PHASE 9: OPERATIONS AND MAINTENANCE PHASE

During the Operations and Maintenance Phase, the information system's availability and performance in executing the work for which it was designed is maintained. The State realizes the largest value for the system during this phase. System operations continue until the system's termination date, when the next phase, Disposition, begins.

1.0 OBJECTIVE/GOALS

Objective
Successful completion of the Operations and Maintenance Phase should comprise:

- Management of changes to the system to support end users
- Monitoring of system performance
- Performance of required security activities such as backups, contingency planning, and audits
- Continuation of end user support through training and documentation

Goals
The purpose of the Operations and Maintenance Phase is to ensure the information system is fully functional and performs optimally until the system reaches its end of life.

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 Systems 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 Systems Team should:

- Write comprehensive, easy to understand documents with no redundant information.
- Develop an organized document repository for critical project information, so Systems 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
Standard Operating Procedures (Updated) – defines in detail how the Operations & Maintenance (O&M) team will perform the business processes related to the operations and maintenance of the system. Whereas the User Guide is focused on the use of the system specifically, the Standard Operating Procedures address all related business processes.	• Provide detailed instructions for future business processes • Ensure consistent execution of business processes • Drive performance improvement and improve organizational results	Systems Team	Agency CIO
Performance Reports – tracks routine metrics as system performance indicators.	• Report on agreed upon system performance measurements • Include key performance indicators	System Manager	No approval required
Implementation Notice – formally requests approval for system changes made during the Implementation Phase.	• Formally request approval for system implementation	Project Manager	Agency CIO
Program Trouble Reports – provide details regarding an incident related to any aspect of an IT service.	• Document and track system incidents • Communicate need to address a disruption in service and/or a reduction of quality of service	Systems Team	No approval required

Deliverable	Goals	Developed By	Approved By
In-Process Review Report – formally reports the health of the system. It includes summary of performance reports but is more formalized and usually developed quarterly.	• Provide Agency CIO with routine insight into system performance • Include results of user satisfaction reviews	System Manager Agency CIO	Agency CIO
User Satisfaction Review – determines the current user satisfaction with the performance capabilities of the system	• Quantify user satisfaction levels	System Manager	Agency CIO
Disposition Plan – identifies how the termination of the system/data will be conducted, and when, as well as the system termination date, software components to be preserved, disposition of remaining equipment, and archiving of life cycle products.	• Address all facets of archiving, transferring, and disposing of the system and data	System Manager	Agency CIO Business Owner

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 during this phase:

- Agency CIO
- System Manager
- Systems Team
- Process Improvement Review Board
- Security Officer

- Procurement Officer
- Business Owner
- Project Stakeholders

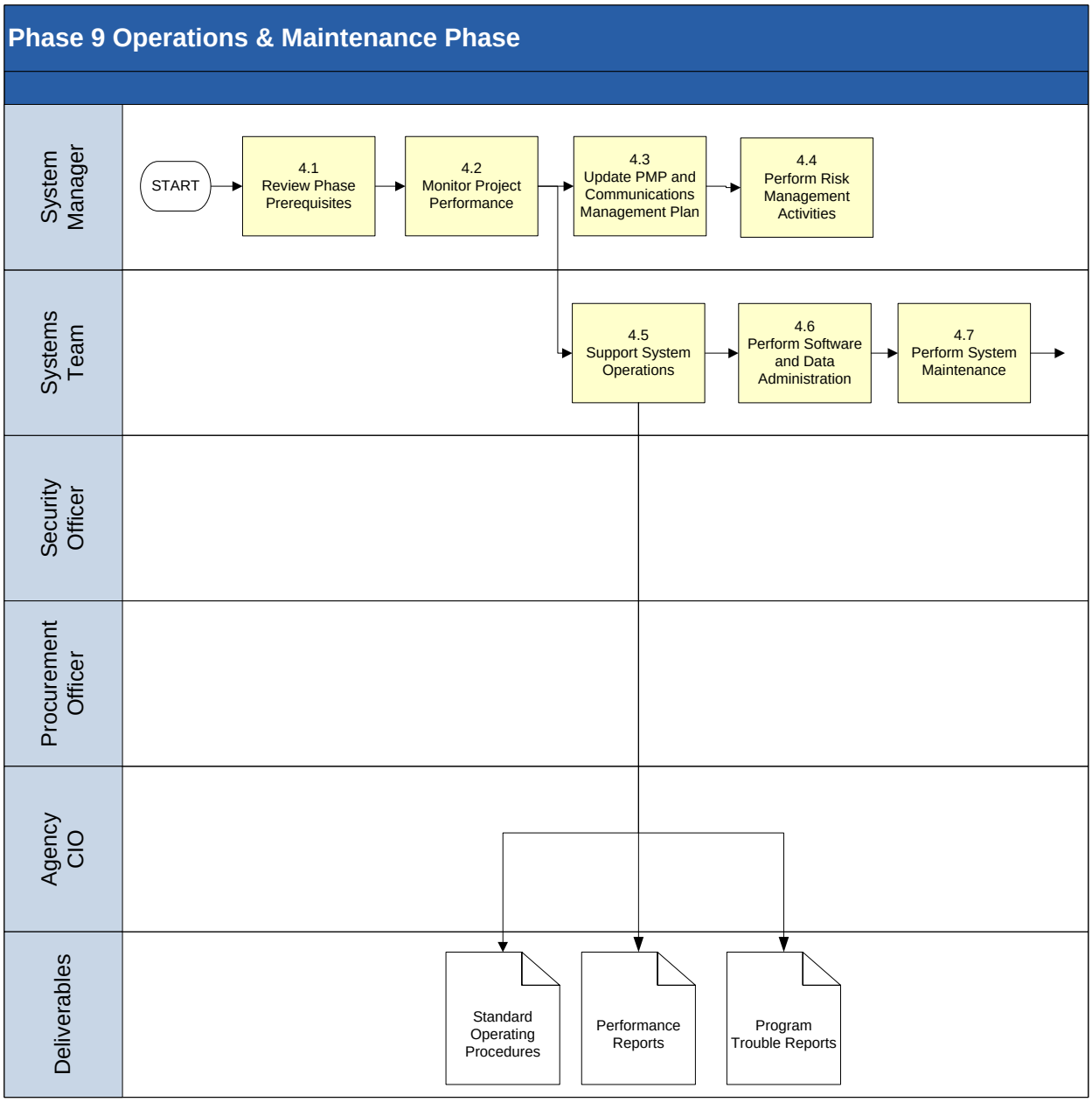
RACI Key
Responsible – Describes role that executes the activities to achieve the task.
Accountable – Describes roles that own the quality of the deliverable and sign off on work that Responsible provides.
Consulted – Describes roles that provide subject matter expertise.
Informed – Describes roles that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

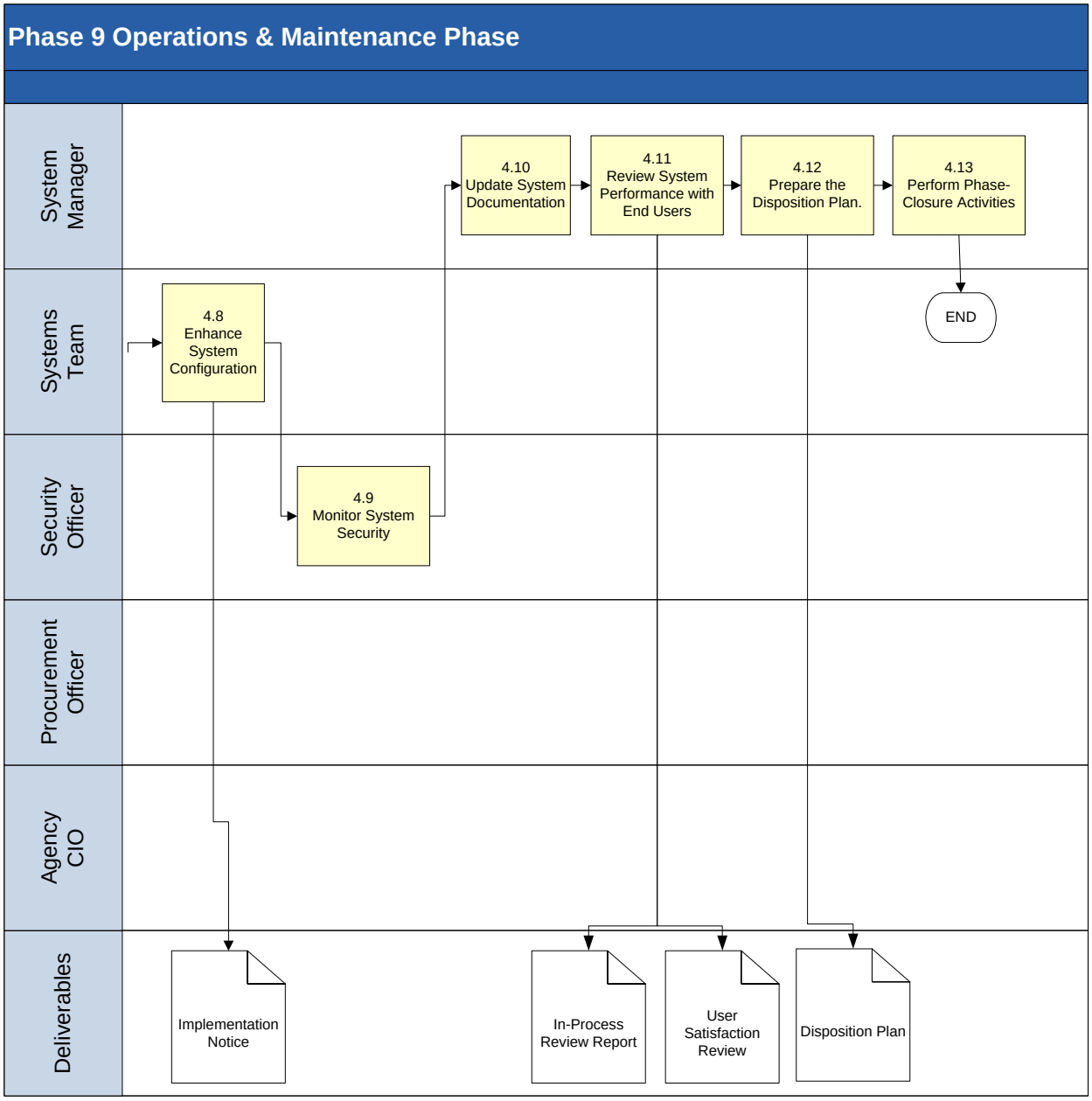
Deliverable	Agency CIO	System Manager	Systems Team	Business Owner	Process Improvement Review Board	Security Officer	Procurement Officer	Project Stakeholders
Standard Operating Procedures	A	R	I	I	I	I	I	C
Performance Reports	A	R	I	I	I	I	I	I
Implementation Notice	A	R	I	I	I	I	I	I
Program Trouble Reports	A	R	I	I	I	I	I	C
In-Process Review Report	A	R	I		I	I	I	I
User Satisfaction Review	A	R	I	I	I	I	I	C
Disposition Plan	A	R	I	A	I		I	I

Possible RACI Matrix

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

4.0 TASKS AND ACTIVITIES





4.1 **Review Phase Prerequisites.**

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

- System has been successfully deployed and is fully functional.
- Operations or System Administration Manual is complete and current.
- User Guide is complete and current.
- End-users have received training on proper system use.
- System documentation is complete and available.
- All deficiencies noted in the Implementation Phase are being corrected.
- System has completed Certification and Accreditation according to DoIT guidelines.

4.2 **Monitor Phase Performance.**

The System Manager monitors phase performance by gathering status information about:

- All changes to baseline system performance
- Change management information
- Activity progress with status details
- Activities initiated and finished
- Testing results and deliverable acceptance
- Resource utilization data

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

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

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

4.4 **Perform Risk Management Activities.**

The System Manager conducts risk management activities during the Implementation Phase; these activities include:

- Identification – determination of 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 section 11 of *PMBOK*.
- Response Planning – planning of methods for developing mitigation, transfer, or avoidance strategies to reduce risk
- Monitoring and Control – tracking risks, monitoring residual risk, identifying new risks, executing response plans, and evaluating risk management effectiveness

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

4.5 **Support System Operations.**

The Systems Team supports the system and its end users as an integral part of the information system's day-to-day operations. The Operations or System Administration Manual defines tasks, activities, and responsible parties for these daily activities and must be updated as changes occur. By monitoring the system continuously, the Systems Team ensures that the production environment is fully functional and performs as specified. Critical support tasks and activities include:

- Guarantee of required system availability
- Implementation of non-emergency requests during scheduled outages
- Ensuring the documentation in the operating procedures of all processes, manual and automated
- Acquisition of critical system supplies (e.g. paper, cabling, toner, tapes, removable disks) before the supply is exhausted
- Performance of routine backup and recovery procedures
- Performance of physical security functions by ensuring all system staff and end users have the proper clearances and access privileges
- Ensuring currency and testing of contingency planning for disaster recovery
- Ensuring periodic training on current and new processes for end users
- Ensuring monitoring and meeting of service level objectives while taking remedial actions for any deficiencies
- Monitoring of performance measurements, statistics, and system logs

The system log, the Operations Manual, journals, and other logs are invaluable in emergencies and should be kept in a central repository with other operational documentation.

The System Manager reviews the Program Trouble Reports, which document problems with the system through an automated system. The reports typically include:

- Date and time
- Issue reporter
- Problem description
- Apparent cause
- Assigned developer
- Resolution
- Test results

Other information may be included and depends on the reporting system. The reporting system should permit an audit of the entire process from problem identification to problem resolution and case closure.

4.6 **Perform Software and Data Administration.**

The Systems Team constantly monitors and performs software and data administration. Team members also monitor software performance to ensure transactions are executed correctly and accurately. The Systems Team performs administrative tasks such as:

- Performance of production control and quality control functions
- Interfacing with other functional areas to maintain system integrity

- Installation, configuration, upgrade, and maintenance of databases and update of any related system documentation
- Development and performance of data and database backup and recovery routines for data integrity and recoverability as documented in the Operations or System Administration Manual
- Development and maintenance of a performance and tuning plan for online processes and databases
- Performance of configuration and design audits to correct software, system, parameter, and configuration deviations

4.7 **Perform System Maintenance.**

The System Manager and the Systems Team continuously monitor the performance of the system in regard to hardware, software, databases, and network. Daily operations of the system require identifying and implementing minor modifications for it to function optimally and correctly. Document these modifications using a Change Implementation Notice in the configuration management repository, and follow the change management process to receive approval for the modifications. The Change Implementation Notice contains a requested change to the system by a user and its priority or urgency.

Maryland law states that agencies must have the approval of the Agency CIO:

> *…before making expenditures on major information technology development projects (MITDP), which were defined as projects that included planning, procuring, creating, installing, testing, or providing initial training on an IT project in which:*
>
> - *the estimated total cost equals or exceeds $1 million;*
> - *the project is undertaken to support a critical business function associated with the public health, education, safety, or financial well-being of the citizens of Maryland; or*
> - *the Secretary of Budget and Management determines that the project requires the special attention and consideration given to a MITDP.*
>
> – *SB212, Acts of 2008*

Change requests that meet the following criteria are maintenance work:
- Estimated cost of modifications are below maintenance costs
- Proposed changes can be implemented within one system year
- Impact to system is minimal or necessary for accuracy of system output

4.8 **Enhance System Configuration.**

The Systems Team implements changes to the information system to upgrade hardware and add new or remove old functionality. These enhancements might originate with user requests for specific capabilities or from the Systems Team's identifying solutions to substantive routine system problems. Document any enhancements using a Change Implementation Notice, and follow the change management process to receive approval for the enhancement. All maintenance and enhancements are part of a continuous improvement process for the system.

After the system has been implemented, any major system modifications required must follow the configuration management process from planning through implementation.

4.9 **Monitor System Security.**

The Security Officer monitors the security of the information system according to the System Security Plan. As modifications occur, the Security Officer confirms the System Security Plan is current. As a part of reviewing system security, the Security Officer performs a risk assessment and analysis; the results provide the basis for new or modified security controls. The Security Officer also oversees routine testing of the Disaster Recovery Plan.

When a security incident occurs, the Systems Team sends an incident report to the System Manager. These incident reports must be filed with the State's Incident Response Group. The System Manager routinely reviews the regular system security reports with the Security Officer.

The System Manager routinely reviews DoIT's security policies and standards on DoIT's website and guidelines endorsed by NIST and the NSA. The System Manager and Security Officer coordinate with project stakeholders on regular disaster recovery tests for the system. Additional information on security and disaster recovery and best practices is available on the NIST Computer Security Division – Computer Security Resource Center website.

4.10 **Update System Documentation.**

The System Manager reviews and updates all system documentation, particularly the Operations Manual and Disaster Recovery Plan, as changes occur or on a regularly scheduled basis.

4.11 **Review System Performance with End Users.**

The System Manager routinely reviews the information system performance with end users to identify changes and problems. A User Satisfaction Review, which might include a Customer Satisfaction Survey, can obtain feedback on operational systems to help determine if the systems are accurate and reliable**.**

The System Manager with the Agency CIO conducts the In-Process Review usually quarterly but at least annually. Agencies should conduct the In-Process Review in mid-year to prepare for annual IT Project Request budgets, due in September.

During the In-Process Review, the System Manager evaluates system performance against baseline performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system. Project stakeholders may request ad hoc reviews when deemed necessary. The User Satisfaction Review, which can be added to the In-Process Review, can indicate the need for a Process Improvement Review Board meeting or initiation of a proposal for a new system. The agency should establish a Process Improvement Review Board comprised of project stakeholders representative of all groups impacted by the system. The Business Process Review Board participates in the In-Process Review meetings to ensure proper communication and decision-making.

4.12 **Prepare the Disposition Plan.**

4.12.1 **Document Description**

The Disposition Plan identifies how the termination of the system/data will be conducted, and when, as well as the system termination date, software components to be preserved, data to be preserved, disposition of remaining equipment, and archiving of life cycle products.

4.12.2 **Typical Content**

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

- Introduction – Includes purpose and scope, points of contact, project references, and glossary
- Notifications – Describes the plan for notifying known users of the system being shut down and other affected parties
- Data Disposition – Describes the plan for archiving, deleting, or transferring to other systems the data files and related documentation
- Software Disposition – Describes the plan for archiving, deleting, or transferring to other systems the software library files and related documentation
- System Documentation Disposition – Describes the plan for archiving, deleting, or transferring to other systems the hardcopy and softcopy systems and user documentation
- Equipment Disposition – Describes the plan for archiving, deleting, or transferring to other systems the hardware and other equipment
- Project Staff – Describes the plan for notifying project team members of the shutdown of the system, and the transfer of these team members to other projects
- Project Records – Describes the plan for archiving, deleting, or transferring to other projects the records of project activity
- Facilities – Describes the plan for transferring or disposing of facilities used by the project staff for the system being shut down

4.12.3 **Guidance for Document Development**

The objective of the Disposition Plan is to end the operation of the system in a planned, orderly manner and to ensure that system components and data are properly archived or incorporated into other systems. At the end of this phase, 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 of the organizations using the system or the operation of other systems that will use the data and/or software of the present system.

The Agency CIO and Business Owner review and sign the Disposition Plan.

4.12.4 **Dos and Don'ts**

- Do ensure that the Disposition Plan is consistent with the State Archivist's records management guidance.
- Do plan to inform users of the decision to terminate operation of the system before the actual termination date.

- Do plan to archive all documentation, including the life-cycle products generated during the earliest tasks of the life cycle as well as the documentation for users and for operation and maintenance personnel.

4.13 **Perform Phase-Closure Activities.**

The System Manager and the Systems Team prepare and present a system status review for the Agency CIO and other project stakeholders after performing Operations and Maintenance Phase tasks. This review addresses:

- Status of Operations and Maintenance Phase activities
- Planning status for the Disposition Phase
- Status on personnel resource availability for Disposition Phase
- Verification that all changes are conducted in accordance with the approved Change Management Plan

The System Manager also updates the risk analysis and the Maryland Enterprise Architecture Repository with any new or updated components before beginning the Disposition Phase.

5.0 CONCLUSION

During the life of the system, the Operations and Maintenance Phase is the longest and most expensive as the information system provides the most value to the organization in this phase. After system functionally becomes obsolete, the information system is ready to move to retirement in its final phase, the Disposition Phase.