is granted.

Deliverables:

Security Certification Package – The certification process prerequisites include completing a Security Risk Assessment, System Security Plan and Security Test and Evaluation. Once complete, the following four documents must be prepared and submitted to the Agency Computer Security Officer for review and approval:

- **Memorandum Stating Completion of Security Activities**
- **Computer Security Certification Statement**
- **Summary of Compliance**
- **Statement of Residual Risk**

They are then submitted to the designated approval authority within the Office of the Chief Information Officer. Please refer to the DOL Computer Security Handbook and work with the OCIO Security Officer for the latest templates, guidance and directions.

Accreditation:

Security Accreditation Letter- Upon completion of the Security Certification, the certification package and Security Accreditation Letter are submitted by the OCIO Program Manager to the DAA for review and approval. Accreditation can provide a short-term interim authority to operate while the system owner clears up specific vulnerabilities, or it can provide a longer-term ATO if the vulnerabilities identified do not present sufficient risk to warrant ongoing attention.

6.3.5 Implement System

The Implementation plan, developed in the previous phase is reviewed. The investment team will incorporate changes as needed and conduct a final system review. As the system is installed in the production environment, data is converted as needed, and sample testing is conducted to verify that the system operates correctly. System and user documentation is reproduced and distributed to appropriate personnel. An Implementation Certification is signed by the Project Manager and the System Owner to confirm that the system has been successfully implemented according to documented plans and procedures.

Successful implementation is ensured when known deficiencies and requirements are addressed and resolved before system implementation. Modifications made to the system both before and during implementation should be documented and provided to system users, operators, and other affected personnel. At the end of this phase, the product baseline (consisting of the production system, database(s), an updated data dictionary, and supporting documentation) is established and archived. Implementation deliverable descriptions follow.

Deliverables:

System Acceptance Letter - This letter is signed by the Project Manager and the System Owner and verifies that the system has been successfully implemented according to documented plans and procedures.

6.3.6 Develop Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern and above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

6.3.7 Update Previous Phase Core & Optional Deliverables

As the IT investment progresses, active investment management results invariably in new product information (i.e. requirements creep, scope modifications, etc.). Any potential IT investment alterations require the update of relevant previous phase core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern) to reflect the new information. Deliverables are living documents that evolve throughout the life cycle and are updated, as needed, to reflect the current level of maturity of the investment.

6.3.8 QA Core & Optional Deliverables

The project manager is required to Quality Assurance check all investment deliverables. This includes maintaining a investment document library, utilizing eCPIC' resource library as the central repository for all appropriate investment planning and documentation deliverables.

6.3.9 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 5 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

6.4 Phase Considerations

A number of investment related decisions are made in this phase that may address the following questions:

- ➢ What changes are necessary to complete the system implementation?
- ➢ Is a process in place to allow for continued upgrade decisions (i.e. a change management board) such as:
  - ➢ What upgrades are required to address new or changing requirements?

- What approvals are necessary to undertake the change?
- Are the appropriate resources and sufficient funding available to support approved system changes, upgrades, and new requirements?

7 OPERATIONS AND MAINTENANCE PHASE

7.1 Phase 6 Overview

Once a system becomes operational, it moves to the Operations and Maintenance Phase. The emphasis of this phase is to ensure that user needs continue to be met and that the system continues to perform according to specifications. Routine hardware and software maintenance and upgrades are performed to ensure effective system operations. User training continues during this phase as needed to acquaint new users to the system or to introduce new features to the current users. Additional user support is provided as an ongoing activity to help resolve reported problems. This phase continues until the system is retired. Figure 9 identifies key activities and deliverables of this phase.

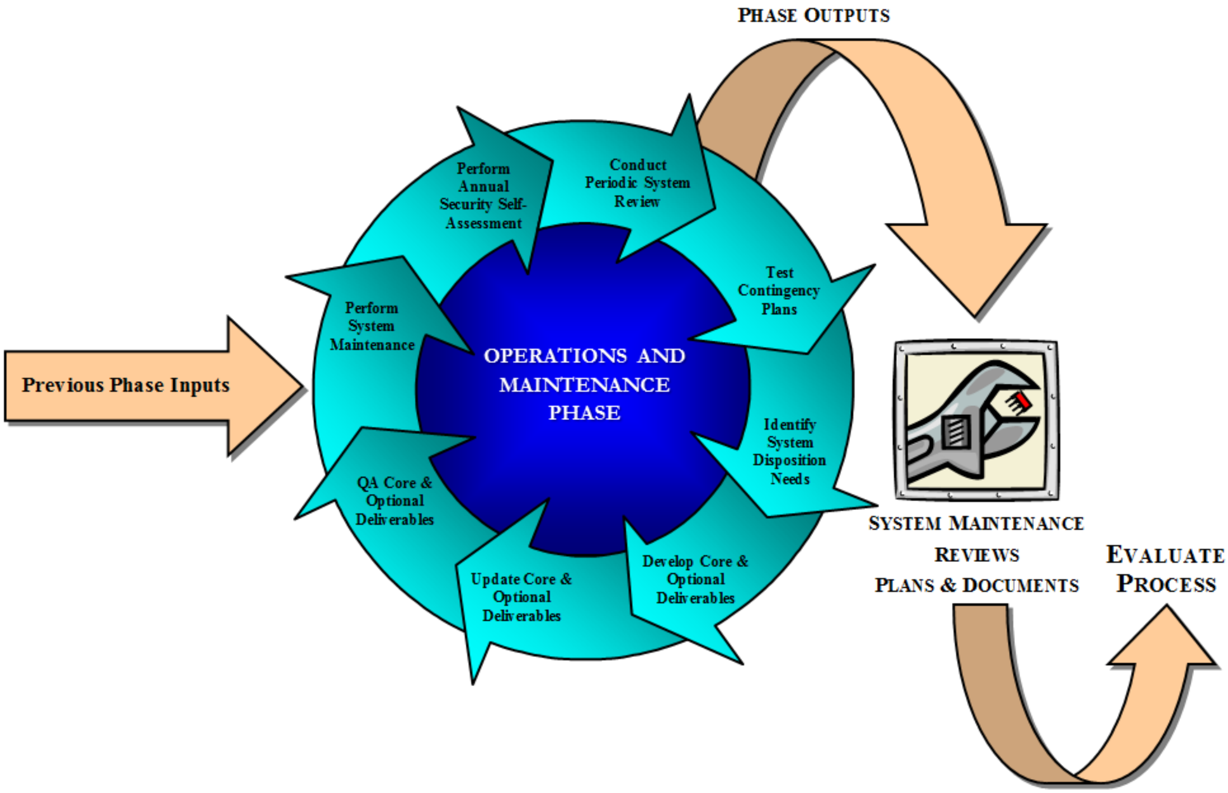
PHASE OUTPUTS
Previous Phase Inputs
OPERATIONS AND MAINTENANCE PHASE
Perform Annual Security Self-Assessment
Conduct Periodic System Review
Test Contingency Plans
Identify System Disposition Needs
Develop Core & Optional Deliverables
Update Core & Optional Deliverables
QA Core & Optional Deliverables
Perform System Maintenance
SYSTEM MAINTENANCE
REVIEWS
PLANS & DOCUMENTS
EVALUATE PROCESS

Figure 9: Operations and Maintenance Phase Activities

7.2 Phase Inputs

The essential inputs to the Operations and Maintenance Phase are the core deliverables that were produced during the Implementation Phase. The critical approvals required to move into O&M are: the Agency Computer Security Certification signed off by the Project Manager and the System Owner, a Security Accreditation letter signed off by the Designated Accreditation Authority and an Implementation Certification Statement signed by the system owner.

7.3 Phase Activities and Deliverables

7.3.1 Perform System Maintenance

All deliverable documents produced in prior phases are turned over to system administrators, maintainers, and support personnel. Documentation is updated as needed utilizing established configuration management and control processes as system changes are incorporated.

System Maintenance encompasses a wide gamut of activities including routine activities such as backing up data and program files and upgrading/replacing hardware/software systems, application software, and vendor supplied COTS packages. Maintenance activities also involve fixing previously undetected errors. Various reviews may be conducted during this phase to gather important information used to assess continued use of the system, to evaluate additional enhancements, and to obtain user comments.

Maintenance personnel determine if modifications to the system and databases are needed to resolve errors, enhance system performance, or to provide new capabilities. New capabilities may take the form of routine maintenance or constitute enhancements to the system or database in response to user requests for new or improved capabilities. The Project Charter is the mechanism used to identify a need or opportunity to enhance a system or fix previously undetected errors.

Proposed changes are reviewed and approved by the appropriate review authority (as per the DOL Guide to IT Capital Investment Management) before implementation. Major system modifications or enhancements that are needed after the system has been implemented will follow the life cycle process from planning through implementation as appropriate. In this case a Project Management Plan including a Project Charter is updated or developed to identify needed modifications to the existing system and related documentation. The appropriate reviews and testing are conducted based on the scope of the modification. The maintenance manual is updated as needed to document approved changes to the system.

7.3.2 Perform Annual Security Self-Assessment

Periodically (normally on an annual basis), system owners and IT managers are required to perform security self-assessments to ensure that their systems are in compliance with the latest requirements and synchronized with the most up-to-date security practices. Furthermore, self-assessments provide a mechanism to ensure that all requisite security documentation has been completed and updated with the latest system changes (see the DOL Security Handbook for requirements). Computer and telecommunications security awareness training is provided to all personnel having access to DOL IT systems. The project manager must also ensure that security operating procedures are kept up to date.

7.3.3 Conduct an Operational Analysis

An OA is an OMB Circular A-11, Part 7 required IT investment performance based management process that is to be conducted at least annually by all DOL Major IT investments that are in the operations and maintenance (O&M) phase (i.e., Steady State). An operational analysis is also required by the O&M elements of “mixed life cycle” IT investments. That is IT investments that have Development, Modernization, and Enhancement (DME) activities and O&M elements occurring at the same time. The operational components of the mixed life cycle investment are required to conduct an Operational Analysis.

An operational analysis provides decision makers timely and accurate information on the performance and any performance gaps of an IT investment. It helps determine whether an IT investment or asset is continuing to meet its planned objectives as well as the current needs of its users, customers, owners, stakeholders, and/or sponsors. The result or output of an Operational Analysis is a recommendation regarding the future operational status of an IT investment or asset. For example, it may be determined that an operational IT investment should be:

- Maintained “as is” without any changes,
- Modified (i.e., requiring operational changes that do not result in any new DME activities),
- Enhanced (i.e., requiring new DME activities),
- Replaced (i.e., decommissioned in a planned manner and replaced with a new capital asset), or
- Terminated (i.e., decommissioned in a planned manner with no replacement)

Depending on the results of the Operational Analysis, an updated or new investment CBA may need to be completed in the O&M Phase to justify for example, an enhancement or a even a replacement investment.

The Operational Analysis process implemented by an IT investment or asset (including any associated documentation) should be commensurate with the size and scope of the IT investment and associated documentation should be as detailed as necessary to support (i.e., justify and substantiate) the conclusion and/or recommendations regarding the future operational status of the IT investment or asset.

The DOL OCIO has developed an OA template within the eCPIC tool as well as a standalone OA Worksheet Guide to support IT investments in the development of their OA. A copy of the OA Worksheet Guide can be found in the OCIO Resource Library under the CPIC subject area.

7.3.4 Test Contingency Plans

Contingency plan(s) are tested during this phase. To the extent possible, all testing should be conducted using simulations of actual conditions. Problems noticed during testing along with optimum solutions should be discussed and disseminated to appropriate parties as “Lessons Learned”. Contingency Plan(s) testing should be done at regular periodic intervals to create and maintain a sense of awareness and preparedness among Agency personnel of likely calamities that could occur.

7.3.5 Identify System Disposition Needs

Since the normal life cycle of an IT system is usually several years, disposition planning may not occur until the end of this phase (i.e., when a decision has been made to retire the IT system).

However, if the system processes sensitive data and interfaces with other IT systems, it is advantageous to identify and document the system Disposition Plan and associated impacts in the early stages of the life cycle. This will ease the effort later in this phase when the final Disposition Plan is prepared.

Deliverables:

Disposition Plan – The objective of the Disposition Plan deliverable is to state the approach and processes for disposing of a system in a planned orderly manner and to ensure that the system is properly archived or incorporated into other systems. The Disposition Plan is initiated (or updated, as needed, if it already exists) in this phase. It is finalized once a decision has been made to retire the system, which may not occur until later in the phase. The plan addresses all facets of archiving, transferring, and disposing of the system and the data. Particular emphasis is given to proper preservation of the data processed by the system so that it can be effectively migrated to another system or archived and restored in accordance with applicable record management regulations and policies.

7.3.6 Develop Core & Optional Deliverables

If the investment is a new IT development effort, core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern and above) are initiated during this phase and are subsequently updated in later phases, as appropriate. If the investment represents a modification or enhancement to an existing system, then the existing core and optional documents are updated as appropriate. Specific deliverable templates are required and can be referenced in the appendix.

7.3.7 Update Previous Phase Core & Optional Deliverables

As the IT investment progresses, active investment management results invariably in new product information (i.e. requirements creep, scope modifications, etc.). Any potential IT investment alterations require the update of relevant previous phase core and optional deliverables (as referenced from the appropriate IT Investment Management Work Pattern) to reflect the new information. Deliverables are living documents that evolve throughout the life cycle and are updated, as needed, to reflect the current level of maturity of the investment.

Deliverables:

Plan of Action and Milestones – Maintain the current status of corrective actions and provide quarterly reports to OCIO Security.

7.3.8 QA Core & Optional Deliverables

The project manager is required to Quality Assurance check all investment deliverables. This includes maintaining an investment document library and utilizing the eCPIC resource library as the central repository for all appropriate investment planning and documentation deliverables.

7.3.9 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 6 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

7.4 Phase Considerations

Key investment approach considerations during this phase may address the following questions:

- How should the evaluation of the system/data be conducted?
- What new or additional user support activities are needed?
- What improvements in system/data functionality, quality, and performance are required?
- What adjustments are needed to the current system/data management procedures?

Investment execution considerations include planning the required changes or enhancements to the system and determining if a particular enhancement should be implemented during this phase or cycled back through the SDLCM as a Project Charter. These can be addressed by obtaining an answer to the following question:

- Does this change/enhancement need to be implemented during this phase or be cycled back through the SDLCM as a Request for Information Technology Service (RITS)?

Planning now begins for the preservation of data in accordance with the records management and property disposal requirements of the Agency. This will include archiving/converting of the data to suit the new environment and eventual archiving of the software. The system planning activities preserve information about the current production system and the evolution of the system through its life cycle. The following question can be asked:

- Is a records management and property disposal process defined to address archiving/conversion of software/data and disposal of hardware for the system under retirement?

8 DISPOSITION PHASE

8.1 Phase 7 Overview

The Disposition Phase represents the end of the systems life cycle. It provides for the systematic termination of a system to ensure that vital information is preserved for potential future access and/or reactivation. The system, when placed in the Disposition Phase, has been declared surplus and/or obsolete, and is scheduled to be shut down. The emphasis of this phase is to ensure that the system (e.g. software, data, procedures, and documentation) is packaged and archived in an orderly fashion, enabling the system to be reinstalled later if desired. System records are retained in accordance with DOL policies regarding retention of electronic records. Figure 10 identifies key activities and deliverables of the Disposition Phase.

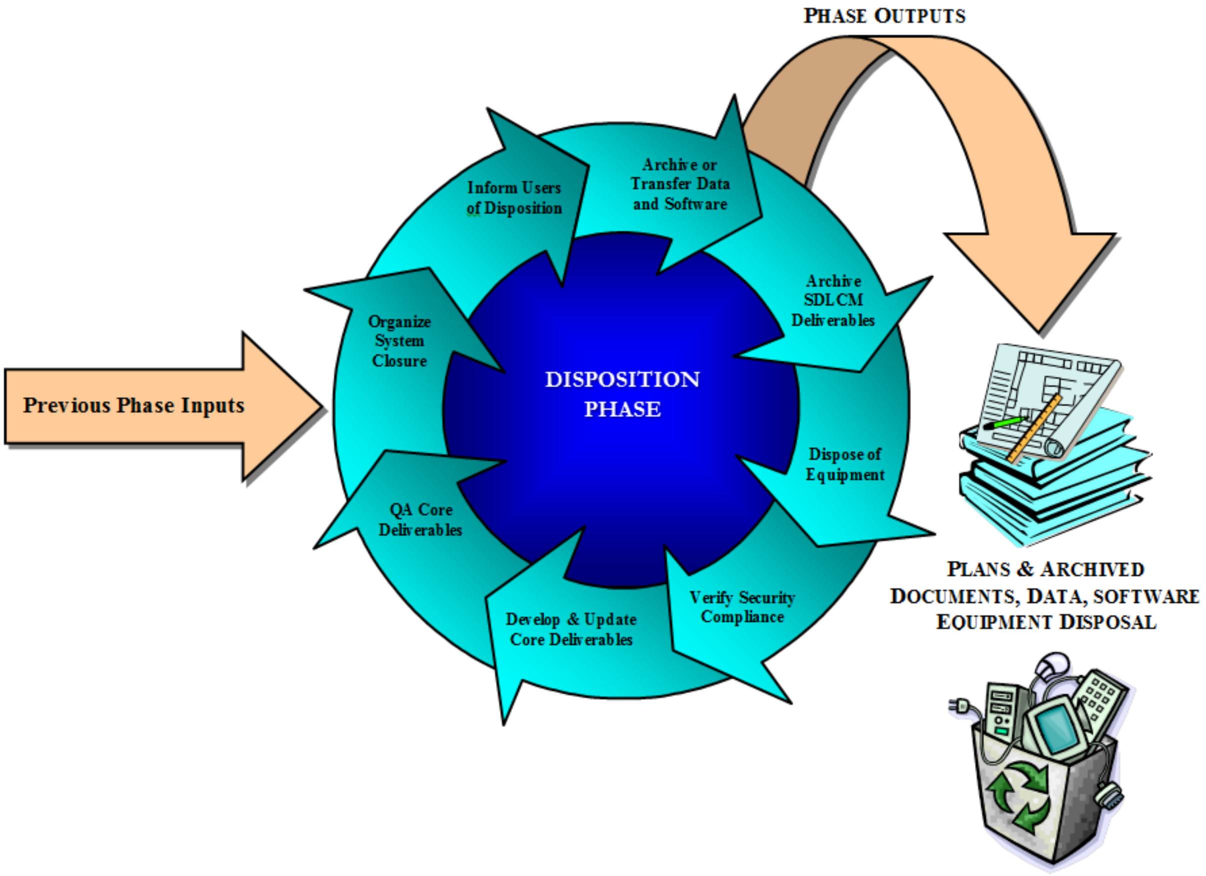
PHASE OUTPUTS
Previous Phase Inputs
DISPOSITION PHASE
Inform Users of Disposition
Archive or Transfer Data and Software
Archive SDLCM Deliverables
Dispose of Equipment
Verify Security Compliance
Develop & Update Core Deliverables
QA Core Deliverables
Organize System Closure
PLANS & ARCHIVED DOCUMENTS, DATA, SOFTWARE EQUIPMENT DISPOSAL

Figure 10: Disposition Phase Activities

8.2 Phase Inputs

The key input to this phase is the Disposition Plan produced during the O&M Phase. The Disposition Plan is executed during this phase and the system is retired in accordance with documented processes.

8.3 Phase Activities and Deliverables

8.3.1 Organize System Closure

Initial disposition planning activities specified in the Disposition Plan are initiated. The schedule for system disposal is finalized and coordinated with involved parties. Specific activities for proceeding are defined and may include: identifying the software components to be preserved; identifying the data to be preserved; determining how the remaining equipment will be disposed of; and identifying what support life cycle products should be archived and the method for doing so.

8.3.2 Inform Users of Disposition

Users, operators, and maintainers of the system are notified of the plans for disposing the system. Ample time must be permitted for users to produce needed reports and/or archive specific information they may need to support their work activities.

8.3.3 Archive or Transfer Data and Software

Copies of code and data are archived to a designated environment specified in the Disposition Plan. Related system build, installation, and set-up scripts are archived so that the system may be reinstalled later. The system disposition activities preserve information not only about the current production system, but also about the evolution of the system through its life cycle.

8.3.4 Archive SDLCM Deliverables

SDLCM life cycle documentation or deliverables are archived for future reference. This includes development information (i.e. requirements, design, and testing documents), planning information (i.e. implementation, risk management, implementation, disposition, and training plans), and information specifying how to use and operate the system (i.e. user and system manuals).

Deliverable:

> **Archived System** - The only deliverable of the Disposition Phase is a system that has been archived in accordance with the procedures set forth in the Disposition Plan. The archived system is comprised of the packaged set of software, data, procedures, and documentation associated with the archived application.

8.3.5 Dispose of Equipment

Retirement of IT systems may result in obsolete or excess equipment that needs to be either disposed of or reallocated. Excess inventory is disposed of or reallocated as needed, in accordance with DOL policies and procedures.

8.3.6 Verify Security Compliance

As specified in the DOL Computer Security Handbook, the retirement of classified systems requires that documentation, software, and data be archived with appropriate security classifications. A determination needs to be made regarding how and when the termination of the system/data should be conducted.

8.3.7 Develop & Update Core Deliverables

If the investment is a new IT development effort, the Disposition Plan is updated as required and the Archived System is organized for system closure in accordance with documented plans and procedures. If the investment represents a modification or enhancement to an existing system, then the existing core documents are updated as appropriate.

8.3.8 QA Core Deliverables

The project manager is required to Quality Assurance check the final investment deliverables (the archived system). This includes ensuring the investment document library, software, and data is maintained as a historical archive in a central repository in accordance with Records Management policy.

8.3.9 Phase Gate Review

A phase gate review determines whether all of the requirements of the phase have been accomplished and whether the IT investment is prepared to move on to the next phase as per the SDLCM.

The phase gate review is conducted by the IT Investment PM, PMO, and/or IPT and involves all contractor teams supporting the IT investment.

The DOL OCIO has developed a Phase 7 - Phase Gate Review Checklist to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the phase gate review. The OCIO may request a copy of the checklist to confirm and/or ensure the phase gate review has occurred. The checklists should be enhanced by the PM and/or PMO/IPT to include or incorporate IT investment requirements or deliverables that are not currently on the checklist and/or are unique to the IT investment. For example, software development life cycle related deliverables or artifacts that are required may not appear on the checklist. Hence, the checklist should be updated to include all IT investment phase related deliverables. A copy of the Phase Gate Review Checklists can be found in Appendix VII.

8.4 Phase Considerations

Key considerations during this phase may address the following questions:

- Have all current and potential future users of the system been notified of the archiving plan?

- Have all necessary code, data, and documentation been located?

- Is the means of preservation of the materials and their location considered secure?

- Will instructions for regeneration of the system be easy to find and understand?

APPENDIX I – 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 11**,** 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 superceded 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 11: Iterative/Incremental SW Development Model Integrated with DOL SDLCM and CPIC Life Cycles

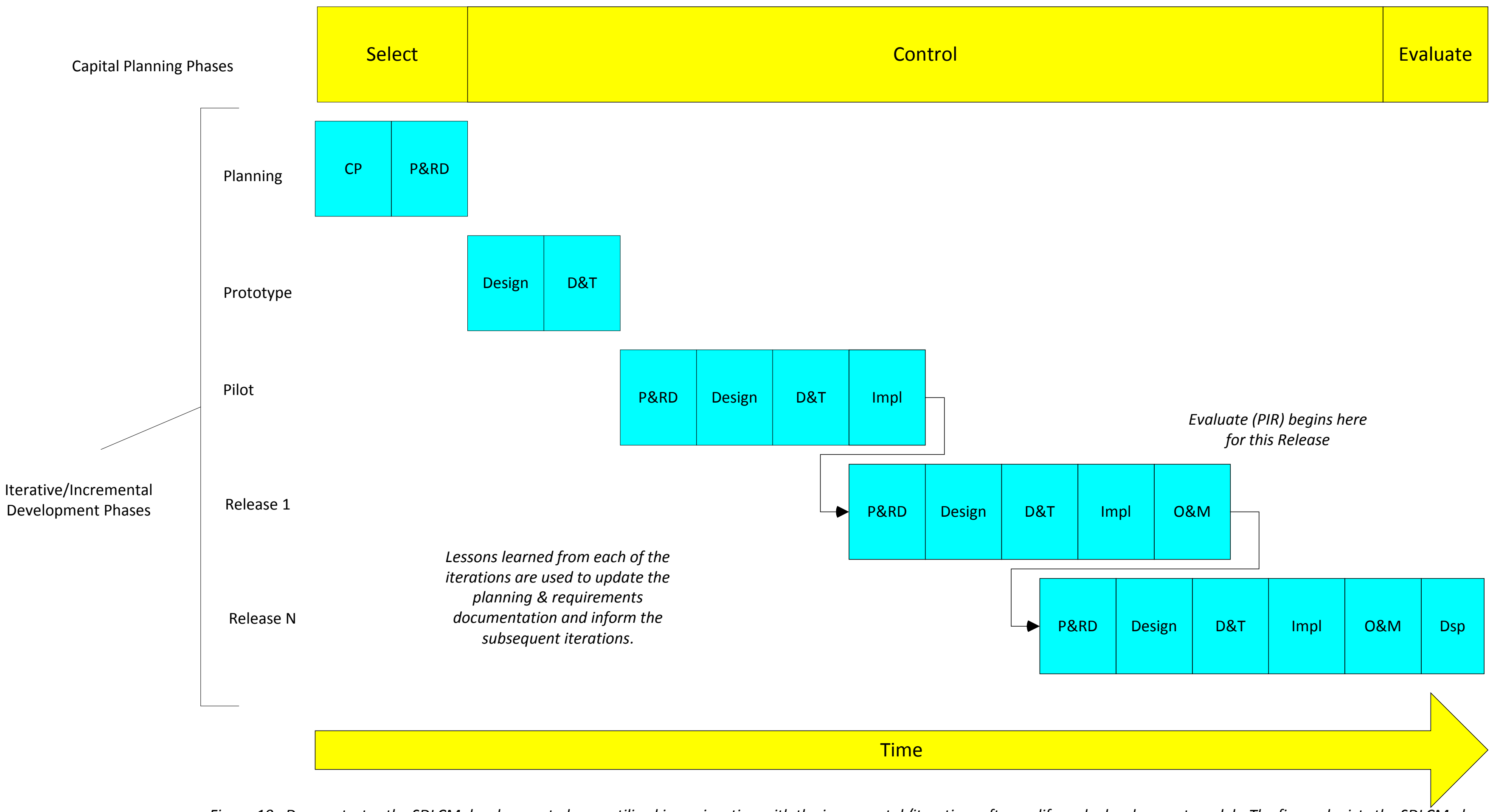
Capital Planning Phases
Select
Control
Evaluate
Iterative/Incremental Development Phases
Planning
CP
P&RD
Prototype
Design
D&T
Pilot
P&RD
Design
D&T
Impl
Evaluate (PIR) begins here for this Release
Release 1
P&RD
Design
D&T
Impl
O&M
Lessons learned from each of the iterations are used to update the planning & requirements documentation and inform the subsequent iterations.
Release N
P&RD
Design
D&T
Impl
O&M
Dsp
Time

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 II – Information References

The following appendix provides links to several information references that are relevant to the SDLCM.

Departmental Guidance

- Computer Security Handbook, Version 4.0, August 2009
  http://www.labornet.dol.gov/itc/it/operations/csh-

- DOL IT Capital Planning and Investment Control (CPIC) Guide: "Managing IT Projects" (Version 2.1, October 2011)
  http://www.labornet.dol.gov/itc/it/policyoversight/DOL-CPIC-Guide-v2.1.doc

- Department of Labor IT Strategic Plan, September 2005-2009
  http://www.dol.gov/cio/programs/ITStrategicPlan2006/IT-Strategic-Plan.htm
- Department of Labor Manual Series (DLMS 1 Records Management)
  http://labornet.dol.gov/workplaceresources/policies/DLMS/DLMS01/dlms1-0100.doc

- Department of Labor Manual Series (DLMS 9 Information Technology)
  http://labornet.dol.gov/itc/it/operations/DLMS-9-IT.htm

- DOL Earned Value Management Guide
  http://labornet.dol.gov/itc/it/policyoversight/Earned-Value-Management-Operational-Guide-v1-7.doc

- DOL Governance Framework for IT Investments Reference Guide for Capital Planning, Security , and Enterprise Architecture, October 2005
  http://labornet.dol.gov/itc/it/policyoversight/ea-governance-guide-approved.htm

- DOL IT Investment Management Quick Reference Guide, V1.0, June 6, 2006
  http://labornet.dol.gov/itc/it/policyoversight/DOL-IT-IM-Quick-Ref-Guide.pdf

DOL Guide to Completing the FY 2013 OMB Exhibit 300, August 31, 2011
http://www.labornet.dol.gov/itc/it/policyoversight/DOL-FY13-Exhibit-300-Guide.PDF

- Office of the Chief Information Officer Document Links
  http://labornet.dol.gov/itc/it/policyoversight/resource-lib.htm

Federal Guidance

- OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs http://www.whitehouse.gov/omb/circulars_a094/
- OMB Circular A-11, Part 7, Planning, Budgeting, Acquisition and Management of Capital Assets (Includes OMB Exhibit 300 information)
  http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc

- Circular A-109, Major Systems Acquisitions
  (Available in hard copy only)
- OMB Director's Policy Memorandum M-97-02 (Raines Rules)
  http://www.whitehouse.gov/omb/memoranda/m97-02.html
- OMB Circular A-130, Management of Federal Information Resources
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- OMB Information Policy, IT and E-Gov
  http://www.whitehouse.gov/omb/inforeg/infopoltech.html
- CIO Council Document Links
  http://cio.gov/index.cfm?function=documents

Legislative Guidance

- E-Government Act of 2002, Public Law 107-347, December 17, 2002.
  http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR02458:|TOM:/bss/d107query.html
- National Technology Transfer and Advancement Act of 1995
  http://www.thomas.gov/cgi-bin/bdquery/z?d104:HR02196:@@@L&summ2=m&Information Technology
- Management Reform Act of 1996 – ITMRA (Clinger-Cohen)
  http://www.cio.gov/Documents/it%5Fmanagement%5Freform%5Fact%5FFeb%5F1996%2Ehtml

APPENDIX III – SLDCM DELIVERABLE SUPPORTING DOCUMENTATION

Deliverable	Type	Supporting Documents
Phase 1 - Conceptual Planning Phase		
Project Charter	Core	FIPS PUB 64 1.3.1 DOL OCIO Project Charter template, which can be found in the DOL OCIO LaborNet Resource Library
Cost Benefit Analysis	Core	DOL OCIO CBA template, which can be found in the DOL OCIO LaborNet Resource Library OMB A-130: Appx IV 8b1; OMB A-94: Section 5; IEEE/EIA 12207.0-1996 Section 5.1.1.6, Clinger-Cohen Act 1996 Sec 5112(c); FIPS PUB 64 1.3.3
Project Management Plan	Core	DOL OCIO PMP template, which can be found in the DOL OCIO LaborNet Resource Library IEEE/EIA 12207.2-1997 Sec 5.2.4.2
Work Breakdown Structure	Core	IEEE/EIA 12207.2-1997 Sec 5.2.4.5 (c)
Risk Management Plan and Risk Register	Core	DOL OCIO Risk Management Plan template and associated Risk Register, which can be found in the DOL OCIO LaborNet Resource Library; DOL OCIO Risk Management FAQ which can be found in the DOL OCIO LaborNet FAQ web page; IEEE/EIA 12207.0-1996 Section 5.1.1.6; NIST Handbook March 16, 1995; OMB A-130 Appx III B; IEEE/EIA 12207.2-1997 Section 7.1.2.1 (f)/Annex L, Clinger-Cohen Act 1996 Sec 5112 (a)(b)(c); 5122(a)(b)(5)
Investment Target Architecture – Business Architecture & Performance Architecture	Core	DOL OCIO Investment Target Architecture template , which can be found in the DOL OCIO LaborNet Resource Library
Investment Transition Strategy	Core	DOL OCIO Investment Transition Strategy template , which can be found in the DOL OCIO LaborNet Resource Library
FIPS 199 System Categorization Report	Core	DOL Computer Security Handbook (CSH) Volumes 4 and 14. FIPS Pub 199.
Statement of Work	Optional	Clinger-Cohen Act 1996 Sec 5312 (c)(2)
Phase 2 - Planning and Requirements Definition Phase		
Acquisition Plan	Core	DOL OCIO Acquisition Plan template, which can be found in the DOL OCIO LaborNet Resource Library Clinger-Cohen Act 1996 Sec 5124 ; OMB A-130 Appx IV Sec 8 b(5) ; OMB A-109; IEEE/EIA 12207.0-1996 Sec 5.1.1.2/5.1.1.8/5.2.4
Functional Requirements Document	Core	IEEE/EIA 12207.0-1996 Sec 5.1.1.2/5.1.1.8/5.2.4.3
Security Risk Assessment	Core	OMB A-130 Appx III A 3 a 2 ; OMB A-130 Appx III A 4 a 3) ; OMB A-130 Appx III B a 2 ; OMB A-130 Appx III B a 3 ; NIST Special Publication 500-223 ; FIPS Pub 102 Sec 1.5.1 ; IEEE/EIA 12207.0-1996 Sec 5.1.1.6 ; Clinger-Cohen Act 1996 Sec 5131 (2)(D); IEEE/EIA 12207.0-1996 Sec. 5.2.4.5
System Security Plan/Security Risk Assessment	Core	OMB A-130 Sec 8 Policy-Info Mgmt/Safeguards; OMB A-130 Appx III B a 2) Security plan; IEEE/EIA 12207.0-1996 Sec 5.2.4.5 (l), Clinger-Cohen Section 5131, DOL Computer Security Handbook
Phase 3 - Design Phase		
Configuration Management Plan	Core	IEEE/EIA 12207.2-1997 Sec 6.2/ISO 10007 ; IEEE/EIA 12207.0-1996 Sec 5.2.4.5
Detailed Design	Core	IEEE/EIA 12207.2-1997 Sec 5.3.4.2, 5.3.5.6, 5.3.7.5, 5.3.8.5; NIST SP 500-223 Sec 2.2, 2.3
Contingency Plan	Core	OMB A-130 Appendix III A 3 b 2) d
Phase 4 - Development and Test Phase		
Test Plan	Core	IEEE/EIA 12207.2-1997 Annex D-H.4 (c),
Implementation Plan	Core	IEEE/EIA 12207.2-1997 Sec 5.3.1
Acceptance Test Plan	Core	IEEE/EIA 12207.2-1997 Sec 5.3.13.1 and Annex D-H.4
Acceptance Test Report	Core	IEEE/EIA 12207.2-1997 Sec 5.3.13.1/5.3.11.2; IEEE 12207.0-1996 Annex E 3, 4
Training Plan	Core	IEEE/EIA 12207.0-1997 Sec 7.4.1.1;OMB A-130 Appendix III A 3a2)b); Clinger-Cohen Act 1996 Section 5112(i) ; IEEE/EIA 12207.0-1996 Sec 5.2.4.5(o)
System manuals	Core	IEEE/EIA 12207.2-1997 Sec 6.1
User Manuals	Core	IEEE/EIA 12207.2-1997 Sec 6.1
Implementation Phase		

Deliverable	Type	Supporting Documents
Computer Security Certification	Core	FIPS Pub 102
Security Accreditation Letter	Core	IEEE/EIA 12207.0-1996 Sec 5.3.13; FIPS Pub 102 Sec 2.5.2, 2.6.2; DOL Computer Security Handbook
System Acceptance Letter	Core	IEEE/EIA 12207.0-1996 Section 5.3.12
Operations and Maintenance Phase		
Disposition Plan	Core	IEEE/EIA 12207.0-1996 Sec 5.2.4
Disposition Phase		
None	N/A	N/A
Deliverable Types:	Core	Deliverable is required for this phase
	Optional	Deliverable may or may not be produced for this phase

APPENDIX IV – Exception Request Form

Procedure and Point of Contact

The OCIO is responsible for oversight regarding the development of IT investments and their compliance within the SDLCM framework. If alternate approaches or non-standard SDLCM deliverables are going to be generated in conjunction with a investment, an exception request needs to be approved by the OCIO. Agency IT investment sponsors and Project Managers will need to coordinate with OCIO staff, discuss the exception process prior to the conceptual planning phase, and submit an SDLCM Exception Request Form for approval. Exception requests will be handled on a case-by-case basis, taking into consideration the complexity of the investment and the applicability of the specific request. Please utilize the exception request form below, and return the form to the OASAM Office of Systems Development and Integration as referenced. The System Development Team and the Capital Planning Team will initially review exception requests and the Deputy CIO will provide final approval.

AGENCY INFORMATION – PLEASE PRINT

AGENCY COMPLETES	AGENCY	DATE
	OFFICE ADDRESS	ROOM
	POINT OF CONTACT	PHONE
	SIGNED (IR MANAGER)	DATE

INVESTMENT INFORMATION

INVESTMENT MANAGER COMPLETES	INVESTMENT NAME	LIFE CYCLE COST
	INVESTMENT DESCRIPTION	LIFE CYCLE TERM (YEARS)
	INVESTMENT MANAGER	ROOM/PHONE
	SIGNED (INVESTMENT MANAGER)	DATE

Exception Information

attach if required

Investment Manager Completes	Are you requesting non-standard SDLCM Deliverable formats? Yes □ No □	If Applicable - List Deliverables
	Are you requesting non-standard SDLCM Development Phases? Yes □ No □	If Applicable – List Phases/Model
	Is your IT investment classified Non-Systems Development? Yes □ No □	If Applicable – Explain
	Detail and justify specific SDLCM Exception Requested (attach if required)	

Return to: **United States Department of Labor**
Office of the Assistant Secretary for Administration and Management
200 Constitution Ave. NW, N-1301
Washington, DC 20210
Attn: ***Office of Systems Development & Integration (Room N-1301 (A-11))***

OCIO Review Feedback

OCIO Staff Completes	System Development POC	Signed Date	Approved: Yes □ No □	Comments(attach if required)
	capital Planning POC	Signed Date	Approved: Yes □ No □	Comments(attach if required)
	Deputy CIO	Signed Date	Approved: Yes □ No □	Comments(attach if required)
	SDLCM Exception Request Approved: Yes □ No □			

APPENDIX V – SDLCM Deliverable Templates

Project Charter

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 under the SDLCM subject area.

Cost Benefit Analysis (CBA)

A CBA document is an important and effective management tool for providing valuable information to decision makers about the viability of initiating or continuing information technology (IT) investments. A CBA provides the results of the financial analysis of the projected life cycle costs and benefits of at least three viable investment alternative solutions to fulfill a business need or performance gap. A CBA supports management in making business decisions about initiating or continuing the life cycle of an IT investment. A CBA includes an Alternatives Analysis section which describes the process in which three viable alternatives were selected, as a result of identifying first the feasible alternatives and then the most viable alternatives. The three most viable alternatives used in the CBA are required to be similar or comparable in size/scope and close the same business need or performance gap. For Major IT investments, the CBA life cycle period is required to be 10 years. For Non-major IT Investments, the life cycle period should be at least 5 years. An investment CBA document should be no more than 5 years old and it is required be reviewed and "refreshed" annually in preparation for the annual CPIC Exhibit 300 budget process. "Refreshed" means the document is reviewed and updated as necessary to reflect any investment changes especially cost and/or benefit changes that could result in a change the NPV, ROI, and/or the chosen alternative. PMs of Major IT investments are required to actively manage the life cycle costs and benefits of the chosen investment on an annual basis. While "sunk" costs (i.e., costs that have already been incurred in prior fiscal years by the existing investment) are not included in a full CBA update, the reuse and/or portability of existing capital assets for the current investment must be leveraged and factored into the life cycle costs/benefits of the other viable alternatives, as applicable.

The DOL OCIO has developed a detailed CBA template to assist and support IT PMs and IPTs in the development and maintenance of a CBA document. A copy of the DOL OCIO CBA template can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area.

In addition, the DOL OCIO has developed a detailed Cost Model to assist and support IT PMs in the development and maintenance of the investment CBA. The Cost Model alone does not represent a CBA as the content and results of a specific investment's Cost Model must be explained and justified in narrative form in the CBA document. A copy of the DOL OCIO Cost Model and associated instructions for using the Cost Model can be found in the DOL OCIO Resource Library on LaborNet at http://labornet.dol.gov/OCIO/resource-lib.htm under the SDLCM subject area.

CBAs serve many purposes, including:

1) Comparison of life cycle costs and benefits information in dollar terms;
2) Assessment of the total effect of potential investment benefits, both in dollar terms and in qualitative terms, over a defined life cycle;

3) Identification of feasible and at least three viable alternatives that best meet program objectives or best fulfills the business need or performance gap;
4) Determination of a baseline for measuring if an IT investment meets performance objectives;
5) The development of critical information, such as performance and cost data, necessary in an ongoing investment management process to help plan, budget, and allocate scarce resources among competing priorities.

Project Management Plan (PMP)

The PMP is prepared for all investments. It is one of several essential investment-planning documents that use a building-block approach to planning. It is a vehicle for documenting investment scope, tasks, schedule, allocated resources, and interrelationships with other investments. It also provides details on the involved Agency units, required job tasks, and milestone and review scheduling.

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 developed a detailed 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 under the SDLCM subject area.

Work Breakdown Structure (WBS)

The WBS is a critical project management planning tool that is included within the Project Management Plan. The WBS is developed at the beginning of the Conceptual Planning Phase along with the PMP and is updated, as necessary in accordance with DOL baseline management requirements, for each of the remaining life cycle phases. (See the DOL IT Baseline Management Guide v1.2, dated January 2012 for a detailed description of DOLs baseline management requirements.) The WBS identifies all of the work activities associated with an IT investment for each of the IT investments life cycle phases. (See the detailed description of the WBS in Section 1.9 of this document for more details.)

Risk Management Plan (RMP) and Risk Register (RR)

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 RR that all DOL IT investments are required to implement. A copy of the Risk Management Plan template and associated RR can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area.

Investment Target Architecture

The DOL OCIO has created an “Investment Target Architecture” template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area.

Investment Transition Strategy and Sequencing Plan

The DOL OCIO has created an “Investment Transition Strategy and Sequencing Plan” template, which can be found in the DOL OCIO LaborNet Resource Library under the Enterprise Architecture subject area

FIPS 199 System Categorization Report

Please refer to the DOL Computer Security Handbook (CSH) Volumes 4 and 14 for information on this deliverable.

Privacy Impact Assessment

Please refer to the DOL Computer Security Handbook for information on this deliverable.

Acquisition Plan (AP)

The AP is a document that shows how all hardware, software, and telecommunications capabilities, along with contractor support services, are acquired during the life of the investment. The AP helps ensure that needed 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 Acquisition Plan template as well as a guide to developing the Acquisition Plan to assist and support IT Investment PMs, PMOs, and/or IPTs in completing the Acquisition Plan. A copy of the Acquisition Plan template can be found in the DOL OCIO Resource Library on LaborNet under the SDLCM subject area.

Statement of Work (SOW)

No standard DOL SOW guidance or template exists at this time. If you have questions regarding this deliverable, contact the OCIO for guidance.

Functional Requirements Document (FRD)

The FRD is formal statement of an application's business requirements. It serves the same purpose as a contract. The developers agree to provide the capabilities specified. The client agrees to find the product satisfactory if it provides the capabilities specified in the FRD. The FRD has the following characteristics:

- It demonstrates that the application provides value to DOL in terms of the business objectives and business processes in the 5-year strategic plan.
- It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything not stated in the FRD.
- It is solution independent. The FRD is a statement of what the application is to do, not of how it works. The FRD does not commit the developers to a design. For that reason, any reference to the use of a specific technology is entirely inappropriate in an FRD.

A sample outline for an FRD is provided in Exhibit 1.

Exhibit 1: Sample Functional Requirements Document Outline

Functional Requirements Document Outline

Cover Page

Table of Contents

1. Introduction

1.1 Investment Description

Provide a brief overview of the investment.

1.1.1 Background

Summarize the conditions that created the need for the application.

1.1.2 Purpose

Describe the business objectives and business processes from the cost-benefit analysis (CBA) that this application supports.

1.1.3 Assumptions and Constraints

Assumptions are future situations, beyond the control of the investment, whose outcomes influence the success of an investment (i.e. availability of a hardware/software platform; pending legislation; court decisions that have not been rendered; future trends in DOL missions; developments in technology). Constraints are conditions outside the control of the investment that limit the design alternatives (i.e. Government regulations; standards imposed on the solution; strategic decisions). Be careful to distinguish constraints from preferences. Constraints exist because of real business conditions. Preferences are arbitrary. For example, a delivery date is a constraint only if there are real business consequences that can happen as a result of not meeting the date. For example, if failing to have the subject application operational by the specified date places DOL in legal default, the date is a constraint. A date chosen arbitrarily is a preference. Preferences, if included in the RD, should be noted as such.

1.1.4 Interfaces to External Systems

Name the applications with which the subject application must interface. State the following for each such application: name of application; owner of application (if external to DOL); details of interface (only if *determined by the other application).*

1.2 Points of Contact

List the names, titles, and roles of the major participants in the investment. At a minimum, list the following: DOL investment leader; development investment leader; user contacts; DOL employee whose signature constitutes acceptance of the FRD.

1.3 Document References

Name the documents that were sources of this version of the RD. Include meeting summaries, white paper analyses, CBA, and other System Development Life Cycle Management deliverables, as well as any other documents that contributed to the RD. Include the Configuration Management identifier and date published for each document listed.

2. Business Requirements

The business requirements describe the core functionality of the application. This section includes the data and process requirements.

2.1 Data Requirements

Describe the data requirements by producing a logical data model, which consists of entity relationship diagrams, entity definitions, and attribute definitions. This is called the application data model. The data requirements describe the business data needed by the application system. Data requirements do not describe the physical database.

2.2 Process Requirements

Process requirements describe what the application must do. Process requirements relate the entities and attributes from the data requirements to the users needs. State the functional process requirements in a manner that enables the reader to see broad concepts decomposed into layers of increasing detail.

3. Operational Requirements

Operational requirements describe the non-business characteristics of an application. State the requirements in this section. Do not state how these requirements will be satisfied. For example, in the Reliability section, answer the question, "How reliable must the system be?" Do not state what steps will be taken to provide reliability. Distinguish preferences from requirements. Requirements are based on business needs. Preferences are not.

3.1 Security

The Security section describes the need to control access to the data. This includes controlling who may view and alter application data.

3.2 Audit Trail

List the activities that will be recorded in the application's audit trail. For each activity, list the data to be recorded.

3.3 Data Currency

Data currency is a measure of how recent data are. This section answers the question, "When the application responds to a request for data how current must those data be?" Answer that question for each type of data request.

3.4 Reliability

Reliability is the probability that the system will be able to process work correctly and completely without being aborted. State the following in this section: damage that could result from this system's failure; minimum acceptable level of reliability; required reliability.

3.5 Recoverability

State the ability to restore functions and data in case of a failure.

3.6 System Availability

System availability is the time when the application must be available for use. Required system availability is used in determining when maintenance may be performed. In this section state the hours during which the application is to be available to users. Include the times when usage is expected to be at its peak. These are times when system unavailability is least acceptable.

3.7 Fault Tolerance

Fault tolerance is the ability to remain partially operational during a failure. Describe the following in this section: which functions need not be available at all times; if a component fails what (if any) functions must the application continue to provide; and what level of performance degradation is acceptable. For most applications, there are no fault tolerance requirements. When a portion of the application is unavailable, there is no need to be able to use the remainder of the application.

3.8 Performance

Describe the requirements for the following: Response time for queries and updates; throughput; expected volume of data; and expected volume of user activity (for example, number of transactions per hour, day, or month).

3.9 Capacity

List the required capacities and expected volumes of data in business terms. For example, state the number of cases about which the application will have to store data; state capacities in terms of the business. Do not state capacities in terms of system memory requirements or disk space.

3.10 Data Retention

Describe the length of time the data must be retained.

4. Requirements Traceability Matrix

The requirements traceability matrix (RTM) provides a method for tracking the functional requirements and their implementation through the development process. Each requirement is included in the matrix along with its associated section number. As the investment progresses, the RTM is updated to reflect the status of each requirement. When the product is ready for system testing, the matrix lists each requirement, what product component addresses it, and what tests verify that it is correctly implemented. Exhibit 16 illustrates a sample RTM.

5. Concepts of Operations (CONOPS)

A concept of operations (CONOPS) is required for all new systems or major system development efforts. A CONOPS is also required for all system enhancement efforts that will significantly affect current operational procedures and processes, or that affect more than a single system. The user group develops CONOPS, includes DOL Operational Experts, Managers, Subject Matter Experts, and System Owners. CONOPS must be consistent with applicable Federal law, Congressional direction and IT investments, the President's priorities, DOL Strategic Plans and Mission Statements.

5.1 Definition of Features

This section describes the features of the system.

5.2 Description of Operations

This section describes all aspects of the operations of the proposed system.

5.3 User Organization View

This section provides an explanation of how the system will look to each user organization.

5.4 Effect on Operations and Personnel

This section describes the effect of the system on personnel and on their operations.

5.5 Effect on Existing Operations

This section describes the effect of the system on existing operations.

5.6 Interfaces to Other Systems

This section describes the interfaces to other systems that will be built into the proposed new system.

5.7 Methods of Implementation

This section describes the intended implementation approach, from the user's point of views.

5.8 Figure (Optional)

This optional section contains a graphical representation of CONOPS.

Security Risk Assessment

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

System Security Plan

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

Security Plan of Action & Milestones (POA&M)

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

Test Plan (TP)

The TP identifies the tasks and activities that need to be performed so that all aspects of the system are adequately tested so that the system can be successfully implemented. It documents the scope, content, methodology, sequence, management of, and responsibilities for test activities. It describes the test activities of the subsystem integration test, the system test, and the acceptance test (including security testing) in progressively higher levels of detail as the system is developed.

The TP provides guidance for the management of test activities, including organization, relationships, and responsibilities. The test case procedures may be included in the Test Plan or in a separate document, depending on system size. The users assist in developing the Test Plan, which describes the nature and extent of tests deemed necessary. This provides a basis for verification of test results and validation of the system. The validation process ensures that the system conforms to the functional requirements in the Functional Requirements Document (FRD) and that other applications or subsystems are not adversely affected. The Test Plan is a dynamic document used for directing the testing of the system throughout the life cycle. A sample outline for a TP is shown in Exhibit 2.

Exhibit 2: Sample Test Plan Outline

Test Plan Outline

Cover Page

Table of Contents

1. **Purpose**

   In this section, present a clear, concise statement of the purpose of the investment test plan and identify the application system being tested by name. Include a summary of the functions of the system and the tests to be performed.

2. **Background**

   This section should provide a brief description of the history and other background leading up to the *system development process. Identify the user organization and the location where the testing will be performed. Describe any prior testing, and note results that may affect this testing.*

3. Scope

This section describes the projected boundaries of the planned tests. Include a summary of any constraints imposed on the testing, whether they are because of a lack of specialized test equipment, or constraints on time or resources. Describe constraints in detail in Section 5.1, Limitations.

4. Glossary

This section provides a list of all terms and abbreviations used in this document. If the list is several pages in length, it may be placed as an appendix.

5. Limitations and Traceability

This section elaborates on the limitations summarized in Section 3, Scope, and cross-references the functional requirements and detailed specifications to the tests that demonstrate or partially demonstrate that capability.

5.1 Limitations

This section describes limitations imposed on the testing, whether they are because of a lack of specialized test equipment, or constraints on time or resources. Indicate what steps, if any, are being taken to reduce the program risk because of the test limitation(s).

5.2 Traceability (Functional Requirements Traceability Matrix)

This section expands the traceability matrix created in the FRD by including test activities that address user requirements. The intent is to show that the test plan covers all functionality, performance, and other requirements associated with each design element (unit, module, subsystem, and system) in the internal design document.

6. Test Plans

This section describes the levels of tests that take place during development: integration, system, security, and user acceptance tests, and the planning that is needed. The test environment is described in terms of milestones, schedules, and resources needed to support testing.

6.1 Test Levels

This section should include a list of the types of software testing to be performed. List all applicable levels and enter "Not applicable" if a particular level of testing does not apply to the investment.

6.1.1 Subsystem Integration Test

This section discusses the tests that examine the subsystems made up of integrated groupings of software units and modules. This is the first level of testing where problem reports are generated; these reports are classified by severity, and their resolution is monitored and reported. Subsystem integration test results (including the test data sets and outputs produced from the tests) may be delivered as part of the final test plan, with the integration test analysis report or as an appendix.

6.1.2 System Test

This section describes the type of testing that determines system compliance with standards and satisfaction of functional and technical requirements when executed on target hardware using simulated operational data files and prepared test data. System documents and training manuals are examined for accuracy, validity, completeness, and usability. During this testing period, software performance, response time, and ability to operate under stressed conditions are tested. External system interfaces are also tested. All findings are recorded in a system test analysis report.

6.1.3 User Acceptance Test

This section describes the tests performed in a non-production environment that mirrors the environment in which the system will be fielded. Every system feature may be tested for correctness and satisfaction of functional requirements. System interoperability, all documentation, system reliability, and the level to which the system meets user requirements are evaluated. Performance tests may be executed to ensure that screen response time, program run time, operator intervention requirements, and overall system operations meet user requirements. Recovery and restart procedures should be evaluated; interfaces to other applications should also be tested.

6.1.4 Security Test

This section is equivalent to the Security Test and Evaluation discussed in the Certification and Accreditation process. These tests evaluate compliance with system security and integrity requirements. System backup, recovery, security, audit trails, reconciliation and other issues are addressed. Include internal controls or application security features mentioned in the context of security testing. Security testing is performed in the operational (production) environment under the guidance of designated security staff. A summary description of these tests and their results are required in the certification package.

6.2 Test Environment and Schedules

This section documents key elements of the test environment, including milestones, schedule, and resource requirements.

6.2.1 Software Description

This section provides a brief description of the inputs, outputs, and functions of the software being tested.

6.2.2 Milestones

This section lists the milestone events and dates for the testing.

6.2.3 Organizations and Locations

This section provides information on the participating organizations and the location where the software will be tested.

6.2.4 Schedule

This section shows the detailed schedule of dates and events for the testing by location. Events should include familiarization, training, test data set generation, and collection, as well as the volume and frequency of the input for testing.

6.2.5 Resource Requirements

This section and associated statements define the resource requirements for the testing.

6.2.5.1 Equipment

This section shows the expected period of use, types, and quantities of equipment needed.

6.2.5.2 Software

This section lists other software needed to support testing that is not part of the software being tested. This should include debugging software and programming aids as well as many current programs to be run in parallel with the new software to ensure accuracy; any drivers or system software to be used in conjunction with the new software to ensure compatibility and integration; and any software required to operate the equipment and record test results.

6.2.5.3 Personnel

This section lists the number of personnel their skill types, and schedules for personnel - from the user, database, Quality Assurance, security, and development groups - who will be involved in the test. Include any special requirements, such as multiple-shift operation or key personnel.

6.2.6 Testing Material

This section lists the materials needed for the test, such as documentation, software to be tested and its medium, test inputs, sample outputs, test control software, and worksheets.

6.2.7 Test Training

This section describes or references the plan for providing training in the use of the software being tested. Specify the types of training, personnel to be trained, and the training staff.

6.2.8 Test Methods and Evaluation

This section documents the test methodologies, conditions, test progression or sequencing, data recording, constraints, criteria, and data reduction.

6.2.8.1 Methodology

This section describes the general methodology or testing strategy for each type of testing described in this test plan.

6.2.8.2 Conditions

This section specifies the type of input to be used, such as real-time entered test data or canned data for batch runs. It describes the volume and frequency of the input, such as the number of transactions per second tested, etc. Sufficient volumes of test transactions should be used to simulate live stress testing and to incorporate a wide range of valid and invalid conditions. Data values used should simulate live data and test limited conditions.

6.2.8.3 Test Progression

This section describes the manner in which progression is made from one test to another, so the entire cycle is completed.

6.2.8.4 Data Recording

This section describes the method used for recording test results and other information about the testing.

6.2.8.5 Constraints

This section indicates anticipated limitations on the test because of test conditions, such as interfaces, equipment, personnel, and databases.

6.2.8.6 Criteria

This section describes the rules to be used to evaluate test results, such as range of data values used, combinations of input types used, or maximum number of allowable interrupts or halts.

6.2.8.7 Data Reduction

This section describes the techniques that will be used for manipulating the test data into a form suitable for evaluation - such as manual or automated methods - to allow comparison of the results that should be produced to those that are produced.

7. Test Descriptions

This section describes each test to be performed. Tests at each level should include verification of access control and system standards, data security, functionality, and error processing. As various levels of testing (subsystem integration, system, user acceptance testing, and security) are completed and the test results are documented, revisions or increments of the test plan can be delivered. The subsections of this section should be repeated for each test within the investment. If there are many tests, place them in an appendix.

7.1 Test Name (repeat for each test)

This section identifies the test to be performed for the named module, subsystem, or system. Address the criteria discussed in the subsequent sections for each test.

7.1.1 Test Description

Describe the test to be performed. Tests at each level of testing should include those designed to verify data security, access control, and system standards; system/subsystem/unit functionality; and error processing as required.

7.1.2 Control

Describe the test control, such as: manual, semiautomatic, or automatic insertion of inputs; sequencing of operations; and recording of results.

7.1.3 Inputs

Describe the data input commands used during the test. Provide examples of input data. At the discretion of the Project Manager, input data listings may also be requested in computer readable form for possible future use in regression testing.

7.1.4 Outputs

Describe the output data expected because of the test and any intermediate messages or display screens that may be produced.

7.1.5 Procedures

Specify the systematic procedures to accomplish the test, include test setup, initialization steps, and termination. Also include effectiveness criteria or pass criteria for each test procedure.

Configuration Management Plan (CMP)

The CMP establishes uniform CM practices in a system development investment to manage the establishment of and changes to, system hardware and software. CM helps maintain the integrity of the system throughout its life cycle and facilitates communication about the system among investment team members, users, and other supporting organizations. CM guidelines are applied through the systematic identification, control, and auditing of system characteristics, including the following:

- Configuration identification of functional and physical characteristics of a system through structured documentation baselines.
- Configuration control of changes to the physical and functional characteristics of hardware and software systems and the baseline documentation describing them.
- Configuration status accounting about the current configuration and changes to it.
- Configuration auditing to verify that system performance and configuration are accurately identified in the baseline documentation.
- Storage and control of access to the baseline documentation, source code, and executable code.

A baseline is a documented technical description that becomes a reference point against which changes can be proposed, evaluated, and incorporated. A sample CMP is shown in Exhibit 3.

Exhibit 3: Sample Configuration Management Plan Outline

Configuration Management Plan Outline

Cover Page

Table of Contents

1. Introduction

Provide a brief statement that introduces the CM plan and describes, in general terms, its use in managing the configuration of the specific investments.

1.1 Purpose

Describe why this CM plan was created, what it accomplishes, and how it is used.

1.2 Scope

Define the scope of CM planning. Include the System Development Life Cycle Management (SDLCM)) work pattern and its limits, effects of CM on the conduct of development methodology, and effects of the involvement of other contractors within the CM process.

1.3 Policy

Identify policy decisions that affect the conduct of CM on the investment.

1.4 System Description

Briefly describe the system, its history, and the environment in which the investment operates (mainframe, client/server, or stand-alone). Describe the system architecture, operating system, and application languages. Identify other legacy or new systems with which this system interfaces. List the number of *sites that are using the system.*

1.5 Definitions

Define the terms that appear in the CM plan.

1.6 Reference Documents

List the documents that are referenced to support the CM process including any investment or standards documents referenced in the body of the CM plan.

1. Organization

Identify the organization in which CM resides and all organization units that participate in the investment. Define the functional roles of these organizational units within the investment structure.

2.1 CM Activities

Identify all CM functions required to manage the configuration of the system.

2.2 CM Responsibilities

List CM responsibilities in supporting this investment.

3. Configuration Identification

Explain that Configuration Identification is the basis on which the configuration items (CIs) are defined and verified; CIs and documents are labeled; changes are managed; and accountability is maintained.

3.1 Configuration Item Identification

Identify the CIs to be controlled and specify a means of identifying changes to the CIs and related baselines.

3.2 Identification Conventions

Describe the identification (numbering) criteria for the software and hardware structure, and for each document or document set.

3.3 Naming Conventions

Provide details of the file naming convention to be used on the investment and how file configuration integrity will be maintained.

3.4 Labels

Describe the requirements for labeling media and application software.

3.5 Configuration Baseline Management

Describe what baselines are to be established. Explain when and how they will be defined and controlled.

3.6 Libraries

Identify the libraries and the media under control, the requirements for the control of documentation, and how access control is to be managed.

4. Configuration Control

Explain that configuration change management is a process for managing configuration changes and variances in configurations.

4.1 Change Process

Define the process for controlling changes to the system baselines and for tracking the implementation of those changes.

4.2 Review and Control Board(s)

Describe any Internal Review Boards and Configuration Control Boards that will be established for the investment. For each board, discuss the members who will participate (and their functional representatives), the Chair, the Secretariat, and the responsibilities of the board and of each member to the board.

4.3 Interface Management

Identify the interfaces to be managed and describe the procedures for identification of interface requirements, establishment of interface agreements, and participation in any Interface Control Working Groups.

3. Configuration Status Accounting

Explain that Configuration Status Accounting (CSA) is the process of keeping records of all change actions pertaining to a configuration item to generate reports on all decisions made and implemented. Also, show that CSA provides a means of storing and cross-referencing the collected data.

4. Configuration Audits

Describe how peer review audits will be accomplished.

5. Reviews

Describe how the technical reviews relate to the establishment of baselines and explain the role of CM in these reviews.

6. CM Plan Maintenance

Describe the activities and responsibilities necessary to ensure continued CM planning during the life cycle of the project; state who is responsible for monitoring the CM plan. Describe how frequently updates are to be performed; how changes to the CM plan are to be evaluated and approved; and how changes to the CM plan are to be made and communicated.

Legacy Data Plan

No standard DOL guidance or template exists at this time. If you have questions regarding this deliverable, contact the OCIO for guidance.

Detailed Design Document (DDD)

The DDD describes the detailed system and subsystem designs, and detailed requirements that will be used in developing the information system. It contains the database structure, file structures, input formats, output layouts, and module processing logic to be used by the investment team during system development. The sections and subsections of the final design document may be organized, rearranged, or repeated as necessary to reflect the best organization for a particular investment. A sample outline for a DDD is shown is Exhibit 4.

Exhibit 4: Sample Detailed Design Document Outline

Detailed Design Document Outline

Cover Page

Table of Contents

1. Introduction

1.1 Purpose and Scope

This section describes the final design document purpose and scope.

1.2 Organization of this Document

This section describes the organization of the final design document.

1.3 Points of Contact

Provide the organization and title of the key points of contact (and alternates if appropriate) for the information system development effort in this section. These points of contact should include the Investment Manager, Investment Owner, system developer, programmer analyst, Quality Assurance (QA)

Manager, Security Manager, Configuration Manager, and other points of contact as appropriate.

1.4 Investment References

In this section, provide a bibliography of key investment references and deliverables that have been produced before this point. For example, these references might include the Project Management Plan, Project Charter, cost-benefit analysis, acquisition plan, QA plan, Configuration Management Plan, Requirements document (RD), computer security plan, and preliminary design document.

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2. System Design Overview

This section briefly describes the system and subsystem architectures and their design specifications. The overview information in this section may partially repeat some of the content of the preliminary design document (such as, the system description and the flow diagrams). The content of this section should include the following: a narrative description of the system that describes all system inputs and outputs; a high-level block diagram of the system; forms sequences illustrating the detailed flow of events; object models; database schema; a system data dictionary.

3. Unit Design Organization

This section describes the segmentation of the system into subsystems (this section may reference the preliminary design document); segmentation of the subsystems into design units (a subsystem may map to one or more design unit per subsystem); and the segmentation of design units into design modules. The section should show - graphically or in tables - the relationship between design modules and the projected actual computer program compilation units. There may be one or more design module per program compilation unit, depending on the software design approach and the computer languages used. The degree and type of modularity above may be modified as necessary for the investment under development.

4. File and Database Design

Interact with the Data Administrator when preparing this section. The section should reveal the final design of all database management system (DBMS) files and the non-DBMS files associated with the system under development in this section. Additional information may be added as required for the particular investment.

4.1 Database Management System Files

This section reveals the final design of the DBMS files and includes the following information: final logical design; a physical database description; access methods; estimate of the DBMS file size or volume; and a definition of the update frequency of the database.

4.2 Non-Database Management System Files

In this section, provide the detailed description of all non-DBMS files and include a narrative description of the usage of each file - including whether the file is used for input, output, or both. If this file is a temporary file, include an indication of which modules read and write the file, etc.; and file structures.

5. Input and Output Design

This section provides the detailed design of the system and subsystem inputs and outputs. Any additional information may be added to this section and may be organized according to whatever structure best presents the system input and designs. Depending on the particular nature of the investment, it may be appropriate to repeat these sections at both the subsystem and design module levels. Additional information may be added to the subsections if the suggested lists are inadequate to describe the investment inputs and outputs.

5.1 System Input Design

This section is a description of the input media used for preliminary data transfers. For example, electronic data interchange, magnetic tape, scanned paper, etc. If appropriate, the input record types, file structures, and database structures provided in Section 4, File and Database Design may be referenced. Define data element definitions. Provide the layout of all input data screens or windows. Provide a graphic representation of each interface. Define or reference all data elements associated with each screen or window.

5.2 System Output Design

This section describes the system output design. System outputs include reports, data display screens, windows, and files. The output files are described in Section 4, and may be either repeated or referenced.

6. Detailed Module Design

A module is the lowest level of design granularity in the system. Depending on the software development approach, there may be one or more modules per program. This section should provide enough detailed information about logic and data necessary to correctly write source code for all modules in the system in this section. At the point at which this document is written, development of the detailed design has been completed for the modules, and that design is documented in this section.

7. Traceability (Requirements Traceability Matrix)

This section extends the traceability matrix created in the FRD to include features from the final design that address user requirements. This matrix begins with the user requirements and assists in tracing how the requirements are addressed in subsequent phases and documents. The matrix may also show traceability between FRD requirements, detailed requirements, and detailed design.

8. System Integrity Controls

Address integrity controls for protecting classified systems and data. This section may reference other documentation.

APPENDIX A

Detailed system requirements developed from Functional Requirements.

Contingency Plan

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

Implementation Plan (IP)

The IP describes how the information system will be installed and transitioned into an operational system. The plan contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. A sample IP is provided in Exhibit 5.

Exhibit 5: Sample Implementation Plan Outline

Implementation Plan Outline

Cover Page

Table of Contents

1. Introduction

This section provides an overview of the information system and includes any additional information that may be appropriate.

1.1 Purpose

This section describes the purpose of the implementation plan. Reference the system name and identify *information about the system to be implemented.*

1.2 System Overview

This section provides a brief overview of the system to be implemented, including a description of the system and its organization.

1.2.1 System Description

This section provides an overview of the processes the system is intended to support. If the system is a database or an information system, provide a general discussion of the description of the type of data maintained and the operational sources and uses of those data.

1.2.2 System Organization

his section provides a brief description of system structure and the major system components essential to the implementation of the system. It should describe both hardware and software, as appropriate. Charts, diagrams, and graphics may be included.

1.3 Investment References

This section provides a bibliography of essential investment references and deliverables that have been produced before this point in the investment development. For example, these references might include the Project Management Plan, Acquisition Plan, Functional Requirements Document (FRD), Test Plan, conversion plan, and preliminary and final detailed design documents.

1.4 Glossary

Provide a glossary of all terms and abbreviations used in the manual. If it is several pages in length, it may be placed in an appendix.

2. Management Overview

The subsequent sections provide a brief description of the implementation and major tasks involved in this section.

2.1 Description of Implementation

This section provides a brief description of the system and the planned implementation approach.

2.2 Points of Contact

In this section, list all managers and staff with whom the implementation must be coordinated, the name of the responsible organization(s), and titles and telephone numbers of the staff who serve as points of contact for the system implementation. These points of contact could include the System Owner, Project Manager, Security Manager, Database Administrator, Configuration Management Manager, or other managers with responsibilities relating to the system implementation. The site implementation representative for each installation or implementation site should also be included, if appropriate.

2.3 Major Tasks

This section provides a brief description of each major task required for the implementation of the system. Add as many subsections as necessary to this section to describe all the major tasks adequately. The tasks described in this section are not site-specific, but generic or overall investment tasks that are required to install hardware and software, prepare data, and verify the system. Include the following information for the description of each major task, if appropriate: what the task will accomplish; resources required to accomplish the task; key person(s) responsible for the task; and criteria for successful completion of the task.

2.4 Implementation Schedule

In this section, provide a schedule of activities to be accomplished during implementation. Show the required tasks (described in Section 2.3, Major Tasks) in chronological order, with the beginning and end dates of each task.

2.5 Security

If appropriate for the system to be implemented, include an overview of the system security features and requirements during the implementation. If the Privacy Act covers the system, provide Privacy Act concerns.

2.5.1 System Security Features

In this section, provide an overview and discussion of the security features that will be associated with the system when it is implemented. It should include the primary security features associated with the system hardware and software. Security and protection of sensitive Agency data and information should be discussed, if applicable. Reference the sections of previous deliverables that address system security issues, if appropriate.

2.5.2 Security During Implementation

This section addresses security issues specifically related to the implementation effort, if any. For example, if local area network (LAN) servers or workstations will be installed at a site with sensitive data preloaded on non-removable hard disk drives, address how security would be provided for the data on these devices during shipping, transport, and installation because theft of the devices could compromise the sensitive data.

3. Implementation Support

Implementation Support - This section describes the support software, materials, equipment, and facilities required for the implementation, as well as the personnel requirements and training necessary for the implementation. The information provided in this section is not site-specific. If there are additional support requirements not covered by the subsequent sections, others may be added as needed.

3.1 Hardware, Software, Facilities, and Materials

Hardware, Software, Facilities, and Materials - In this section, list support software, materials, equipment, and facilities required for the implementation, if any.

3.1.1 Hardware

This section provides a list of support equipment and includes all hardware used for testing the implementation. For example, if a client/server database is implemented on a LAN, a network monitor or "sniffer" might be used, along with test programs, to determine the performance of the database and LAN at high-utilization rates. If the equipment is site-specific, list it in Section 4, Implementation Requirements by Site.

3.1.2 Software

This section provides a list of software and databases required to support the implementation. Identify the software by name, code, or acronym. Identify which software is commercial off-the-shelf and which is DOL-specific. Identify any software used to facilitate the implementation process. If the software is site-specific, list it in Section 4.

3.1.3 Facilities

In this section, identify the physical facilities and accommodations required during implementation (i.e. physical workspace for assembling and testing hardware components, desk space for software installers, and classroom space for training the implementation staff). Specify the hours per day needed, number of days, and anticipated dates. If the facilities needed are site-specific, provide this information in Section 4.

3.1.4 Material

This section provides a list of required support materials, such as magnetic tapes and disk packs.

3.2 Personnel

This section describes personnel requirements and any known or proposed staffing requirements, if appropriate. Also, describe the training, if any, to be provided for the implementation staff.

3.2.1 Personnel Requirements and Staffing

In this section, describe the number of personnel, length of time needed, types of skills, and skill levels for the staff required during the implementation period. If particular staff members have been selected or proposed for the implementation, identify them and their roles in the implementation.

3.2.2 Training of Implementation Staff

This section addresses the training, if any, necessary to prepare staff for implementing and maintaining the system; it does not address user training, which is the subject of the training plan. Describe the type and amount of training required for each of the following areas for the system: system hardware/software installation; system support; and system maintenance and modification. Present a training curriculum listing the courses that will be provided, a course sequence, and a proposed schedule. If appropriate, *identify which courses particular types of staff should attend by job position description.*

3.3 Performance Monitoring

This section describes the performance monitoring tool and techniques and how it will be used to help decide if the implementation is successful.

3.4 CM Interface

This section describes the interactions required with the Configuration Management (CM) representative on CM-related issues, such as when software listings will be distributed, and how to confirm that libraries have been moved from the development to the production environment.

4. Implementation Requirements by Site

This section describes specific implementation requirements and procedures. If these requirements and procedures differ by site, repeat these subsections for each site; if they are the same for each site, or if there is only one implementation site, use these subsections only once.

4.1 Site Name or Identification for Site X

This section provides the name of the specific site or sites to be discussed in the subsequent sections.

4.1.1 Site Requirements

This section defines the requirements that must be met for the orderly implementation of the system and describes the hardware, software, and site-specific facilities requirements for this area. Any site requirements that do not fall into the following three categories and were not described in Section 3, Implementation Support, may be described in this section, or other subsections may be added following Facilities Requirements: hardware requirements; software requirements; data requirements; and Facilities Requirements.

4.1.2 Site Implementation Details

This section addresses the specifics of the implementation for this site. Include a description of the implementation team, schedule, procedures, and database and data updates. This section should also provide information on the following: team; schedule, procedures; database; and Data Update.

4.1.3 Back-Off Plan

This section specifies when to make the go/no go decision and the factors to be included in making the decision. The plan then goes on to provide a detailed list of steps and actions required restoring the site to the original, pre-conversion condition.

4.1.4 Post-implementation Verification

This section describes the process for reviewing the implementation and deciding if it was successful. It describes how an action item list will be created to rectify any noted discrepancies. It also references the back-off plan for instructions on how to back-out the installation, if, because of the post-implementation verification, a no-go decision is made.

Acceptance Test Plan

TBD – No standard DOL guidance or template exists at this time. During the next revision to the SDLCM, this issue will be addressed. If you have questions regarding this deliverable, contact the OCIO for guidance.

Security Control Assessment Aid (SCAA) / Security Test & Evaluation (ST&E) Report

The security controls assessment (SCA) of the full set of security controls performed in support of the certification and accreditation (C&A) process is an important step in ensuring the security of an information system. This assessment occurs at a single point in time. Deliverable: (1) Security Test and Evaluation (ST&E) Report; Computer Security Handbook (CSH) Volume 6 and (2) Security Self-Assessment, Security Control Assessment Aid (SCAA). (Source: Computer Security Handbook (CSH) Volume 4.)

Acceptance Test Report (ATR) and Approval

The ATR documents the results of acceptance test activities as defined in the Test Plan. It records results of the tests and presents the capabilities and deficiencies for review, if applicable. Test Problem reports, documenting problems encountered during testing, are included in the ATR, as appropriate. A sample outline for an ATR is shown in Exhibit 6 followed by description of each of the report subsections.

Exhibit 6: Sample Acceptance Test Report and Approval Outline

Acceptance Test Report and Approval Outline

Cover Page

Table of Contents

1. **Purpose**

This section should present a clear, concise statement of the purpose for the Acceptance Test Report.

2. **Scope**

This section identifies the system tested and the test(s) conducted covered by this report. Provide a brief summary of the investment objectives, and identify the Investment Owner and users.

3. **Reference Documents**

This section provides a bibliography of essential investment references and deliverables applicable to acceptance testing. These references might include the Functional Requirements Document, User Manual, Operations Manual, Maintenance Manual, Test Plan, and any prior test reports.

3.1 Security

This section describes any security considerations associated with the system being tested, the test analysis, and the data being handled - such as confidentiality requirements, audit trails, access control, and recoverability. Reference those portions of the document that specifically address system security issues, if any.

3.2 Glossary

This section defines all terms and provides a list of abbreviations used in the test analysis report. If the list is several pages in length, it may be placed as an appendix.

4. **Test Analysis**

This section describes the results of each test performed. It should include verification of access control and system standards, functionality, and error process. Repeat the subsections of this section for each test performed.

4.1 Test Name (repeat for each test)

The test performed for the specified system is discussed in this section. For each test, provide the subsequent sections.

4.1.1 System Functions

A high-level description of the functions tested and a description of system capabilities designed to satisfy *these functions are contained in this section. Each system function should be described separately.*

4.1.2 Functional Capability

This section evaluates the performance of each function demonstrated in the test. This section also assesses the manner in which the test environment may be different from the operational environment and the effect of this difference on functional capabilities.

4.1.3 Performance Capability

This section quantitatively compares the system performance characteristics with the criteria stated in the test plan. The comparison should identify deficiencies, limitations, and constraints detected for each function during testing. If appropriate, a test history or log can be included as an appendix.

5. Software and Hardware Requirements Findings

This section summarizes the test results, organized according to the numbered requirements listed in the Traceability section of the test plan. Each numbered requirement should be described in a separate section. Repeat the subsections of this section for each numbered requirement covered by the test plan.

5.1 Requirement Number and Name (repeat for each test)

The requirement number provided in the title to this section is the number from the requirements traceability matrix in the Test Plan and the name provided is the requirement's short name.

5.1.1 Findings

This subsection briefly describes the requirement, including the software and hardware capabilities, and states the findings from one or more tests.

5.1.2 Limitations

This subsection describes the range of data values tested, including dynamic and static data, for this requirement and identifies deficiencies, limitations, and constraints detected in the software and hardware during the testing.

6. Summary and Conclusions

6.1 Demonstrated Capabilities

This section provides an overview and summary analysis of the acceptance-testing program. Describe the overall capabilities and deficiencies of the test activity. In cases where tests were intended to demonstrate one or more specific performance requirements, findings should be presented that compare the test results with the performance requirements. Include an assessment of any differences in the test environment versus the operational environment that may have had an effect on the demonstrated capabilities. Provide a statement, based on the results of acceptance testing concerning the adequacy of the system or module to meet overall security requirements.

6.2 System Deficiencies

This section describes acceptance test results showing system deficiencies. Identify all problems by name and number when placed under configuration control. Describe the cumulative or overall effect of all detected deficiencies on the system of module. Generate Test Problem Reports for each deficiency as required. If the Test Problem Reports are tracked in an automated database, then include reports extracted from the database in an appendix.

6.3 System Refinements

This section itemizes any indicated improvements in system design or operation based on the results of the test period. Accompanying each improvement or enhancement suggested should be a discussion of the added capability it provides and the effect on the system design. Name and requirement number when placed under configuration control should indicate the improvements.

6.4 Recommendations and Estimates

This section provides a statement describing the overall readiness for system implementation. For each deficiency, address the effect on system performance and design. Include any estimates of time and effort required for correction of each deficiency and any recommendations on the following: the urgency of each correction; parties responsible for corrections; and recommended solution or approach to correcting deficiencies.

6.5 Test Problem Report

This section contains copies of Test Problem Reports related to the deficiencies found in the test results. Test Problem Reports will vary according to the IT system development investment, its scope and complexity, etc.

6.6 Test Analysis Approval

This section contains a brief summary of the perceived readiness for migration of the software as a result of acceptance testing. In the case of a user acceptance test, it serves as the user's recommendation for migration to production.

Training Plan (TP)

The TP outlines the objectives, needs, strategy, and curriculum to be addressed when training users on the new or enhanced information system. The plan presents the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks. A sample outline for a TP is shown is Exhibit 7.

Exhibit 7: Sample Training Plan Outline

Training Plan Outline

Cover Page

Table of Contents

1. Introduction

This section provides a management summary of the entire plan. It is not required to provide information in this section if the descriptions provided in the subsequent sections are sufficient.

1.1 Background and Scope

This section provides a brief description of the investment from a management perspective. It identifies the system, its purpose, and its intended users. This section also provides a high-level summary of the training plan and its scope.

1.2 Points of Contact

This section provides the organization name (code) and the titles of key points-of-contact for system development. It includes such points-of-contact as the Project Manager, QA Manager, Security Manager, Training Coordinator, and Training representative, as appropriate.

1.3 Document Organization

The organization of the training plan is described in this section.

1.4 Investment References

This section provides a bibliography of key investment references and deliverables that have been produced before this point. For example, these references might include the PMP, FRD, Test Plan, Implementation Plan, and preliminary and detailed design documents.

1.5 Security and the Privacy Act

If applicable, this section provides a brief discussion of the system's security controls and the need for security and protection of sensitive DOL data. If the system handles sensitive or Privacy Act information, information should be included about labeling system outputs as sensitive or Privacy Act-related. In addition, if the Privacy Act protects the system, include a notification of the Privacy Act's civil and criminal penalties for unauthorized use and disclosure of system data.

1.6 Glossary

This section is a glossary of all terms and abbreviations used in the plan. If it is several pages in length, it *may be placed as an appendix.*

2. Requirements Traceability (optional)

If applicable, this section presents a traceability matrix that lists user requirements as documented in the FRD and traces how they are addressed in such documents as preliminary and final design documents, test plans, and training plans. Cross-reference the user requirements and training needs in the appropriate sections of the Training Plan. The requirements matrix may be broken into segments, if appropriate. For example, provide a separate matrix of the training plan sections that trace to particular sections in the Detailed Design Document, preliminary design, FRD, and the Statement of Work.

3. Instructional Analysis

3.1 Development Approach

This section discusses the approach used to develop the course curriculum and ensure quality-training products. This description includes the methodology used to analyze training requirements in terms of performance objectives and to develop course objectives that ensure appropriate instruction for each target group. The topics or subjects on which the training must be conducted should be listed or identified.

3.2 Issues and Recommendations

Any current and foreseeable issues surrounding training are included in this section. Recommendations for resolving each issue and constraints and limitations should also be listed.

3.3 Needs and Skills Analysis

This section describes the target audiences for courses to be developed. Target audiences include technical professionals, user professionals, data entry clerks, clerical staff members, automated data processing (ADP), non-ADP managers, and executives. The tasks that must be taught to meet objectives successfully and the skills that must be learned to accomplish those tasks are described in this section. A matrix may be used to provide this information. In addition, the training needs for each target audience are discussed in this section. If appropriate, this section should discuss needs and courses in terms of staff location groupings, such as headquarters and field offices.

4. Instructional Methods

4.1 Training Methodology

This section describes the training methods to be used in the proposed courses. These methods should relate to the needs and skills identified in Section 3.3, Needs and Skills Analysis, and should take into account such factors as course objectives, the target audience for a particular course, media characteristics, training setting criteria, and costs. The materials for the chosen training approach (such as course outlines, audiovisual aids, instructor and student guides, student workbooks, examinations, and reference manuals) should be listed or discussed in this section. Sample formats of materials can be included in an appendix, if desired.

4.2 Training Database

If applicable, this section identifies and discusses the training database and how it will be used during computer systems training. It discusses the simulated production data related to various training scenarios and cases developed for instructional purposes. This section also explains how the training database will be developed. If this section is not applicable to the system involved, indicate "Not applicable."

4.3 Testing and Evaluation

This section describes methods used to establish and maintain QA over the curriculum development process. This description should include methods used to test and evaluate training effectiveness, evaluate student progress and performance, and apply comments to modify or enhance the course materials and structure.

5. Training Resources

5.1 Course Administration

This section describes the methods used to administer the training program, including procedures for class enrollment, student release, reporting of academic progress, course completion and certification, *monitoring of the training program, training records management, and security, as required.*

5.2 Resources and Facilities

This section describes the resources required by both instructors and students for the training, including classroom, training, and laboratory facilities; equipment such as an overhead projector, projection screen, flipchart or visual aids panel with markers, and computer and printer workstations; and materials such as memo pads and pencils, diskettes, viewgraphs, and slides.

5.3 Schedules

This section presents a schedule for implementing the training strategy and indicating responsible parties. Included are key tasks to be completed, such as when to set up training facilities and schedule participants; other activities essential to training; and dates on which those tasks and activities must be finished. This section provides an overview of tasks; deliverables, such as approach and evaluation forms; scheduled versus actual milestones; and estimated efforts, such as the work plan. In the final version of the Training Plan, actual course schedules by location should be included.

5.4 Future Training

This section discusses scheduled training modifications and improvements. This information can include periodic updating of course contents, planned modifications to training environments, retraining of employees, and other predicted changes. Indicate procedures for requesting and developing additional training.

6. Training Curriculum

This section provides descriptions of the components that make up each course. If a large number of courses or modules is described, place these descriptions in an appendix. Subsections of this section, if any, should be created for each course. Each course may comprise one or more modules. A course description should be developed for each module. At a minimum, each course description should include the course/module name; the length of time the course/module will take; the expected class size (minimum, maximum, optimal); the target audience; course objectives; module content/syllabus; specific training resources required, such as devices, aids, equipment, materials, and media to be used; and any special student prerequisites. The course description could also include information on instructor-to student ratio, total number of students to be trained, estimated number of classes, location of classes, and testing methods.

Systems Administration Manual (SAM)

A SAM serves the purpose of an operations manual in distributed (client/server) applications. A sample outline for a SAM is shown in Exhibit 8.

Exhibit 8: Sample Systems Administration Manual Outline

Systems Administration Manual Outline

Cover Page

Table of Contents

1. General

1.1 Introduction and Purpose

This section introduces and describes the purpose of the Systems Administration Manual, the name of the system to which it applies, and the type of computer operation.

1.2 Investment References

This section lists, as appropriate, the User Manual, Maintenance Manual, and other pertinent available systems documentation.

1.3 Glossary

This section lists all definitions or terms unique to this document or computer operation and subject to interpretation by the user of this document.

2. System Overview

2.1 System Application

This section provides a brief description of the system, including its purpose and uses.

2.2 System Organization

This section describes the organization of the system by the use of a chart depicting components and their interrelationships.

2.3 Information Inventory

This section provides information about data files, and databases that are produced or referenced by the system.

2.3.1 Resource Inventory

This section lists all permanent files and databases that are referenced, created, or updated by the system.

2.3.2 Report Inventory

This section lists all reports produced by the system, including each report name and the Software that generates it.

2.4 Processing Overview

This section provides information that is applicable to the processing of the system. It includes system restrictions, waivers of operational standards, and interfaces with other systems.

2.5 Communications Overview

This section describes the communications functions and process of the system.

2.6 Security

This section describes the security considerations associated with the system.

2.7 Privacy Act Warning

If the Privacy Act covers the system, then this section provides the appropriate Privacy Act notice and warning.

3. Site Profile(s)

This section contains information pertaining to the site(s) where the application is running. That information includes the information contained in the subsequent sections.

3.1 Site Location(s)

This is the official address(es) of the site(s).

3.2 Primary Site

For the site(s) designated as primary, this section describes the essential personnel names and telephone numbers for the automated data processing site contacts.

4. Systems Administration

This section introduces the responsibilities of the System Administrator, as discussed in the subsequent sections.

4.1 User and Group Accounts

This section introduces topics related to system users.

4.1.1 Adding/Deleting Users

This section describes procedures to create/delete user logins and password accounts.

4.1.2 Setting User Permissions

This section describes procedures to give users/restrict access to certain files.

4.1.3 Adding/Deleting User Groups

This section contains procedures to create/delete user groups.

4.2 Server Administration

This section describes procedures to setup servers, including naming conventions and standards.

4.2.1 Creating Directories

This section describes procedures to create server directories.

4.2.2 Building Drive Mappings

This section describes procedures to create server drive mappings.

4.3 System Backup Procedures

This section describes procedures for regularly scheduled backups of the entire network, including data storage, and the creation and storage of backup logs.

4.3.1 Maintenance Schedule

This section describes documented daily and weekly backup schedules and procedures.

4.3.2 Off-Site Storage

This section describes the location, schedule, and procedures for off-site storage.

4.3.3 Maintenance of Backup Log

This section describes procedures for creating and maintaining backup logs.

4.4 Printer Support

This section discusses procedures for installing, operating, and maintaining printers.

4.4.1 Maintenance

This section describes maintenance contracts, procedures, and equipment information (Configurations, Toner, Etc.).

4.4.2 Print Jobs

This section describes procedures to monitor, delete, and prioritize print jobs.

4.5 System Maintenance

This section discusses procedures for maintaining the file system.

4.5.1 Monitoring Performance and System Activity

This section contains procedures to monitor system usage, performance, and activity. This may include descriptions of system monitoring tools, the hours of peak demand, a list of system maintenance schedules, etc.

4.5.2 Installing Programs and Operating System Updates

This section includes procedures on how and when to install operating system updates.

4.5.3 Maintaining Audit Records

This section describes procedures to setup and monitor system audit trails.

4.5.4 Maintenance Reports

This section includes procedures to create and update maintenance reports.

4.6 Security Procedures

This section describes the process for obtaining identifications (IDs) and passwords. It includes information concerning network access and confidentiality requirements.

4.6.1 Issuing IDS and Passwords

This section describes procedures for issuing IDs and passwords.

4.6.2 License Agreements

This section describes licensing agreements and procedures for ensuring that all licenses are current.

4.7 Network Maintenance

This section describes procedures to maintain and monitor the data communications network.

4.7.1 LAN Design

This section contains a layout of the network.

4.7.2 Communications Equipment

This section contains a layout of the telecommunications equipment.

4.8 Inventory Management

This section contains a complete hardware and software inventory to include make, model, version numbers, and serial numbers.

4.8.1 Maintaining Hardware and Software Configurations

This section describes procedures for maintaining the configuration information for the hardware and software actually installed.

4.8.2 Maintaining Floor Plans

This section describes procedures for maintaining floor plans showing the location of all installed equipment.

4.8.3 Installing Software and Hardware

This section describes procedures for installing new or upgraded hardware and software.

4.8.4 Maintaining Lists of Serial Numbers

This section describes procedures for maintaining all serial number lists required at a site.

4.8.5 Maintaining Property Inventory

This section describes procedures for maintaining a property inventory at the site.

4.9 Training the Backup Administrator

This section describes how to train a backup administrator.

4.10 Procedures for End-User Support

This section provides necessary end-user contact information and the procedures for providing end-user support.

4.10.1 Escalation Procedures

This section describes the formal escalation procedures to be used by System Administrators in response to priority user problem resolution requests.

4.11 Documentation

This section describes the documentation required of System Administrators as they perform system administration.

4.11.1 Troubleshooting Issues

This section describes how to conduct and document troubleshooting activities.

User Manual (UM)

The UM contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and systematic procedures for system access and use. Use graphics where possible in this manual. A sample UM is shown in Exhibit 9.

Exhibit 9: Sample User Manual Outline

User Manual Outline

Cover Page

Table of Contents

1. Introduction

1.1 Purpose and Scope

This section provides a description of the purpose and scope of the User Manual.

1.2 Organization

This section describes the organization of the User Manual.

1.3 Points of Contact

This section identifies the organization codes and staff (and alternates if appropriate) who may assist the system user. If a help desk facility or telephone assistance organization exists, describe it in this section.

1.4 Investment References

This section provides a bibliography of key investment references and deliverables that have been produced before this point in the system development process. References might include the quality assurance plan, Configuration Management Plan, FRD, preliminary design, or Detailed Design Document.

1.5 Primary Business Functions

This section discusses the business perspective of the user's primary responsibilities and tasks as they are supported by the system. Introduce the business functions so that the focus may rest on the systematic steps to support the business functions in later sections.

1.6 Glossary

This section provides a glossary of all terms and abbreviations used in the manual. If the glossary is several pages or more in length, it may be placed as an appendix.

2. System Capabilities

This section provides a brief overview of the system and its capabilities.

2.1 Purpose

This section describes the purpose of the application system.

2.2 General Description

This section provides an overview of the system's capabilities, functions, and operation, including the specific high-level functions performed by the system. Use graphics and tables, if appropriate.

2.3 Privacy Act Considerations

3. Description of System Functions

This section describes each specific function of the system. In this high-level section, describe any conventions to be used in the associated subsections. Each of the subsequent sections should be repeated as often as necessary to describe each function within the system. The term "Function X" in the subsection title is replaced with the name of the function.

3.1 Function X Title

This section provides the title of the specific system function.

3.2 Detailed Description of Function

This section provides a description of each function. Include the following, as appropriate: purpose and uses of the function; initialization of the function, if applicable; execution options associated with this function; description of function inputs; description of expected outputs and results; relationship to other functions; and summary of function operation.

3.3 Preparation of Function Inputs

This section defines required inputs. These inputs should include the basic data required to operate the system. The definition of the inputs include the following: title of each input; description of the inputs, including graphic depictions of display screens; purpose and use of the inputs; input medium; limitations and restrictions; format and content on inputs, and a descriptive table of all allowable values for the inputs; sequencing of inputs; special instructions; relationship of inputs to outputs; and examples.

3.4 Results

This section describes expected results of the function. Include the following in the description, as applicable: description of results, using graphics, text, and tables; form in which the results will appear;

output form and content; report generation; instructions on the use of outputs; restrictions on the use of outputs, such as those mandated by Privacy Act and E-Government Act of 2002 restrictions; relationship of outputs to inputs; function-specific error messages; function-specific or context-sensitive help messages associated with this function; and examples.

4. Operating Instructions

This section provides detailed, step-by-step system operating instructions.

4.1 Initiate Operation

This section contains procedures for system logon and system initialization to a known point, such as a system main menu screen. This initialization procedure should describe how to establish the required mode of operation and set any initial parameters required for operation. Software installation procedures should be included if the software is distributed on diskette and should be downloaded before each use.

4.2 Maintain Operation

This section defines procedures to maintain the operation of the software where user intervention is required.

4.3 Terminate and Restart Operations

This section defines procedures for normal and unscheduled termination of the system operations and should define how to restart the system.

5. Error Handling

This section should address error message and help facilities. Additional information and subsections may be added as necessary. Included in this section should be a list of all possible error messages, including the following: any numeric error codes associated with the error message; a description of the meaning of the error message; and a discussion of how to resolve the error.

6. Help Facilities

This section describes any resident help software or any Service or contractors help desk facility that the user can contact for error resolution. Help Desk telephone numbers should be included.

Security Certification and Accreditation Package

The security certification and accreditation (C&A) process includes completing a Risk Assessment, System Security Plan, Security Test and Evaluation (ST&E), and Certification Statements. Only when these items have been completed can the system be accredited. ST&E involves determining a system's security mechanisms adequacy for completeness and correctness, and the degree of consistency between system documentation and actual implementation. This is accomplished through a variety of assurance methods such as analysis of system design documentation, inspection of test documentation, and independent execution of function testing and penetration testing. Please refer to the DOL Computer Security Handbook for information on the deliverables associated with this package or contact the DOL OCIO Security Office for assistance.

Contingency Plan Test Report

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

Security Accreditation Letter

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

System Acceptance Letter

A system acceptance letter is signed by the Project Manager and the System Owner and verifies that the system has been developed and tested as planned, meets all known requirements, has been successfully implemented, and accepted by both the Project Manager and the System Owner.

A sample System Acceptance letter is shown in Exhibit 10.

Exhibit 10: Sample System Acceptance Letter

System Acceptance Letter

I have carefully considered the requirements for the ____________________ system. Based on reviews of requirements, design documentation, programming, and testing, I have determined that this system conforms to all known requirements and is ready to be installed into production, except for the weaknesses noted in the certification report.

Based upon the report and my judgment, I hereby certify, subject to the corrections recommended in the certification report, that the _________________ system meets all documented and approved requirements.

Weighing the remaining residual risks against operational requirements, I recommend that the _______________________________ system be accredited for continued operation and that the recommendations included in the certification report be implemented.

Signed ___________________________________ Date ______________
Project Manager

I am in concurrence with the above and formally accept the ______________________ system.

Signed ___________________________________ Date ______________
System Owner

Security Controls Test Report / Continuous Monitoring Annual Report

Please refer to the DOL Computer Security Handbook (Volume 4) for information on the deliverables associated with these reports including (1) Security Self- Assessment, Security Control Assessment Aid (SCAA) and (2) Continuous Monitoring Annual Report.

Security Recertification and Accreditation Package

Please refer to the DOL Computer Security Handbook (Volume 4) for information on the deliverables associated with this package.

Security Self-Assessment (Annual)

Please refer to the DOL Computer Security Handbook for information on this deliverable, including a template.

Disposition Plan (DP)

The DP is the most significant deliverable in the disposition of the information system, and the plan will vary according to the system and DOL requirements. The objectives of the plan are to end the operation or the system in a planned, orderly manner and to ensure that system components (i.e., hardware, software, data, and documentation) are properly archived or incorporated into other systems. At the end of this task, the system will no longer exist as an independent entity. The completion of the systems life cycle is carefully planned and documented to avoid disruption to the organizations using the system or the operation of other systems that use the data and/or software of the present system. A sample template for a DP is provided in Exhibit 11.

Exhibit 11: Sample Disposition Plan Outline

Disposition Plan Outline

Cover Page

Table of Contents

1. Introduction

This section provides a brief description of introductory material.

1.1 Purpose and Scope

This section describes the purpose and scope of the Disposition Plan. Reference the information system name and provide identifying information about the system-undergoing disposition.

1.2 Points of Contact

This section identifies the System Owner. Provide the name of the responsible organization and staff (and alternates, if appropriate) who serve as points of contact for the system disposition. Include telephone numbers of key staff and organizations.

1.3 Investment References

This section provides a bibliography of key investment references and deliverables that have been produced before this point in the investment development. These documents may have been produced in a previous engineering life cycle that resulted in the initial version of the system now undergoing disposition or may have been produced in subsequent enhancement efforts.

1.4 Glossary

This section contains a glossary of all terms and abbreviations used in the plan. If it is several pages in length, it may be placed in an appendix.

2. System Disposition

2.1 Notifications

This section describes the plan for notifying known users of the system being shut down, as well as other affected parties, like those responsible for other interfacing systems and operations staff members involved in running the system.

2.2 Data Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the data files and related documentation in the system being shut down.

2.3 Software Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the software library files and related documentation in the system being shut down.

2.4 System Documentation Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the hardcopy and softcopy systems and user documentation for the system being shut down.

2.5 Equipment Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the hardware and other equipment used by the system being shut down.

3. Investment Closedown

3.1 Investment Staff

This section describes the plan for notifying investment team members of the shutdown of the system, and the transfer of these team members to other investments.

3.2 Investment Records

This section describes the plan for archiving, deleting, or transferring to other investments the records of investment activity for the investment that has been maintaining the system being shut down.

3.3 Facilities

This section describes the plan for transferring or disposing of facilities used by the investment staff for the system being shut down.

Additional Deliverables

Requirements Traceability Matrix (RTM)

The RTM provides a method for tracking the functional requirements and their implementation through the development process. It may be part of the Functional Requirements Document (see Exhibit 1), or produced separately Exhibit 12 illustrates a sample RTM.

Exhibit 12: Sample Requirements Traceability Matrix

Functional Requirement		*Verification Method				Test Plan Reference
Description	**Paragraph Reference**	**A**	**I**	**D**	**T**	**Test Plan Reference**
The functionality of the Enhanced Primary Verification Process will be an expansion of the functionality of the point of sale (POS) emulation logic that is currently in place to support primary verification queries to ASVI.	3.2-01				X	TC 2.3.1.6
The 200 employers who will be part of the Phase II TVS Pilot will submit data	3.2-02				X	TC 2.3.1.6

Functional Requirement		***Verification Method**				**Test Plan Reference**
Description	**Paragraph Reference**	**A**	**I**	**D**	**T**	**Test Plan Reference**
electronically via an interface with the ASVI system.						
All secondary information will be passed electronically to the LA FCO from ASVI for secondary verification.	3.2-03				X	TC 2.3.1.10
After a determination has been made on a case, the status verifier will then send the response back to the employer electronically; the return path is the exact opposite of the preceding path to the FCO.	3.2-04				X	TC 2.3.1.10
The new system will be capable of tracking information on each case throughout both the primary and secondary verification processes.	3.2-05				X	TC 2.3.1.6, 2.3.1.7, 2.3.1.11

A = ANALYSIS I = INSPECTION D = DEMONSTRATION T = TEST

Test Problem Report (TPR)

The TPR is generated during testing and is attached to the Acceptance Test Report (see Exhibit 6), as appropriate. A sample outline for a TPR is shown in Exhibit 13.

Exhibit 13: Sample Test Problem Report Outline

Test Problem Report Outline

TO: ____

FROM: ____

PREPARER/CONTACT: _________________________ **PHONE**: ________

PROGRAM BEING TESTED: ____

DESCRIPTION OF TEST PROBLEM

A. Expected Results

B. Actual Results

DISPOSITION OF PROBLEM

Action Taken and Date Corrected

Risk Impact if Problem Not Corrected

Changes Required for Existing Documentation

SIGNATURES: ______________________ ______________________
Project Manager System Developer

________________ ________________
Date Date

Maintenance Manual (MM)

The MM provides maintenance personnel with the information necessary to maintain the system effectively. The manual provides the definition of the software support environment, the roles and responsibilities of maintenance personnel, and the regular activities essential to the support and maintenance of program modules, job streams, and database structures. In addition to the items identified for inclusion in the MM, additional information may be provided to facilitate the maintenance and modification of the system. Appendices to document various maintenance procedures, standards, or other essential information may be added to this document as needed. A sample outline for a MM is shown in Exhibit 14.

Exhibit 14: Sample Maintenance Manual Outline

Maintenance Manual Outline

Cover Page

Table of Contents

1. Introduction

This section provides general reference information regarding the maintenance manual. Whenever appropriate, additional information may be added to this section.

1.1 Purpose

In this section, describe the purpose of the manual and reference the system name and identifying information about the system and its programs.

1.2 Points of Contact

This section identifies the organization(s) responsible for system development, maintenance, and use. This section also identifies points-of-contact (and alternate if appropriate) for the system within each organization.

1.3 Investment References

This section provides a bibliography of key investment references and deliverables produced during the information system development life cycle. If appropriate, reference the Functional Requirements document (FRD), preliminary design, Detailed Design Document, Test Plan, Acceptance Test Report, other system manuals (i.e. Operations Manual), and User Manuals.

1.4 Glossary

Provide a glossary with definitions of all terms, abbreviations, and acronyms used in the manual. If the glossary is several pages in length, place it as an appendix.

2. System Description

The subsequent sections provide an overview of the system to be maintained.

2.1 System Application

This section provides a brief description of the purpose of the system, the functions it performs, and the business processes that the system is intended to support. If the system is a database or an information system, include a general description of the type of data maintained, and the operational sources and uses of those data.

2.2 System Organization

In this section, provide a brief description of the system structure, major system components, and the functions of each major system component. Include charts, diagrams, and graphics as necessary.

2.3 Security and the Privacy Act

This section provides an overview of the system's security controls and the need for security and protection of sensitive data.

2.4 System Requirements Cross-Reference

This section contains an exhibit that cross-references the detailed system requirements with the preliminary design document, final design document, and test plans. This document, also called a traceability matrix in other documents, assists maintenance personnel by tracing how the user requirements developed in the FRD are met in other products of the life cycle. Because this information is provided in the Detailed Design Document, it may be appropriate to repeat or enhance that information in this section.

3. Support Environment

This section describes the operating and support environment for the system and program(s). Include a discussion of the equipment, support software, database characteristics, and personnel requirements for supporting maintenance of the system and its programs.

3.1 Equipment Environment

This section describes the equipment support environment, including the development, maintenance, and target host computer environments. Describe telecommunications and facility requirements, if any.

3.1.1 Computer Hardware

This section discusses the computer configuration on which the software is hosted and its general characteristics. The section should also identify the specific computer equipment required to support software maintenance if that equipment differs from the host computer. For example, if software development and maintenance are performed on a platform that differs from the target host environment, describe both environments. Describe any miscellaneous computer equipment required in this section, such as hardware probe boards that perform hardware-based monitoring and debugging of software.

3.1.2 Facilities

This section describes the special facility requirements, if any, for system and program maintenance and includes any telecommunications facilities required to test the software.

3.2 Support Software

This section lists all support software such as operating systems, transaction processing systems, and database management systems (DBMSs) as well as software used for the maintenance and testing of the system. Include the appropriate version or release numbers, along with their documentation references, with the support software lists.

3.3 Database Characteristics

This section contains an overview of the nature and content of each database used by the system. Reference other documents for a detailed description, including the preliminary design and final design documents as appropriate.

3.4 Personnel

This section describes the special skills required for the maintenance personnel. These skills may include knowledge of specific versions of operating systems, transaction processing systems, high-level languages, screen and display generators, DBMSs, testing tools, and computer-aided system engineering tools.

4. System Maintenance Procedures

This section contains information on the procedures necessary for programmers to maintain the software. If the conventions follow standard programming practices and a standards document, that document may be referenced, if it is available to the maintenance team.

4.1 Conventions

4.2 Verification Procedures

This section includes requirements and procedures necessary to check the performance of the system following modification or maintenance of the system's software components. Address the verification of the system-wide correctness and performance. Present, in detail, system-wide testing procedures. Reference the original development test plan if the testing replicates development testing. Describe the types and source(s) of test data in detail.

4.3 Error Conditions

This section describes all system-wide error conditions that may be encountered within the system, including an explanation of the source(s) of each error and recommended methods to correct each error.

4.4 Maintenance Software

This section references any special maintenance software and its supporting documentation used to maintain the system.

4.5 Maintenance Procedures

This section describes systematic, system-wide maintenance procedures, such as procedures for setting up and sequencing inputs for testing. In addition, present standards for documenting modifications to the system.

5. Software Unit Maintenance Procedures

For each software unit within the system, provide the information requested. If the information is identical for each of the software units, it is not necessary to repeat it for each software unit.

Operations Manual (OM)

The OM provides computer control personnel and computer operators with a detailed operational description of the information system and its associated environments. A sample outline for an OM is shown in Exhibit 15.

Exhibit 15: Sample Operations Manual Outline

Operations Manual Outline

Cover Page

Table of Contents

1. General

1.1 Introduction and Purpose

Describe the introduction and purpose of the Operations Manual, the name of the system to which it applies, and the type of computer operation.

1.2 Investment References

List, as appropriate, the User Manual, Maintenance Manual and other pertinent documentation.

1.3 Glossary

List any definitions or terms unique to this document or computer operation and subject to interpretation by the user of this document.

2. System Overview

2.1 System Application

Provide a brief description of the system, including its purpose and uses.

2.2 System Organization

Describe the operation of the system by the use of a chart depicting operations and interrelationships.

2.3 Software Inventory

List the software units, to include name, identification, and security considerations. Identify software *necessary to resume operation of the system in case of emergency.*

2.4 Information Inventory

Provide information about data flies and databases that are produced or referenced by the system.

2.4.1 Resource Inventory

List all permanent files and databases that are referenced, created, or updated by the system.

2.4.2 Report Inventory

List all reports produced by the system. Include report name and the software that generates it.

2.5 Processing Overview

Provide information that is applicable to the processing of the system. Include system restrictions, waivers of operational standards, and interfaces with other systems.

2.6 Communications Overview

Describe the communications functions and process of the system.

2.7 Security

Describe the security considerations associated with the system.

2.8 Privacy Act Warning

Include a Privacy Act warning if the Privacy Act covers the system.

3. Description of Runs

3.1 Run Inventory

List the runs showing the software components, the job control batch file names, run jobs, and purpose of each run if any portion of the system is run in batch mode. For online transaction-based processing, provide an inventory of all software components that must be loaded for the software system to be operational.

3.2 Run Sequence

Provide a schedule of acceptable phasing of the software system into a logical series of operations. If the system is a batch system, provide the execution schedule, which shows, at a minimum, the following: job dependencies; day of week/ month/date for execution; time of day or night (if significant); and expected run time in computer units.

3.3 Diagnostic Procedures

Describe the diagnostic or error-detection features of the system, the purpose of the diagnostic features and the setup and execution procedures for any software diagnostic procedures.

3.4 Error Messages

List all error codes and messages with operator responses, as appropriate.

3.5 Run Descriptions

Provide detailed information needed to execute system runs. For each run, include the information discussed in the subsequent sections.

3.5.1 Control Inputs

Describe all operator job control inputs; for example, starting the run, selecting run execution options, activating an online or transaction-based system, and running the system through remote devices, if appropriate.

3.5.2 Primary User Contact

Identify the user contacts (and alternate if appropriate) for the system, including the person's name, organization, address, and telephone number.

3.5.3 Data Inputs

Describe the following if data input is required at production time: who is responsible for the source data; format of the data; data validation requirements; and disposition of input source and created data.

3.5.4 Output Reports

Identify the report names, distribution requirements, and any identifying numbers expected to be output *from the run. Describe reports to be produced from the system run by other than standard means.*

3.5.5 Restart/Recovery Procedures

Provide instructions by which the operator can initiate restart or recovery procedures for the run.

3.5.6 Backup Procedures

Provide instructions by which the operator can initiate backup procedures. Cross reference applicable instructions with procedures in the Contingency Plan.

3.5.7 Problem Reporting/Escalation Procedure

Provide instructions for reporting problems to a point of contact. Include the person's name and telephone numbers (that is, office, home, pager, etc.).

SDLCM Phase Gate Review Checklists

The DOL OCIO has created phase gate review checklists for IPT teams to use in performing SDLCM phase gate reviews. A copy of the checklists can be found in Appendix VII.

APPENDIX VI – Strategic Planning Discussion

Information Technology Systems are required to support DOL's strategic goals. Strategic planning is not part of the SDLCM, but it influences what information systems investments are to be initiated and will continue to receive funding. A description of the strategic planning process is outside the scope of the SDLCM; however, there are several important activities that affect an investment's life cycle. They are described below.

Strategic Management Process

DOL has defined the strategic management process in the "Information Technology Architecture, Phase I: Mission Critical Baseline Characterization and Opportunity Assessment, March 16, 2000." The aim of the strategic management process is to identify potential improvements to DOL information systems and to gain commitment of the required resources to change these systems. This strategic management process ensures that effective plans are deployed and that the "return on investment" is an essential measure of performance. It enables each individual application systems investment to develop detailed plans that support the overall DOL effort, while solving investment-specific problems.

Business Process Reengineering

Business process reengineering (BPR) is performed to change the way an organization conducts its business. BPR is the redesign of the organization, culture, and its business processes to achieve significant improvements in costs, time, service, and quality. It complements and augments the strategic management process, and may result in the initiation of an application systems investment(s). BPR is performed before initiation of an application systems investment.

APPENDIX VII – 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/or 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:		***Level of Integrity* *4 3 2 1 - Circle***			
		CPIC Threshold			
	SDLCM - Conceptual Planning Phase	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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
		CPIC Threshold			
	SDLCM - Planning and Requirements Phase	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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
	SDLCM - Design Phase	**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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
	SDLCM - Development and Test Phase	**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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
	SDLCM - Implementation Phase	**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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
	SDLCM - Operations and Maintenance Phase	**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:		***Level of Integrity*** ***4 3 2 1 - Circle***			
	SDLCM – Disposition Phase	**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 VIII – List of Acronyms

Acronym	Definition
AA	Application Architecture
AP	Acquisition Plan
ATO	Authority To Operate
ATR	Acceptance Test Report
BPR	Business Process Reengineering
CBA	Cost Benefit Analysis
CCA	Clinger Cohen Act
CIO	Chief Information Officer
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COTS	Commercial Off-the-Shelf
CPIC	Capital Planning and Investment Control
CPC	IT Capital Planning Committee
CSAM	Cyber Security Assessment and Management
CSH	Computer Security Handbook
CSPP	Cyber Security Program Plan
CSO	Computer Security Officer
DA	Data Architecture
DAA	Designated Accrediting Authority
DDD	Detailed Design Document
DGS	Digital Government Strategy
DLMS	Department of Labor Manual Series
DP	Disposition Plan
DOL	Department of Labor
EA	Enterprise Architecture
eCPIC	Electronic Capital Planning and Investment Control
EIC	Enterprise Implementation Committee
EVM	Earned Value Management
EVMS	Earned Value Management System
FAQ	Frequently Asked Question
FAC P/PM	Federal Acquisition Certification for Program and Project Managers
FITF	Field IT Forum
FISMA	Federal Information Security Management Act
FOIA/PA	Freedom of Information Act/Privacy Act
FRD	Functional Requirements Document
GOTS	Government-Of-The-Shelf
IATO	Interim Authority To Operate
IBR	Integrated Baseline Review
IMLC	Investment Management Life Cycle
IP	Implementation Plan

Acronym	Definition
IPT	Integrated Project Team
IRM	Information Resource Management
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
LAN	Local Area Network
LCC/B	Life Cycle Cost/ Benefit
MOU	Memoranda of Understanding
MOU/A	Memoranda of Understanding/Agreement
NPV	Net Present Value
NIST	National Institute for Standards and Technology
O&M	Operations & Maintenance
OA	Operational Analysis
OCIO	Office of the Chief Information Officer
OASAM	Office of Assistant Secretary for Administration and Management
OMB	Office of Management and Budget
OPA	Office of Public Affairs
PA	Performance Architecture
PA	Privacy Act
PIR	Post Implementation Review
PKI	Public Key Infrastructure
PM	Project Manager
PMB	Performance Measurement Baseline
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
PRA	Paperwork Reduction Act
PRM	Performance Reference Model
Q&A	Question and Answer
QA	Quality Assurance
RA	Risk Assessment
RITS	Request for Information Technology Services
RMP	Risk Management Plan
ROI	Return On Investment
RR	Risk Register
SAM	Systems Administration Manual
SBAC	Strategic Business Alignment Committee

Acronym	Definition
SBM	Strategic Business Management
SCAA	Security Control Assessment Aid
SDLCM	System Development Life Cycle Management
SDLCMM	System Development Life Cycle Management Manual
SOW	Statement of Work
ST&E	Security Test & Evaluation
SW	Software
T&IF	Technology & Innovation Forum
TA	Target Architecture
TP	Test Plan
TP	Training Plan
TS&SP	Transition Strategy and Sequencing Plan
UM	User Manual
WAN	Wide Area Network
WBS	Work Breakdown Structure (WBS)