PHASE 5: DESIGN PHASE

During the Design Phase, the system is designed to satisfy the requirements identified in the previous phases. The requirements identified in the Requirements Analysis Phase are transformed into a System Design Document that accurately describes the design of the system and that can be used as an input to system development in the next phase.

1.0 OBJECTIVE/GOALS

Objectives
Successful completion of the Design Phase should comprise:

- Transformation of all requirements into detailed specifications covering all aspects of the system
- Assessment and planning for security risks
- Approval to progress to the Development Phase

Goals
The purpose of the Design Phase is to transform the requirements into complete and detailed system design specifications. Once the design is approved, the Development Team begins the Development Phase.

2.0 DELIVERABLES AND APPROVALS

SDLC deliverables help State agencies successfully plan, execute, and control IT projects by providing a framework to ensure that all aspects of the project are properly and consistently defined, planned, and communicated. The SDLC templates provide a clear structure of required content along with boilerplate language agencies may utilize and customize. State agencies may use formats other than the templates, as long as the deliverables include all required content.

The development and distribution of SDLC deliverables:

- Ensure common understanding among Development Team members and stakeholders,
- Serve as a reminder of specified plans as projects become increasingly complex,
- Provide agency senior management and other State officials insight into project risks and ongoing performance,
- Encourage the execution of repeatable and consistent processes,
- Facilitate the implementation of project management and agency IT best practices, and
- Result in a comprehensive record of project performance useful for many purposes (e.g. staff knowledge transfer, budgetary and other assessment activities, lessons learned).

During the development of documentation, the Development Team should:

- Write comprehensive, easy to understand documents with no redundant information.
- Develop an organized document repository for critical project information, so Development Team members can easily access, store, and reference project documents and other deliverables from all life cycle phases.
- Implement routine deliverable reviews to correct inaccuracy, incompleteness, and ambiguities.

- Recognize that sample templates for deliverables are available; agencies might accept deliverables in different formats as long as all required information is present. The content of these deliverables might expand or shrink depending on the size, scope, and complexity of the project.
- Recycle or reference information from earlier documents where possible and beneficial.

The following is a listing of deliverables required of all projects for this phase of work.

Deliverable	Goals	Developed By	Approved By
System Design Document – specifies the construction details of the system, each system component's interaction with other components and external systems, and the interface that allows end users to operate the system and its functions.	• Document the results of the system design process • Describe how the system with satisfy requirements	Development Team	Project Sponsor Agency CIO Project Manager
System Security Consensus Document (SSCD) – a single document containing all information relevant to completing the system's C&A.	• Define the system's security architecture, security policies, risk assessments, and security tests • Consolidate all information for the C&A	Project Manager	Agency CIO
Security Plan – documents the scope, approach, and resources required to assure system security.	• Describe planned activities to control access and protect the system and its information	Development Team	Project Manager Agency CIO
Data Retention Plan – describes the project policies for data and records management.	• Record retention and disposition responsibilities • Document retention and disposition requirements • Record management process • Document retention and disposition schedules	Development Team	Project Manager Agency CIO

Deliverable	Goals	Developed By	Approved By
Disaster Recovery Plan – IT-focused plan designed to restore operability of targeted systems, applications, or a computer facility due to a natural or man-made extended interruption of an agency's business services.	• Identify plans to restore operability in the event of extended interruption of services • Define and document concept of operations • Document notification procedures • Record damage assessment procedures, recovery activities, and reconstitution procedures	Development Team	Project Manager Agency CIO
Unit and Integration Test Plans (Begin) – detailed scripts used in the Development and Test Phases for evaluating the completeness and correctness of the smallest parts of the system and the components created from those parts. The test scripts are more specific than the Test Master Plan, which is high-level and more focused on processes.	• Identify detailed scripts for testing system components	Development Team	Agency CIO Project Manager
Conversion Plan (Begin) – describes the strategies and approaches for converting/migrating data from an existing system to another hardware or software environment.	• Document all planned activities to ensure a smooth data conversion from a legacy system to a new environment	Development Team	Agency CIO
Implementation Plan – describes how the information system will be deployed as an operational system.	• Define all planned activities to ensure successful implementation to production operations	Development Team	Project Sponsor Agency CIO

Deliverable	Goals	Developed By	Approved By
Operations or System Administration Manual (Begin) – The Operations Manual focuses on mainframe systems; the Systems Administration Manual is oriented for distributed (client/server) applications. Both documents provide details on system operations.	• Provide detailed instruction for system operations	Development Team	Agency CIO
Maintenance Manual (Begin) – details effective system maintenance. Appendices might document maintenance procedures, standards, or other essential information on areas such as backup, networking and connectivity, access and authentication, cabling, and critical services.	• Provide maintenance personnel with the information necessary to effectively maintain the system	Project Manager	Agency CIO
Training Plan – outlines training needs for end users on the new or enhanced information system.	• Ensure that the schedule accounts for all necessary training needs to successfully implement, operate, and maintain the system	Development Team	Project Sponsor
User Manual (Begin) – describes to end users how to make full use of the information system, including system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use.	• Provide users with detailed information to fully utilize the system	Development Team	Agency CIO

Deliverable	Goals	Developed By	Approved By
Requirements Traceability Matrix (Update) – a table that links requirements to their origins and traces them throughout the project life cycle.	• Establish a baseline for requirements change control, design, and testing	Development Team	Agency CIO Business Owner Project Manager

All deliverables other than those identified as Updates should be developed in this phase. Deliverables identified as Updates should be revisited and enhanced as necessary as prescribed in this phase.

Deliverables produced during this phase must be reviewed in detail and should follow the approval path as defined in the above table. A signature page or section should accompany each deliverable requiring approval. DoIT will periodically request copies of these documents as part of its oversight responsibilities.

3.0 ROLES

The following personnel participate in the work activities of this phase:

- Project Sponsor
- Executive Sponsor
- Agency CIO
- Project Manager
- Development Team
- Project Stakeholders
- Security Officer
- Secretary of DoIT

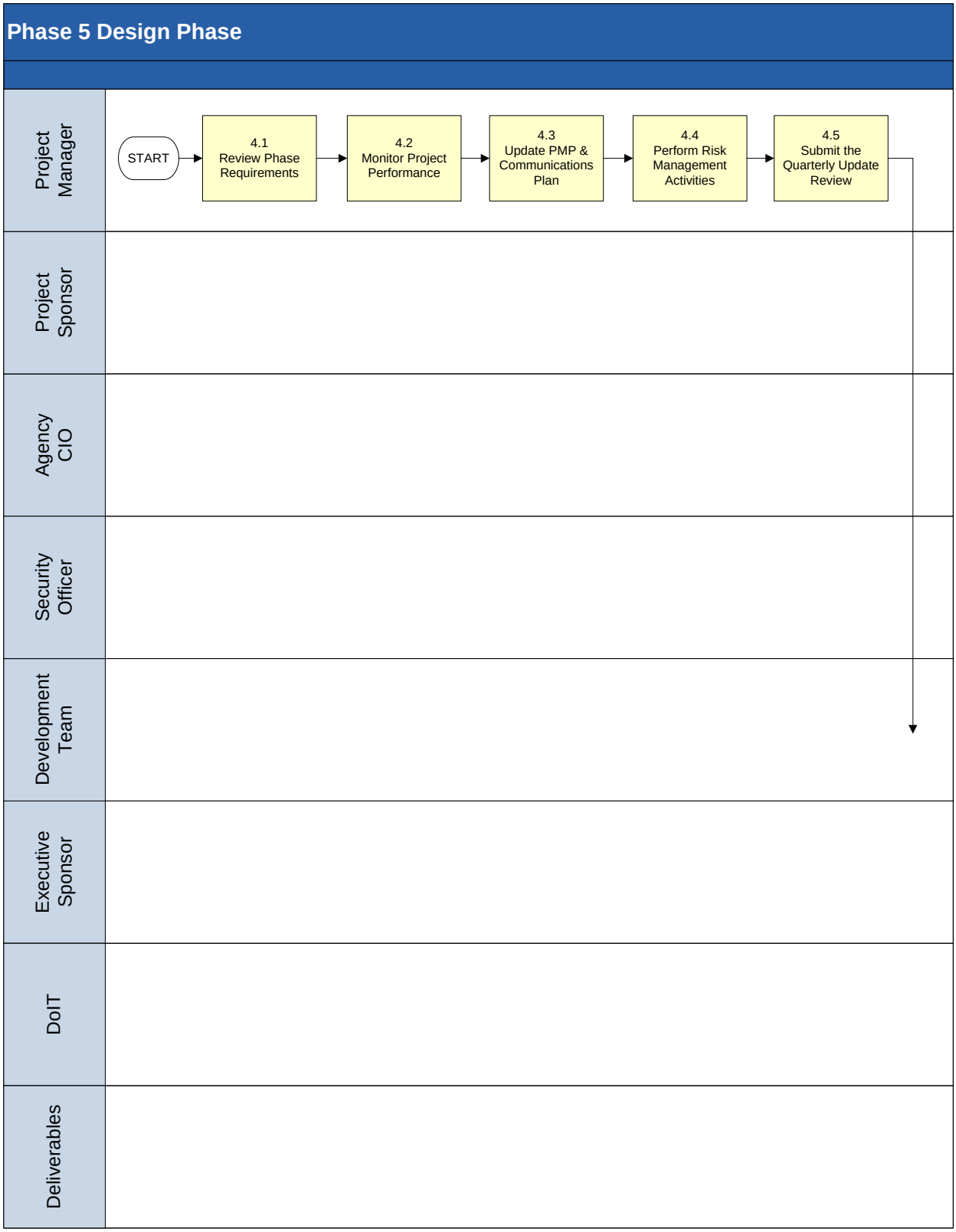
RACI Key
Responsible – Describes role that executes the activities to achieve the task.
Accountable – Describes roles that own the quality of the deliverable and sign off on work that Responsible provides.
Consulted – Describes roles that provide subject matter expertise.
Informed – Describes roles that receive information about the task.

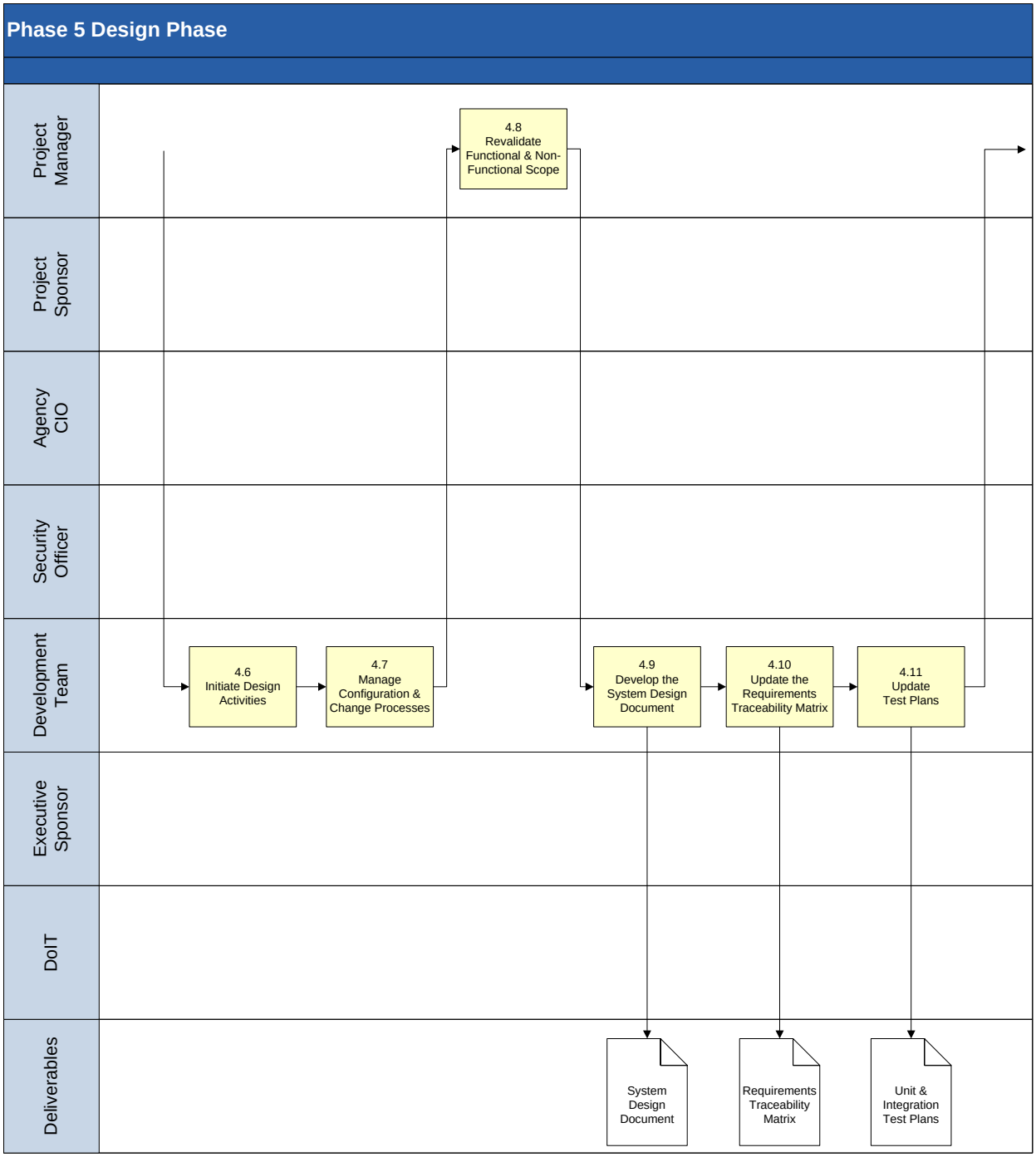
Deliverable	Executive Sponsor	Project Sponsor	Agency CIO	Project Manager	Development Team	Project Stakeholders	Security Officer	DoIT
System Design Document	I	A	A	R	I	C		C
System Security Consensus Document	I	I	A	R	I	I	A	C
Security Plan	I	I	A	R	I	I	A	C
Disaster Recovery Plan	I	I	A	R	I	I	A	C
Unit and Integration Test Plans	I	I	A	R	I	C		C
Conversion Plan	I	I	A	R	I	I		C
Implementation Plan	I	A	A	R	I	I		C
Operations or System Administration Manual	I	I	A	R	I	I		C
Maintenance Manual	I	I	A	R	I	I		C
Training Plan	I	A	A	R	I	I		C
User Manual	I	I	A	R	I	I		C
Requirements Traceability Matrix	I	A	A	R	I	C		C

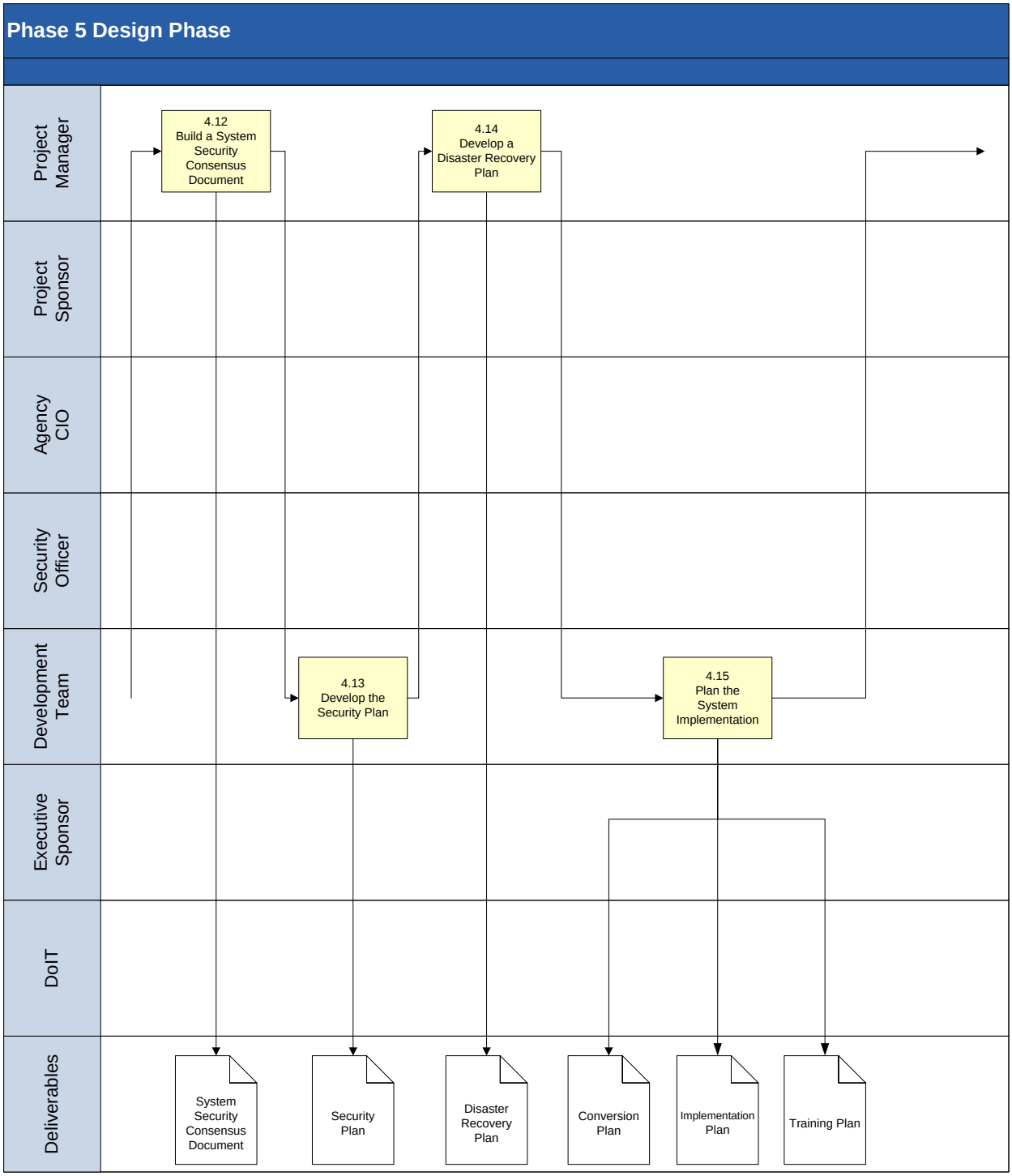
Possible RACI Matrix

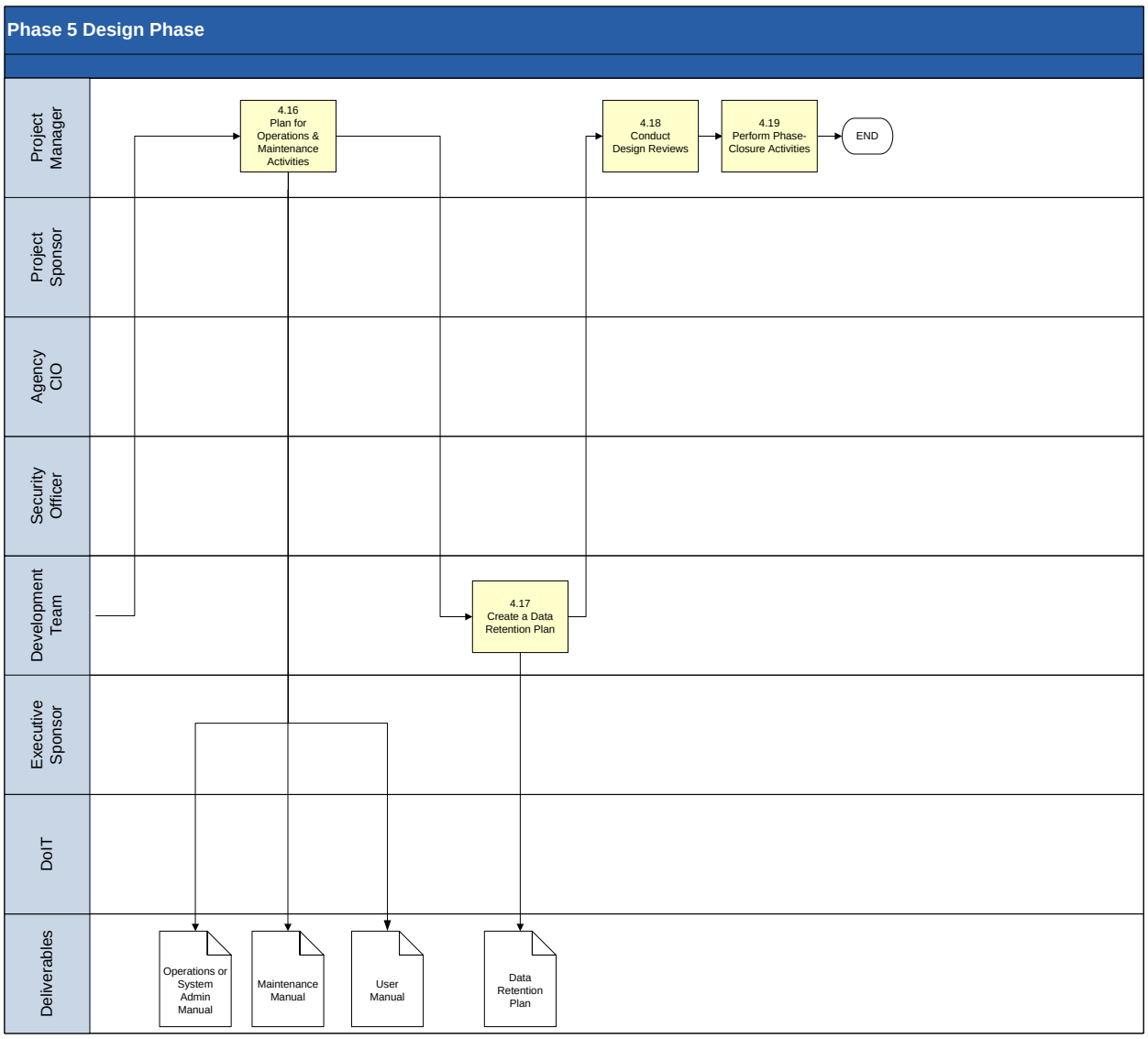
The Roles and Responsibilities page has detailed descriptions of these roles and their associated responsibilities.

4.0 TASKS AND ACTIVITIES




Phase 5 Design Phase
Project Manager
Project Sponsor
Agency CIO
Security Officer
Development Team
Executive Sponsor
DoIT
Deliverables
4.8 Revalidate Functional & Non-Functional Scope
4.6 Initiate Design Activities
4.7 Manage Configuration & Change Processes
4.9 Develop the System Design Document
4.10 Update the Requirements Traceability Matrix
4.11 Update Test Plans
System Design Document
Requirements Traceability Matrix
Unit & Integration Test Plans


Phase 5 Design Phase
Project Manager
Project Sponsor
Agency CIO
Security Officer
Development Team
Executive Sponsor
DoIT
Deliverables
4.12 Build a System Security Consensus Document
4.14 Develop a Disaster Recovery Plan
4.13 Develop the Security Plan
4.15 Plan the System Implementation
System Security Consensus Document
Security Plan
Disaster Recovery Plan
Conversion Plan
Implementation Plan
Training Plan



4.1 **Review Phase Prerequisites.**

The Project Manager ensures the following prerequisites for this phase are complete:

- The PMP and the schedule showing the target termination date for the system are current.
- The PSS is current and complete.
- The FRD is complete.
- Procurement for development work is complete.

4.2 **Monitor Project Performance.**

The Project Manager monitors project performance by gathering status information about:

- Cost expenditures to date and cost variances from the cost performance baseline
- Change management information
- Activity progress with status details from all Development Team members
- Vendor contract compliance
- Vendor status reports

- Risk Register review
- Late tasks review
- List of complete and incomplete deliverables
- WBS activities started and finished
- Estimated time to completion
- Resource utilization data
- Changes to project scope

The Project Manager also organizes and oversees systematic quality management reviews of project work as a part of monitoring the project performance.

To measure project effort at all phases of the life cycle, the Project Manager establishes timelines and metrics for success at each phase of work when planning project tasks.

The *PMBOK* provides additional details on controlling project work in sections 4.4 and 4.5 and on project scope control in section 5.5.

4.3 **Update PMP and Communication Management Plan.**

The Project Manager updates the PMP routinely (at least quarterly) to ensure the PMP reflects project performance accurately. Review project performance controls and risks for deviations from the baseline.

Information distribution is one of the most important responsibilities of the Project Manager. The Project Manager reviews and updates the Communication Management Plan at least quarterly to account for potential changes in project stakeholders. The Project Manager distributes the updated PMP and risk management information according to the revised Communication Management Plan. *PMBOK*, section 10 contains additional details on project communications and information distribution.

4.4 **Perform Risk Management Activities.**

The Project Manager conducts periodic risk management activities during the Design Phase; these activities include:

- Identification – determination of initial risks that might affect the project and emerging risks as well as each risk characteristic
- Risk Analysis – conducting quantitative and/or qualitative analysis of each identified risk. Usually, qualitative risk management techniques are the most applicable for State projects. These risk analysis methods, as well as the conditions under which each method might be used, are described in detail in *PMBOK*, section 11.
- Response Planning – planning of methods for developing mitigation, transfer, or avoidance strategies to reduce risk
- Monitoring and Control – definition of procedures to track risks, monitor residual risk, identify new risks, execute response plans, and evaluate risk management effectiveness

These activities occur throughout the project duration to track and mitigate any new or changed project risks. The *PMBOK*, section 11 has details for risk management activities, particularly sections 11.2 through 11.6.

4.5 **Submit the Quarterly Update Review.**

The Project Manager assembles all project documentation, including the Communication Management Plan, PMP, issue logs, and any other relevant artifacts reflecting day-to-day management of the project, each quarter and submits this information to DoIT as a quarterly update review. DoIT reviews this information, particularly differences from the previous quarter and determines whether to recommend any action.

4.6 **Initiate Design Activities.**

The Development Team has several important decisions to make as the solution begins to take shape. During the process of creating the design, the Project Manager and Development Team should consult with the Maryland EA Repository for possible components to integrate into the new system, potentially saving money through reuse. Project stakeholders should be involved periodically throughout the Design Phase to ensure that the development team understands their expectations and that it develops the system in accordance with requirements.

The Development Team makes critical design decisions, including:

- Approach decisions
    - Validate proposed COTS components
    - Prototype to refine and improve understanding of requirements
    - Select development and implementation methodologies and tools
    - Determine how user support will be provided, how the remaining life cycle phases will be integrated, and newly identified risks and issues handled
    - Determine user acceptance criteria (refer to the User Acceptance page in Related Links)
- Execution decisions
    - Identify modifications that must be made to the initial information system need
    - Identify modifications that will be made to current procedures
    - Identify modifications that will be made to current systems/databases or to other systems/databases under development
    - Determine how conversion of existing data will occur
- Continuation decisions
    - Determine continued development activities based on needs identified in design
    - Identify availability of sufficient funding and other required resources for the remainder of the life cycle

During the process of this decision-making, the Development Team may consult other technical resources, such as agency production operations staff to identify technical issues in the Operations and Maintenance Phase, for additional information.

4.7 **Manage Configuration and Change Processes.**

The Development Team sets up a configuration management repository and establishes change management procedures to track changes to the system, ensure requirements compliance, and enhance development quality.

This effort involves three inter-related concepts:

- Configuration management – focuses on establishing and maintaining consistency in the system's performance and its functions throughout its life cycle.
- Change management – the process of requesting, planning, implementing, and evaluating changes to the system; this process supports changes to the system and allows for their traceability.
- Change control – ensures that changes to the system are introduced by a controlled and coordinated method; change control is a part of change management.

Creating the right balance in change management is difficult but critical to system development: too much control may cause work to be impeded; too little control may cause the project to devolve into chaos.

Establishing a solid configuration management repository and clear change management processes improve requirements traceability. Requirements traceability begins in the Design Phase as the Development Team validates requirements and begins the process of creating exact specifications to meet those requirements. Managing those requirements properly increases project success.

For more information on configuration management best practices, see Related Links.

4.8 **Revalidate Functional and Non-Functional Scope.**

The Project Manager schedules a review of the system requirements, both functional and non-functional, to ensure the scope has not changed since the end of the Requirements Analysis Phase. This review includes project stakeholders and Development Team members and covers the FRD deliverable created in the Requirements Analysis Phase: re-validating the FRD in this phase ensures the FRD reflects the user's perspective of the system design.

4.9 **Develop the System Design Document.**

The Development Team constructs the Systems Design Document (SDD), which maps the system requirements to the technical implementation and contains details about the environment, hardware architecture, software architecture – including subsystems and components, files, database design – and internal and external interfaces.

4.9.1 **Document Description**

The SDD describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

4.9.2 **Typical Content**

The key elements of the SDD include the following. Additional guidance is provided in the SDLC template.

- Software components
    - A description of software modules and their use to build operating components
    - A list of components and how they are connected including middleware
    - Traces of key business processes through all components
    - Design for individual components (e.g. class diagrams, behavioral diagrams, persistence models, concurrency strategies and tactics, interfaces, inputs and outputs)
    - Documentation of all protocols and data transfer syntax and semantics for all internal and external interfaces
    - Dependencies between modules as well as external programs or source code
    - Dependencies between components
- Diagrams
    - A deployment diagram
    - A network diagram
    - Data flow diagrams
    - Data model
    - Context diagram for each component
- Supporting technologies
    - Description of security architecture
    - Description of availability and scalability strategy
    - Description of how to monitor the production system
- Project or system decisions
    - Description of the build process
    - Description of the deployment process
    - Map of requirements/features to the modules and components that implement them
    - Documentation of architecture, frameworks, and design patterns used or developed in the design and the rationale for their selection
    - User interface design (Refer to Nonvisual Access Regulatory Standards on the Maryland.gov site)
    - User acceptance testing scripts and activities (Refer to the User Acceptance page in Related Links)

Not all projects require these elements for every type of system. Large-scale custom development projects need nearly all, but, for example, in a COTS implementation, the user interface information will be in the User Manual and not required in a design document. For a network deployment or hardware upgrade, the SDD should emphasize the deployment of the system. The Project Manager and the Project Sponsor must ensure proper documentation for development and to meet the requirements.

4.9.3 **Guidance for Document Development**

The effort to develop the SDD may iterate through several cycles from a general design to the desired level of granularity as significant architecture decisions are made and the design moves toward the target architecture.

The SDD documents the transformation of abstract business requirements to detailed hardware and software specifications for construction and assembly.

4.9.4 **Dos and Don'ts**

- Do conduct periodic design reviews as the Development Team formulates design and develops the SDD.
- Do utilize prototyping to elicit stakeholder feedback in the design process.
- Do ensure that the SDD addresses all aspects of the system design in detail.
- Don't postpone any aspect of detailed design until a later phase.

4.10 **Update the Requirements Traceability Matrix.**

The Development Team updates the RTM after the SDD is approved. An RTM aids in moving from requirements to design and enabling the System Team to track problems occurring in the Operations and Maintenance Phase back through testing and design to original requirements.

4.11 **Update Test Plans.**

The Development Team builds on the TMP created in the Requirements Analysis Phase as the system architecture and its components are specified. Refine test cases and procedures as the design process continues.

4.12 **Build a System Security Consensus Document.**

The Project Manager coordinates a comprehensive security risk assessment, which addresses threats, vulnerabilities, risks, outcomes, and security controls and documents the results in the SSCD. The risk assessment evaluates compliance with baseline security requirements, identifies threats and vulnerabilities, and assesses alternatives for mitigating or accepting residual risks.

4.12.1 **Document Description**

The SSCD includes a definition of the system and its security architecture, security policies, risk assessments, and security test plans.

4.12.2 **Typical Content**

The key elements of the SSCD include at minimum:

- Mission description
- System identification
- Environment and threat description
- System architecture description
- Certification and Accreditation team
- Tailored Certification and Accreditation process

4.12.3 **Guidance for Document Development**

The SSCD is designed to retain all information for the C&A in one document. State policy for IT systems requires that all Executive Branch agencies certify and accredit the IT systems and sites under their ownership and control. The Development Team should review the *DoIT*

Information Technology Security Certification and Accreditation Guidelines and the project's SSCD for any actions needed to enable the system to become certified and accredited prior to implementation. These documents are available at the DoIT State Information Technology Security Policy and Standards webpage. In addition, the Development Team should review all applicable federal government guidance to ensure relevant security requirements are addressed:

- National Security Agency (NSA) Security Recommendation Guides
- Federal Information Security Management Act (FISMA)
- National Institution of Standards & Technology (NIST) Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook
- NIST Special Publication 800-30 Risk Management Guide for Information Technology
- NIST Special Publication 800-41 Guidelines on Firewalls and Firewall Policy
- NIST Special Publication 800-44 Guidelines for Securing Public Web Servers.
- NIST Special Publication 800-45 Guidelines for Electronic Mail Security
- NIST Special Publication 800-55 Security Metrics Guide for Information Technology Systems
- NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling
- NIST Special Publication 800-88 Media Sanitization Guide
- NIST Special Publication 800-100 Information Security Handbook

In addition to the C&A policies, the Development Team should review other DoIT security policies and standards (posted on DoIT's website) to determine which ones apply. The Development Team adds to the SSCD a plan to implement those policies that apply and identify security controls to remediate risks and vulnerabilities discovered during the risk assessment.

4.13 **Develop the Security Plan.**

The Development Team develops the Security Plan to address security risks identified in the SSCD.

4.13.1 **Document Description**

The Security Plan documents the scope, approach, and resources required to assure system security.

4.13.2 **Typical Content**

The key elements of the Security Plan include at minimum:

- Security personnel and their responsibilities
- Secure operating environment description
- Sensitivity of information handled
- External system dependencies
- Access authorization
- Information sharing restrictions
- Physical protection requirements
- Countermeasures to be used to mitigate vulnerabilities identified in SSCD
- Description of how security requirements will be met
- Description of security support structure

- References to relevant security policies and standards
- Network audit policies to be executed including the C&A schedule
- Security incident reporting
- Work breakdown and schedule of security activities

4.13.3 **Guidance for Document Development**

The Development Team should create the Security Plan after the SSCD to ensure that all known vulnerabilities and requirements are addressed. The purpose of the Security Plan is to specifically identify all planned controls and activities necessary to meet security requirements. The document also outlines responsibilities of all system users.

4.14 **Develop a Disaster Recovery Plan.**

The Project Manager also coordinates with the Development Team and project stakeholders to define a Disaster Recovery Plan (DRP) for the system.

4.14.1 **Document Description**

The DRP is an IT-focused plan designed to restore operability of targeted systems, applications, or a computer facility due to a natural or man-made extended interruption of an agency's business services.

4.14.2 **Typical Content**

The key elements of the DRP include at minimum:
- Concept of operations
- Notification procedures
- Plan activation criteria
- Damage assessment procedures
- Recovery activities
- Reconstitution procedures

4.14.3 **Guidance for Document Development**

The Development Team should conduct a Business Impact Analysis (BIA) to identify IT resources, identify outage impacts and allowable times, and develop recovery priorities. The information gathered during the BIA serves as critical input to the DRP. The DRP should also address operability risk mitigation strategies identified during the security risk assessment. Additional DRP guidance may be found in the State of Maryland Information Technology Disaster Recovery Guidelines found on the DoIT website.

4.14.4 **Dos and Don'ts**

- Do protect the DRP with the same level of controls used to protect sensitive data from unwarranted disclosure.

4.15 **Plan the System Implementation.**

The Development Team begins documenting implementation procedures for the system in the target environment, including any necessary resources and information. The implementation

procedures include migration strategies to support running parallel activities during the transition. The Conversion and Implementation Plans should address data migration to ensure a smooth implementation.

Identify implementation resources from the Development Team, which may be a combination of State employees and external vendors, based on the technologies and the implementation methodology. The implementation resources must have technical skills, the ability to communicate issues and changes, understanding of both the problem domain and the implementation environment, and good leadership.

The Conversion Plan, Implementation Plan, and the Training Plan should be in draft form by the end of the Design Phase.

4.16 **Plan for Operations and Maintenance Activities.**

The Project Manager and Development Team draft an Operations or System Administration Manual and a Maintenance Manual. The System Team will use these documents during the Operations and Maintenance Phase to support the system.

Schedule a review near the end of the Design Phase to evaluate any particular operations or maintenance requirements for system administration.

The User Manual should be in draft form at the end of this phase.

4.17 **Create a Data Retention Plan.**

The Development Team creates a formal Data Retention Plan according to the policies and standards established by the State Archivist.

4.17.1 **Document Description**

The Data Retention Plan describes the project policies for data and records management.

4.17.2 **Typical Content**

The key elements of the Data Retention Plan include at minimum:

- Retention and disposition responsibilities
- Retention and disposition requirements
- Retention and disposition schedules
- Management process

4.17.3 **Guidance for Document Development**

State of Maryland has legally mandated data retention policies that apply to all State agencies and State-created entities and any public records. The State Archivist's website has records management guidance, including the laws, rules, and regulations, at http://www.msa.md.gov/msa/intromsa/html/record_mgmt/homepage.html. The Code of Maryland states that "The willful, unauthorized destruction or alienation of any public record is a misdemeanor subject to criminal penalties." The State policy is that "a public record may not be disposed of without authorization from the State Archivist" and expects any part of the State,

county, or local governments to follow this policy. This site provides additional guidance on how to develop a records retention schedule, which in turn helps the agency and Development Team create a Data Retention Plan for the project.

The Project Manager reviews the Data Retention Plan with the Development Team and project stakeholders to ensure acceptance and compliance.

4.18 **Conduct Design Reviews.**

The Project Manager oversees periodic system design reviews of the system functions, performance requirements, security requirements, and platform characteristics.

A system/subsystem design review is held at the end of the Design Phase to resolve open issues regarding one or more of the following:

- System-wide or subsystem-wide design decisions
- Architectural design of a software system or subsystem

A software design review is held at the end of the Design Phase to resolve open issues regarding one or more of the following:

- Software-wide design decisions
- Architectural design of a software item
- Detailed design of a software item or portion thereof (such as a database)

4.19 **Perform Phase-Closure Activities.**

The Project Manager and the Development Team prepare and present a project status review for the Agency CIO, Project Sponsor, Executive Sponsor, and other project stakeholders after completion of all Design Phase tasks. This review addresses:

- Cost expenditures to date and cost variances to the cost performance baseline
- Status of Design Phase activities
- Planning status for all subsequent life cycle phases, with significant detail about the next phase
- Status on resource availability
- Project scope control as described in the PSS and any required adjustments
- Changes to the project schedule and estimated completion date
- Vendor contract compliance
- A final design review of the system covering issues raised in earlier design reviews
- “Go-No Go” decision made to proceed to next phase, based on Design Phase information
- Acquisition risk assessments of subsequent life cycle phases given the planned acquisition strategy
- Verification that all changes are conducted in accordance with the approved Change Management Plan

The Project Manager compares actual project performance to the baseline and the projected cost of the project to detect and understand any variances from the cost baseline during the phase-end review. The Project Manager also performs a comprehensive risk assessment of the project to

update the Risk Register. The Project Manager updates the Maryland EA Repository with any new or revised components before beginning the next phase, Development.

The Project Manager must obtain deliverable approval signatures before proceeding to the Development Phase.

Update the project documentation repository upon completion of the phase-closure activities.

5.0 CONCLUSIONS

The Design Phase results in one of the two key elements to the project: the design. Without a detailed design, the second key element, the system, cannot be constructed, implemented, trained upon, or operated. The decisions made in this phase regarding technology, frameworks, implementation, and configuration and change management ensure a sound foundation for the project. While ambiguous requirements are the greatest source of project failure, a poor design ranks second. The approval of the Design Phase deliverables, the completion of the Design project status review, and the approval to proceed to the next phase, signify the end of the Design Phase.