NOT MEASUREMENT SENSITIVE

DOE G 413.3-14
9-12-08

Information Technology Project Guide

[*This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not construed as requirements in any audit or appraisal for compliance with the parent Policy, Order, Notice, or Manual.*]

U.S. Department of Energy
Office of the Chief Information Officer

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of the Chief Information Officer

TABLE OF CONTENTS

SECTION 1.0. INTRODUCTION

1.1 Purpose

This Guide provides the Department of Energy (DOE) recommended guidelines to ensure that the acquisition of information technology (IT) capital assets is performed in compliance with DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, dated 7-28-06. This guide is written for the benefit of the federal project director, the IT project manager, the integrated project team, the program manager (if applicable), the program office, and the acquisition executive.

The guide is dissimilar to other DOE 413.3-series guides because rather than focusing on a single acquisition process topic or phase, the guide covers all process phases where IT-specific guidance is relevant and necessary.

This Guide is intended to be used in tandem with other DOE 413.3-series guides. Section 1.3 provides exclusive guidance for IT-specific project requirement areas identified in DOE O 413.3A and IT-specific guidance for requirement areas more fully addressed in other DOE 413.3-series guides. In instances where requirement areas are applicable to IT projects but wholly addressed in other DOE 413.3-series guides, Section 1.3 refers the reader to the appropriate guide. Requirement areas not applicable to IT projects are omitted from the Guide.

Section 2.0 contains supplemental guidance for the planning, programming, budgeting, and acquisition of IT capital assets consistent with the Clinger-Cohen Act of 1996, P.L. 104-208, and the following Office of Management and Budget (OMB) Circulars

- OMB Circular A-11, Preparation, Submission, and Execution of Budget, Part 7, Planning, Budgeting, Acquisition and Management of Capital Assets;
- OMB Circular A-123, Management’s Responsibility for Internal Control; and
- OMB Circular A-130, Management of Federal Information Resources

The source material identified in Section 2.0 should be considered the primary point of reference and requirements related to the information provided therein.

1.2 Scope

The guidance provided herein applies to any departmental IT project satisfying the applicability criteria set forth in DOE O 413.3A.

1.3 Mapping of DOE O 413.3A to IT Project Management

The following table lists the project requirement areas, identified in DOE O 413.3A, that pertain exclusively to IT projects or IT-focused portions of projects, or for which IT-specific guidance exists, along with IT project documents and/or activities corresponding to the requirement area. Requirement areas that are not applicable to IT projects are omitted from the table, and a

reference to the appropriate DOE 413.3-series guide is provided in instances where a requirement area is applicable to an IT investment but is wholly addressed by another guide.

Table 1: Guidance for IT-related DOE O 413.3A Critical Decision Phases

ORDER 413.3A REQUIREMENT AREA	CORRESPONDING IT PROJECT DOCUMENTS/ACTIVITIES
CD-0 Requirement Areas	
Pre-conceptual planning	Perform pre-conceptual planning activities such as preparing summary requirements description, order-of-magnitude cost estimate and preliminary schedule
Mission need statement	• Refer to the DOE 413.3-series guide related to this topic on developing a mission needs statement • Develop an initial Exhibit 300 according to the requirements identified in OMB Circular A-11, *Part 7, Planning, Budgeting, Acquisition and Management of Capital Assets*
Tailoring strategy	Refer to the DOE 413.3-series guide related to this topic on developing a project execution plan
Mission validation independent project review	Refer to the DOE 413.3-series guide related to this topic on developing a performance baseline and baseline management
Departmental Enterprise Architecture framework	• Ensure that IT investment alignment and compliance with the DOE target Enterprise Architecture (EA). Program offices are responsible for working collaboratively with the DOE EA program and coordinating efforts to ensure integration with the Department-wide architecture • For new investments, notify the Office of the Chief Information Officer's (OCIO) capital planning team of the new investment and complete summary documentation to determine the investment's alignment to the EA
CD-1 Requirement Areas	
Conceptual design report	Refer to DOE G 200.1-1, *Software Engineering Methodology*, dated 5-21-97.
Acquisition strategy	• Refer to the DOE 413.3-series guide related to this topic on developing an acquisition strategy • Include Section 508 requirements, as defined in the Section 508 of the Rehabilitation Act of 1973, as amended, for IT acquisitions • Include requirements defined in OMB Memorandum 07-18 • Determine and include cyber security requirements including configurations found at http://checklists.nist.gov

ORDER 413.3A REQUIREMENT AREA	CORRESPONDING IT PROJECT DOCUMENTS/ACTIVITIES
Project execution plan	Refer to the DOE 413.3-series guide related to developing a project execution plan and the DOE 413.3-series guide related to developing a risk management plan and risk assessment
Federal project director	Federal project director and/or IT project manager who is appointed should be qualified at the appropriate level according to OCIO IT Project Management Qualification Requirements located at http://cio.energy.gov
Integrated project team	• Establish integrated project team (IPT) • Prepare IPT charter and responsibility assignment matrix
Design review	Review preliminary system description document (SDD)
Integrated safety management	Refer to DOE P 226.1 as appropriate
Preliminary security vulnerability assessment report	• Conduct a cyber security risk assessment in accordance with organizational program cyber security plan (PCSP) • Update risk management plan (if applicable)
Initial system security plan	Prepare an initial system security plan to document required security controls in accordance with DOE O 205.1A, other Departmental cyber security directives, and organizational PCSP
Quality assurance program	• Refer to the DOE 413.3-series guide related to this topic on developing Quality Assurance Programs • Develop Plan of Action and Milestones (POA&M) for the system
CD-2 Requirement Areas	
Performance baseline	• Refer to the DOE 413.3-series guide related to this topic on developing a performance baseline and baseline management • Report performance baseline in OMB Exhibit 300
Project execution plan	• Update system development documentation • Update OMB Exhibit 300 to reflect changes to system project management documentation

ORDER 413.3A REQUIREMENT AREA	CORRESPONDING IT PROJECT DOCUMENTS/ACTIVITIES
Earned value management system (EVMS)	• Employ an American National Standard Institute (ANSI) Standard compliant EVMS for IT investments where the life cycle development/modernization/enhancement (D/M/E) funding is greater than $20M and D/M/E funding is greater than $5 million in either the Current Year (CY) and/or Budget Year (BY) • For investments required to employ an ANSI Standard compliant EVMS, report actual cost and schedule data on a monthly basis in OECM's Project Assessment and Reporting System
Performance baseline validation external independent review or performance baseline validation independent project review	• Conduct an independent baseline review, in accordance with OMB Memorandum 05-23 • Complete and submit an Integrated Baseline Review Summary Report to the OCIO, indicating that the review was completed and identifying any findings from the review
Independent cost estimate or independent cost review	Refer to the DOE 413.3-series guide related to this topic on Cost Estimating for additional information
Quality Assurance Program	Refer to the DOE 413.3-series guide related to this topic to ensure that the investment's Quality Assurance Program acceptable and continues to apply
Preliminary design	Create system design document. Refer to DOE G 200.1 as related to systems design documentation.
Design review	Conduct design review of preliminary System Design Documentation
Preliminary security vulnerability assessment report	• Update the cyber security risk assessment • Update risk management plan (if applicable)
Initial system security plan	Update the system security plan
CD-3 Requirement Areas	
Final design	Review final system description documents
Update CD-2 project documentation and required approvals	Update system description documents
Preliminary security vulnerability assessment report	• Update the cyber security risk assessment as needed • Update risk management plan (if applicable)

ORDER 413.3A REQUIREMENT AREA	CORRESPONDING IT PROJECT DOCUMENTS/ACTIVITIES
System security plan	• Update the system security plan as needed • Draft Security Test and Evaluation procedures and prepare for security testing
Quality Assurance Program	Update Quality Assurance Program, in accordance with the DOE 413.3-series guide related to this topic
CD-4 Requirement Areas	
Key performance parameters or project completion criteria	Complete system performance/testing report
Readiness assessment or operational readiness review	Complete initial readiness assessment or operational readiness review as required
Checkout, testing, and commissioning plan	Complete final system testing and issue final system design documentation
Project transition to operations plan	Complete final operations and support plan
Quality assurance plan	Issue an updated quality assurance plan, in accordance with the DOE 413.3 series guide related to this topic
Security vulnerability assessment report	Finalize risk assessment
System security plan and certification and accreditation	• Finalize system security plan • Complete security certification testing and obtain authority to operate (ATO) in accordance with the certification and accreditation process defined in Departmental cyber security directives and organizational PCSP • Identify and track security deficiencies in plans of action and milestones (POA&Ms)
Post CD-4 Requirement Areas	
Final project closeout report	• Prepare a close-out Exhibit 300 and submit to the OCIO • Report dates when the system will be terminated, as well as the actual cost, schedule, and performance data for the final year of operation
Lessons learned report	Refer to post implementation review guidance below for guidance on conducting lessons learned

ORDER 413.3A REQUIREMENT AREA	CORRESPONDING IT PROJECT DOCUMENTS/ACTIVITIES
Operational documentation	• For steady-state components of investments, conduct operational analyses and maintenance in accordance with OMB Circular A-11 • Report operational analysis summary in Exhibit 300 and in the OCIO's Operational Analysis Summary Results Template
Post implementation review	• Within six to eighteen months of becoming operational, conduct a post implementation Review (PIR) to ensure projected costs/benefits were achieved. Summarize the results of the assessment in the Exhibit 300 (guidance for conducting a PIR is available from the OCIO). • Develop lessons learned when conducting the PIR to share among the DOE project management community • Conduct Continuous Monitoring in accordance with cyber security directives and organizational PCSP

SECTION 2.0. SUPPLEMENTAL IT PROGRAM AND PROJECT INFORMATION

This section provides guidance for ensuring that IT capital assets conform to established departmental IT program and project management processes.

2.1 IT Program Management Processes

The integration of IT program management processes into the initiation phase of an IT capital asset includes strategic planning, enterprise architecture (EA), project management, CPIC, acquisition, security and privacy.

Figure 1 illustrates how these processes are interrelated, spanning from strategic planning to individual IT projects.

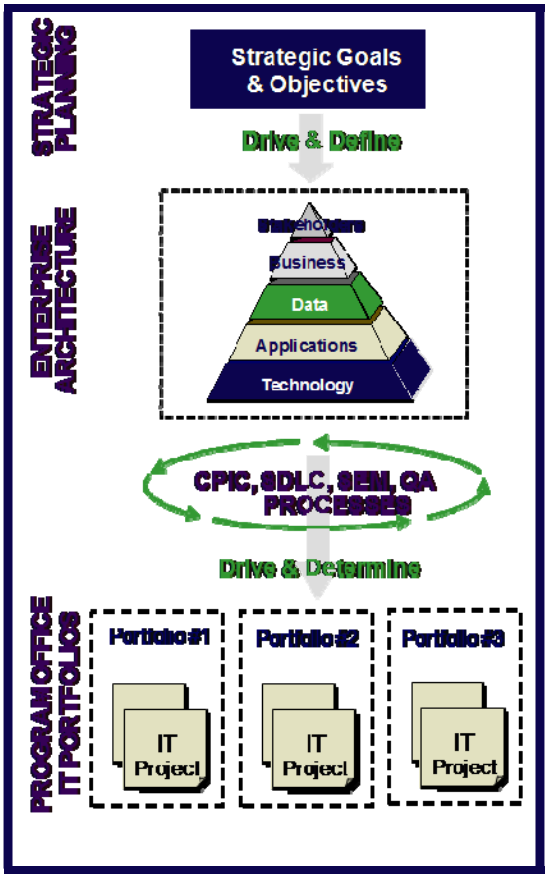

Figure 1: IT Management Process Integration

In essence, DOE has a mission to accomplish and, in doing so, has established priorities as stated in the DOE Strategic Plan and the DOE Information Resource Management (IRM) Strategic Plan. These priorities and supporting functions and processes and related IT assets are captured

in the DOE EA and documented as the baseline and target EA. In particular, a transition plan is documented to ensure that the mission priorities are achieved.

In addition, CPIC processes have been established to ensure that investments and projects are mapped to mission priorities, that funding is budgeted for these investments and projects, and that their progress is tracked. The CPIC process also includes a mechanism for coordinating with budget processes to ensure that IT investments and priorities are included, are consistent with the DOE EA, and are consistent with acquisition data, especially the Exhibit Form 300 prescribed by OMB Circular A-11. Once the Exhibit Form 300s or projects are approved and funding is provided, project management and systems engineering processes are established to ensure successful completion.

The following sections provide more detail into these management processes and how they integrate or provide their unique contribution to the successful accomplishment of mission priorities.

2.1.1 Integration of Strategic Planning

Strategic planning is the process by which the Department and the Office of the Chief Information Officer (OCIO) determine future direction and identify the resources and transformational agendas needed to meet that direction. The DOE Strategic Plan is the roadmap to address the energy, environmental and nuclear security challenges for DOE. The IRM Strategic Plan outlines IT strategic goals, outcomes, priorities, and the means for accomplishing the goals. The IRM Strategic Plan communicates the linkage of IT strategies to the overall Departmental Strategic Plan, and thereby, ensures proper guidance and technological support to accomplish DOE's critical-mission requirements.

IRM strategic planning precedes the selection of IT investments to ensure that annual investments and operations fully support organizational goals and missions. The annual selection of IT investments is completed in coordination with the budget-formulation process under the direction of the CIO and Chief Financial Officer (CFO) to ensure that IT investment needs and requests are fully integrated into DOE's annual budget request.

2.1.2 Integration of Enterprise Architecture (EA)

DOE EA Program

The DOE EA Program helps ensure compliance with OMB Circular A-130 and the Clinger-Cohen Act by promoting standard architectural practices, providing a framework for corporate systems modernization, and establishing an enterprise architecture vision aligned with the Department's strategic goals. It has defined the foundations, baseline, guidance, standards, and vision for the development and implementation of an architecture-based process for making IT investment decisions. A primary tenet of the DOE enterprise architecture methodology is that business needs drive the need for applications and technology. The architecture is used to ensure that legacy and development systems are aligned with key business, technical, and operational criteria.

EA analysis feeds into the CPIC process. In the selection process, the IT investment is analyzed to assure it is compliant with the EA. The EA is also aligned with the annual budget cycle and provides updates that further define the Baseline and Target architectures based on decisions made in the IT CPIC process.

EA Process

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and the technology that supports the processes. An EA describes the current and target architectures, as well as the transition strategy. The EA strengthens management of the Department's information and the effective use of it.

For each DOE IT project, a requirement for the project's architecture to be in alignment and compliance with the DOE target EA should be included in the project's Requirements Specifications. This, like all other project requirements, should be included in the solution and tracked through to implementation, and should be included in the traceability matrix to ensure an audit trail and closure.

The program office should work collaboratively within the DOE EA framework and coordinate efforts to ensure the integration of the Department-wide architecture as well as architectures specific to individual Departmental elements. During the Control Phase, the investment should be monitored throughout its development life cycle including focus on how well the technology (design) aligns with the enterprise technology architecture (infrastructure). These assessments compare the final design specifications of the investment to the higher level common design components of DOE's EA.

More information, including the DOE EA Guidance and Practice document, is available on the OCIO web site under the "Enterprise Architecture" tab.

2.1.3 Integration of Project Management

The IT projectlife cycle approach is the process by which a project is planned, monitored and evaluated. It covers all activities conducted within the scope of the entire project, from project startup to project close-out. An IT project should follow a defined systems development life cycle (SDLC) methodology that communicates expectations for common activities that are to be included in an IT project. An SDLC life cycle provides defined phases for an IT project. Further guidance is provided in Section 2.2.

2.1.4 Integration of Capital Planning and Investment Control (CPIC)

CPIC, as defined in Section 53 of OMB Circular A-11, is the same as capital programming and is a decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency mission and business needs. The CPIC process is a life cycle for capital projects including major IT systems projects. The DOE CPIC process is iterative with inputs coming from across the Department and outputs feeding into the budget and control process.

CPIC is a systematic approach to managing the risks and returns of IT investments for a given mission. It is an integrated management process which provides for the continuous selection, control, and life-cycle management and evaluation of IT investments and is focused on achieving a desired business outcome. CPIC is the program management life cycle for DOE's IT investments. The relationship between project management phases and Critical Decisions, CPIC phases and DOE SDLC phases is depicted in the table below.

Table 2: CD/Project Management, CPIC and SDLC Phase Relationships

CD/Project Management	CD-0 Initiation Phase	CD-1 Definition Phase	CD-2/CD-3 Execution Phase		CD-4 Transition/Closeout	
CPIC	Initiate/ Select	Control				Evaluate
SDLC*	Pre-planning	Planning/ Requirements Definition	Functional Design	System Design	Construction (Programming) / Integration and Testing/ Installation	Acceptance Maintenance

*The SDLC process is iterative in nature or, if a spiral process is used, cyclical

The DOE CPIC phases are defined as:

Select—The process the Department uses to determine priorities and make decisions about which initiatives (new and ongoing) will be funded and included in the IT portfolio.

Control—An ongoing management process designed to monitor the progress of initiatives against projected costs, schedule, performance, and expected mission benefits.

Evaluate—Once initiatives are fully implemented, actual versus expected results are evaluated to assess the initiative's impact on strategic performance; identify any changes or modifications to the initiative that may be needed; and revise the investment management processes based on lessons learned.

More information, including the DOE CPIC Guide, is available on the OCIO web site under the "IT Capital Planning" tab.

2.1.5 Integration of Acquisition

It is the policy of DOE when acquiring IT solutions to integrate project management, financial management, acquisition management, and quality oversight processes into a cohesive process to achieve programmatic goals. Strong acquisition strategy mitigates risk to the Federal Government, accommodates Section 508 of the Rehabilitation Act as needed, and uses contracts and statements of work (SOWs) that are performance based. The implementation of the acquisition strategy should be clearly defined.

Various drivers identify needs for new or improved IT solutions that are aligned with DOE mission and business goals and objectives. Through activities such as conceptualization, functional analysis, feasibility study, business case analysis, and design synthesis, these needs are translated into high-level requirements that become input to the solution development process. High-level requirements are strategically mapped against the current system baseline and functional gaps are identified. A decision may be made to either develop the solution "in-house" by DOE Federal or contractor personnel or acquire it via a DOE acquisition vehicle from industry vendors that are expert in a particular solution development.

Once the planning activities for the acquisition strategy have been conducted, the project should be approved and funded based on OMB Circular A-11, Sections 53 and 300, via the submission guidelines as outlined in the fiscal year reporting instructions. Note that not all projects initiated through the Acquisition Strategy result in projects that move beyond this point and into development of an IT solution.

2.1.6 Integration of Security

Computer security requirements should be developed in conjunction with the system owner's computer system security officer and other stakeholders who provide competent input in the information system security area. This involvement affords early determination of classifications and levels of access protection required for the product.

Applicable security controls and procedures should be implemented to ensure data integrity and protection from unauthorized disclosure, particularly during development efforts. The organization that owns the data defines the data classification. The project team should be aware of all the types of data and of any classified or proprietary algorithms used in the product.

The following procedure can be used to determine computer security requirements.

1. Identify the types of data that will be processed by the system.

2. Determine preliminary data protection requirements.

    a. For systems processing classified information refer to—

        - DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, dated 10-29-07;

        - DOE O 475.2, *Identifying Classified Information*, dated 8-28-07;

        - DOE M 475.1-1B, *Manual for Identifying Classified Information*, dated 8-28-07; and

        - DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

    b. For systems processing unclassified information, including sensitive and mission essential data, refer to DOE O 205.1A, Department of Energy Cyber Security

Management, dated 12-4-06; other Departmental cyber security directives; and organizational program cyber security plan (PCSP),

3. Coordinate with the owner of the host platform to identify existing supporting computer security controls, if applicable.

4. Incorporate security into the requirements specification. Departmental cyber security directives and organizational PCSPs identify minimum management, operational, assurance, and technical security controls that should be addressed and documented in system security plans. These controls address a wide range of system design features, such as access controls, audit requirements, encryption requirements, configuration management planning, backup requirements, contingency planning, data integrity, physical protection, and many more.

Security requirements should be documented in the system security plan and incorporated into the requirements specification.

The cyber security C&A should be completed before the system is placed into operation. The C&A process ensures that security controls are selected and properly implemented to adequately protect the system and its information. Certification ensures that the controls are tested and deficiencies are documented in Plans of Action and Milestones (POA&M) where they are tracked to closure. The accreditation process ensures a senior official assesses any residual risk and authorizes the system to go into production. C&A tasks include planning, documenting, and testing activities that need to be addressed in all stages of the system development life cycle.

More information is available on the OCIO web site under the Cyber Security tab.

2.1.7 Integration of Privacy

If a system or component under development processes sensitive personal information, appropriate safeguards should be established to protect the information from unauthorized disclosure. Refer to the OMB web site for guidance on the Privacy Act.

For systems processing sensitive personal information, contact the Office of Management's Freedom of Information Office Act and Privacy Act Division for coordination and assistance in complying with policy and guidance.

More information is available on the Office of Management web site under the FOIA/Privacy Act tab.

2.2 IT Systems Development Processes

An SDLC life cycle provides defined phases for an IT project.

2.2.1 Systems Development Life Cycle

A life cycle is the process for how a project is planned, monitored and evaluated from startup to close-out. A project should follow a defined SDLC methodology that communicates expectations

for common activities that are to be included in an IT project. The DOE Life Cycle standard, DOE G 200.1-1, Software Engineering Methodology (SEM), provides a generic, adaptable IT systems development life cycle. The SEM integrates systems engineering, software engineering, project management, and quality assurance processes into a life cycle that is controllable, predictable, and repeatable. The life cycle processes are compatible with Departmental policy on development and maintenance of information technology projects, and compliant with Level 2 and 3 key process areas in the Software Engineering Institute's Capability Maturity Model.

The life cycle processes are divided into stages, activities, and tasks that can be combined or modified to tailor as necessary to fit the needs of various types and sizes of projects.The following table compares the SEM to the DOE O 413.3A critical decision requirements.

Table 3: Comparison of SEM to Critical Decisions

Life Cycle Phase	Description	Decision Milestone
Planning	Analyze user needs. Develop Feasibility Statement.	CD-0, Approve Mission Need
Planning/Requirements Definition	Project Plan developed, requirements analysis initiated.	CD-1, Approve Selection and Cost Range
Functional Design	Requirements Documented, Functional Design completed.	CD-2, Approve Performance Baseline
System Design	System Design completed.	CD-3, Approve Start of Construction
Construction/Programming /Integration and Testing/Installation and Acceptance	IT project is ready for implementation.	CD-4, Approve Start of Operations
Maintenance	Project has been Operational for a period of time.	Post CD-4 Review

The SEM includes a Stage Exit process which is similar in principle to the Critical Decision Points. The Stage Exit process ensures that an IT project meets the DOE and project standards and milestones identified in the project plan.

The Stage Exit is conducted by the project manager with the project stakeholders, (e.g., system owner and the following points of contact: user, quality assurance, security, architecture and standards, project manager's manager, and platform.) It is a high-level evaluation of all work products developed in an SDLC life cycle stage.

It is assumed that each deliverable has undergone several peer reviews, as appropriate, prior to the Stage Exit process. The Stage Exit focuses on the satisfaction of all requirements for the stage of the SDLC life cycle, rather than the specific content of each deliverable.

2.2.2 SEM Life Cycle Phases

The amount of project and system documentation required throughout the life cycle is commensurate with project size and complexity. The life cycle methodology should communicate the documentation requirements and provide guidelines for life cycle adaptability based on project attributes and development methodology.

Figure 2 below shows the SEM life cycle phases with deliverables and activities identified by stage of development. This figure presents the minimum set of documentation contained within the SEM. The SEM is exclusive in stating where documentation is initiated and when this documentation should be updated; all documentation is subject to update and revision throughout the project's lifecycle.

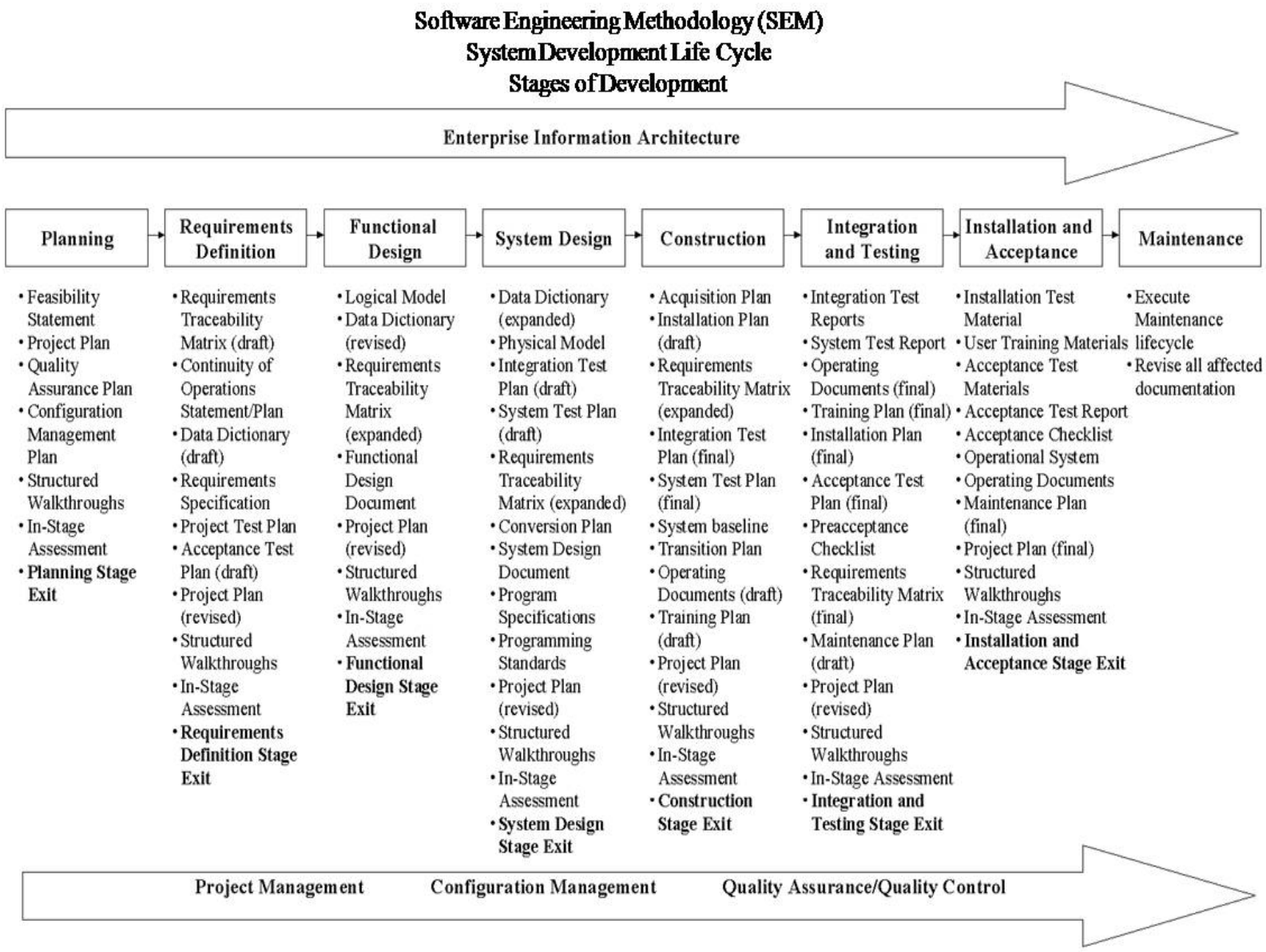

Figure 2: SEM Stages of Development

Planning

The planning stage is the first stage in the life cycle. It is the time when the scope and feasibility of the project is determined. The team focuses on identifying what the project will automate, and whether developing an IT solution makes sense from business, cost, and technical perspectives. If the project is feasible, then time, cost, and resource estimates are formulated and risk factors are assessed. The information gathered in this stage is used to plan and manage the project throughout its life cycle.

Requirements Definition

The primary goal of this stage is to develop a basis of mutual understanding between the system stakeholders and the project team about the requirements for the project. The result of this understanding is an approved Requirements Specification that becomes the initial baseline for product design and a reference for determining whether the completed product performs as the stakeholder requested and expected. Each requirement identified in the Requirements Specification should be traceable to one or more design entities. This traceability ensures that the product will satisfy all of the requirements and will not include inappropriate or extraneous functionality.

Functional Design

The functional design process maps the "what to do" of the Requirements Specifications into the "how to do it" of the design specifications. During this stage, the overall structure of the product is defined from a functional viewpoint. The focus is on the functions and structure of the components that comprise the products. The goal of this stage is to define and document the functions of the product to the extent necessary to obtain the stakeholders' understanding and approval and to the level necessary to build the system design.

System Design

The goal of this stage is to translate the user-oriented functional design specifications into a set of technical, computer-oriented system design specifications; and to design the data structure and processes to the level of detail necessary to plan and execute the next stages of the life cycle.

Construction (Programming)

The goal of this stage is to translate the set of technical, computer-oriented system design specifications into a language the computer can understand and execute. Construction involves coding, validation and unit testing by a developer. Any hardware or software procured to support the construction effort is installed. The activities in this stage result in the transformation of the system design into the first complete, executable representation of the product.

Integration and Testing

Integrating and testing activities should focus on the interfaces between and among the components of the product. In this stage, components are integrated and tested to determine

whether the product meets predetermined functionality, performance, quality, interface, and security requirements.

Installation and Acceptance

Installation and acceptance of the product are initiated after the system test has been successfully completed. The objectives of the activities in this stage are to verify that the product meets design requirements and to obtain stakeholder acceptance and approval of the product and assure the product is fully operational. At the conclusion of this stage, the responsibility of the IT Solution is formally transferred from the project team to the system owner and maintenance staff.

Maintenance

The maintenance stage is the iterative processes for maintaining and improving the IT solution once it has been placed in production. These processes allow the maintenance team to better plan, optimize use of resources, take advantage of scale and better control outcome in terms of both schedule and product quality.

More IT project management information, including the SEM and Stage Exit Process documents, is available on the OCIO web site under the IT Project Management tab.

APPENDIX A—REFERENCES

1. American National Standards Institute/Electronic Industries Alliance Earned Value Management System Standard (ANSI/EIA-748-A-1998).

2. DOE G 200.1-1, *Software Engineering Methodology*, dated 5-21-97.

3. DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

4. DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*, dated 3-7-06.

5. DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, dated 10-29-07.

6. DOE M 475.1-1B, *Manual for Identifying Classified Information*, dated 8-28-07.

7. DOE N 203.1, *Software Quality Assurance*, dated 10-02-00.

8. DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-04-06.

9. DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, dated 7-28-06.

10. DOE O 414.1C, *Quality Assurance*, dated 6-17-05.

11. DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*, dated 10-9-07.

12. DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.

13. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Information*, dated 6-30-00.

14. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.

15. U.S. Department of Energy's Guide to IT Capital Planning and Investment Control, dated September 2007.

16. P.L. 100-235, the Computer Security Act of 1987.

17. P.L 105-220, section 508, The Rehabilitation Act, as amended by the Workforce Investment Act of 1998.

18. P.L. 107-347, Federal Information Security Management Act of 2002.

19. P.L. 104-208, the Clinger-Cohen Act of 1996.

20. 5 U.S.C. 552, Freedom of Information Act.

21. 5 U.S.C. 552a, Privacy Act of 1974.

22. Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget*, dated 6-26-08.

23. OMB Circular A-123, Management's Responsibility for Internal Control, dated 12-21-04.

24. OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, dated 11-28-00.

25. OMB Memorandum 05-23, Improving Information Technology (IT) Project Planning and Execution, dated 8-4-05.

26. U.S. Department of Energy's FY 2008—2010 Information Resource Management Strategic Plan.

APPENDIX B—ACRONYMS

ANSI/EIA	American National Standards Institute/Electronic Industries Alliance
ATO	authority to operate
BY	budget year
C&A	certification and accreditation
CD	Critical Decision
CFR	Code of Federal Regulations
CFO	Chief Financial Officer
CPIC	capital planning and investment control
CY	current year
D/M/E	development/modernization/enhancement
DOE	Department of Energy
EA	Enterprise Architecture
EVMS	Earned Value Management System
FOIA	Freedom of Information Act
IPT	integrated project team
IRM	Information Resources Management
IT	information technology
O	order
OCIO	Office of the Chief Information Officer
OECM	Office of Engineering and Construction Management
OMB	Office of Management and Budget
PCSP	program cyber security plan
PIR	post implementation review
POA&M	plans of action and milestones
PY	prior year
SDD	system description document
SDLC	systems development life cycle
SEM	Systems Engineering Methodology
SOW	statement of work
TPC	total project cost

APPENDIX C—DEFINITIONS

1. Capital Planning and Investment Control (CPIC). A decision-making process for making sure IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues. (Source: Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget,* dated 6-26-08.)

2. Configuration Management (CM). A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (Source: IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.)

3. Departmental Element.

    a. A first-tier organization at Headquarters and in the field. First-tier at Headquarters is the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and staff office directors).

    b. First-tier in the field is managers of the eight operations offices, managers of the three field offices, and the Administrators of the Power Marketing Administrations.

    c. Headquarters and field elements are described as follows:

    d. Headquarters elements are DOE organizations located in the Washington Metropolitan Area and

    e. Field element is a general term for all DOE sites (excluding individual duty stations) located outside of the Washington, DC, Metropolitan Area. (Source: DOE Glossary in the Directives System.)

4. Enterprise Architecture (EA). A business-driven plan that describes the current state, future vision, and transitional states of an operation presented in terms of: strategy and performance; business; applications and services; technology; data; and security, all at the end of a two-to-five year planning horizon.

5. Information Resources. Personnel, equipment, funds, and information technology.

6. Information Resources Management. The oversight of the acquisition and use of information resources to accomplish Agency missions and to improve Agency performance.

7. Information System. A discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated information technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. (Source: Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget*, dated 6-26-08.)

8. Information Technology. Any equipment, interconnected system, or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. NOTE: equipment can be used by an executive agency either directly or by a contractor that requires the use of such equipment in performing a service or furnishing a product. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and resources.

9. Office of the Chief Information Officer (OCIO). Responsible for ensuring that IT is acquired and information resources are managed consistent with statutory, regulatory, and Departmental requirements and priorities.

10. Quality Assurance.

    a. A planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established operational, functional, and technical requirements.

    b. A set of activities designed to evaluate the process by which products are developed or manufactured. (Source: IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.)

11. Risk Management. An approach to problem analysis that is used to identify, analyze, prioritize, and control risks. (Source: DOE Software Engineering Methodology, 5-21-1997.)

12. Software. All computer programs or procedures or rules and associated documentation pertaining to the operation of a computer system customized for DOE use, proposed for use, under development, or being maintained and used, whether developed in-house, licensed from a commercial vendor for customized use, obtained from another organization, or otherwise acquired. Types include:

    a. administrative/business-oriented programs,

    b. scientific/engineering software,

    c. manufacturing-oriented software, and

    d. process control (e.g., programmable logic control instructions).

13. Software Engineering. The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software.

14. System Testing. A process conducted on a complete, integrated system to evaluate compliance with specified requirements. (Source: IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.)

15. Unit Testing. A process for evaluating individual hardware or software units or groups of related units. The isolated testing of each flow path of code with each unit. The expected output from the execution of the flowpath should be identified to allow comparisons of the planned output against the actual output. (Source: DOE Software Engineering Methodology, 5-21-1997.)

16. Validation. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (Source: IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.)