

530R86123

c.1

CONFIGURATION MANAGEMENT

GUIDANCE

Prepared by:

Information Management Staff
Office of Policy, Budget, and Program Management
Office of Solid Waste and Emergency Response
U.S. Environmental Protection Agency
Washington, D.C. 20460

15 APR 1986

U.S. Environmental Protection Agency
Region V, Library
230 South Dearborn Street
Chicago, Illinois 60604

U.S. Environmental Protection Agency

U.S. Environmental Protection Agency

TABLE OF CONTENTS

CONFIGURATION MANAGEMENT GUIDANCE

PART I: MANAGEMENT SUMMARY

A. PURPOSE OF CONFIGURATION MANAGEMENT

- 1.1 CM Defined
- 1.2 History of CM
- 1.3 Objectives of CM
- 1.4 Relationship to Life Cycle Management

B. IRM ROLES IN OSWER

- 2.1 Program Offices
- 2.2 OSWER Managers
- 2.3 Configuration Management Boards

C. CM FUNCTIONS AND BASELINES

- 3.1 Functions
- 3.2 Baselines

D. INTEGRATING LIFE CYCLE AND CONFIGURATION MANAGEMENT

- 4.1 CM and LCM

E. CM CHANGE CONTROL

- 5.1 Change Classification
- 5.2 Change Procedures
- 5.3 Reviews and Audits
- 5.4 Configuration Status Accounting

PART II: CONFIGURATION MANAGEMENT GUIDANCE

A. SCOPE OF CONFIGURATION MANAGEMENT

- 1.1 Configuration Management Plan

B. CM RESPONSIBILITIES

- 2.1 Roles of Participants

C. CONFIGURATION MANAGEMENT FUNCTIONS

- 3.1 Configuration Management Board
- 3.2 CMB Responsibilities at Project Initiation
- 3.3 CMB Baseline Management Responsibilities
- 3.4 CMB Change Control Responsibilities
- 3.5 CMB Reviews of the AIS
- 3.6 Configuration Audits

SUMMARY OF CM FUNCTIONS

Configuration Identification
Configuration Change Control
Configuration Status Accounting
Configuration Auditing

PART III: DOCUMENTATION REQUIREMENTS AND CONTROL PROCEDURES

A. CONFIGURATION MANAGEMENT BOARD

1.1 Establishment
1.2 Meetings
1.3 Minutes

B. CONFIGURATION MANAGEMENT PLAN

2.1 Approval

C. CONFIGURATION CHANGE CONTROL

3.1 Classes of Change
3.2 Change Control Documentation
3.3 Reviews and Audits
3.4 Prototyping and Fourth Generation Languages

CM PLAN CHECKLIST

OSWER LCM & CM GLOSSARY

APPENDIX

CONFIGURATION MANAGEMENT
MANAGEMENT SUMMARY
PART I

CONFIGURATION MANAGEMENT

PART I

SUMMARY

A. PURPOSE OF CONFIGURATION MANAGEMENT

The purpose of this document is to provide guidance on configuration management (CM) of automated information systems (AIS) in the Office of Solid Waste and Emergency Response (OSWER). Configuration management is a method applying technical and administrative direction and surveillance throughout the life of an AIS. It is applied consistently and uniformly throughout the life cycle of the system. It ensures that each AIS supports the programmatic functions for which it is intended.

1.1 CM Defined

Configuration management is a discipline which manages the changes to an AIS. A change is defined as any event, action, or policy requirement which can or does affect the scope of an AIS, its schedule, or resource requirements. CM involves technical and administrative reviews of the various stages of development and operation of an AIS. It is used to perform the following activities:

- o Identify and document functional and physical characteristics of the components of an automated information system;
- o Control changes to those characteristics;
- o Record and report these changes as well as the resulting implemented status of the AIS;
- o Identify and document inconsistencies among successive control points as they are established through configuration audits;
- o Resolve inconsistencies as they relate to system design, system test results, and system operations. Ensure that technical and user documentation reflect the resolution of these issues.

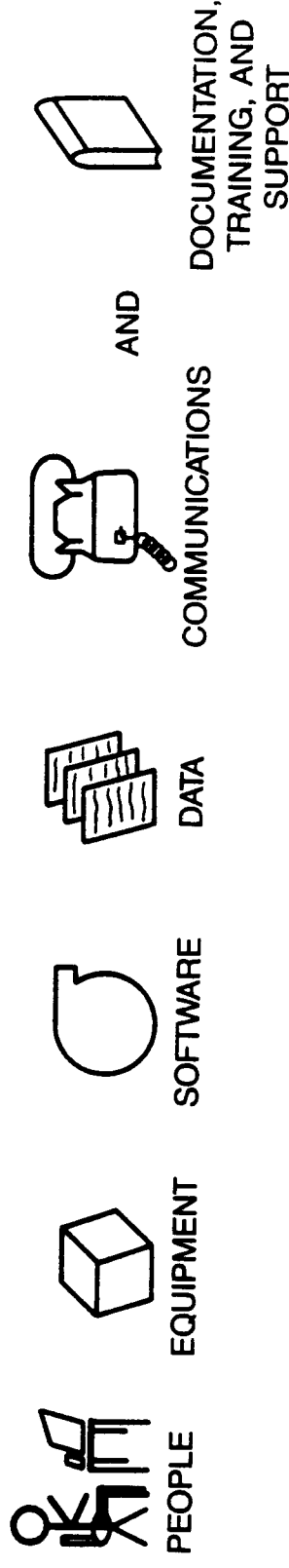
The configuration management process is used in concert with the life cycle management process to direct the total development of an automated information system. These are complementary processes.

1.2 History of CM

CM as a discipline was started in the 1950's as part of the construction of large-scale software projects. By the 1970's CM had achieved a place in the world of data processing as a well-defined discipline for project management. The growth of CM as a set of control mechanisms followed hand-in-hand with the growth in the complexity and cost of computer-based information systems.

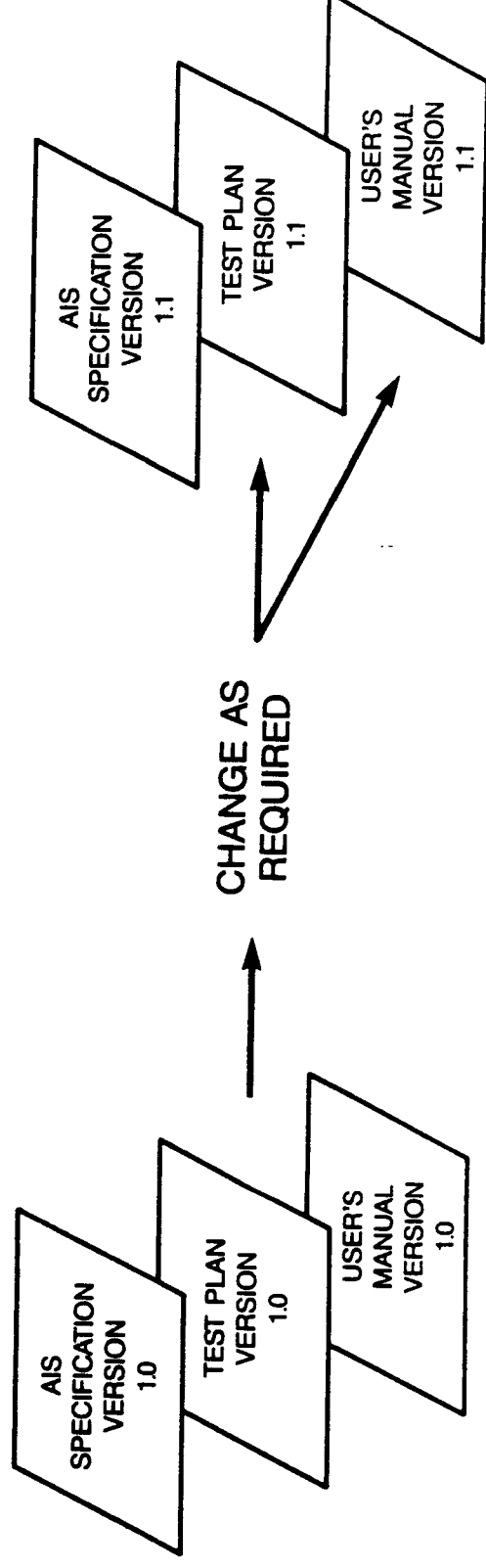
AUTOMATED SYSTEM OVERVIEW

AN OSWER AUTOMATED INFORMATION SYSTEM (AIS) IS:



TO PERFORM A SPECIFIC TASK

CONFIGURATION MANAGEMENT PERMITS EVOLUTION



WHILE MAINTAINING A USABLE SYSTEM THAT MEETS ITS ORIGINAL REQUIREMENTS

CM is practiced today in the Federal government based on two parts of the Federal Information Processing Standards publications (FIPS PUBS) issued by the National Bureau of Standards, U.S. Department of Commerce. These are FIPS PUBS 38 and 64 which discuss software documentation issues. In 1986, the Office of Management and Budget emphasized the use of FIPS PUBS in its Circular A-130; "Information Resources Management."

1.3 Objectives of CM

OSWER configuration management requires that all elements or components of an AIS be fully defined in terms that can be examined, measured, and verified. CM is the only assurance that OSWER-developed software programs and systems will function as required and planned. Configuration management provides assurance of system compliance with OSWER goals, objectives, and requirements, and ensures all changes are thoroughly documented and continue to meet the initial program mission.

There are five basic objectives for configuration management in OSWER.

1. Provide a mechanism to ensure the documentation of all changes.
2. Anticipate the effects of changes on the costs or schedules for each AIS.
3. Maintain the integrity of the project schedule.
4. Maintain up-to-date documentation on the status of the AIS and the project.
5. Ensure that changes and the project administrator's responses to them are communicated to all project personnel.

Developers of large or complex AISs often ask why they should follow CM practices. The answer is simple. Suppose everyone working on an AIS suddenly left town? If there was a good CM system in place, it would still be possible to:

- know the latest accepted version of every system, subsystem, or document;
- know the entire change history of the system; and,
- know everything the system was supposed to do and how to test it.

Further, if these questions can be answered, it is then possible for new personnel to do the following critical tasks with the system.

- operate the system
- maintain the system
- modify the system; or,
- complete the system if they had to.

At every stage of development or operation of an AIS, there is documentation defining and describing the system. This documentation is in the form of system specifications, requirements, manuals, definitions such as Data Element Dictionaries (DED), and instructions. To maintain system integrity, CM ensures that any necessary change at any level is reflected properly at all hierarchical levels. In addition, there must be an "audit" trail from every functional requirement through the system to the point in the programming at which that requirement is satisfied. This audit function provides a memory for the AIS.

CM deals with the process of change. Changes to an AIS can result from internal or external factors. Internal factors include changes in an organization's functions, its lines of authority, new personnel or new assignments for existing personnel, as well as the inevitable changes in resources and priorities for them. External factors can in some ways mimic or even be the cause of internal changes. These include new legislation, new hardware or software, changes in the skill mix of the employees due to changes in the labor market, or other, unknown external events which cannot be anticipated

CM is also the management discipline used to assess the impacts of changes to an AIS. In many cases, changes will affect the project schedule, the amount of resources required, and other factors that the Project Administrator has "locked up" in the AIS project plan. If project disasters are to be avoided, then changes must be handled in an orderly and controlled manner. The procedures for controlling changes to an AIS over time must be a formal part of every AIS project plan. This component of an AIS project plan is called a "Configuration Management Plan," and it will be described in detail in Parts II and III of this guidance.

1.4 Relationship to Life Cycle Management

Configuration management and life cycle management (LCM) have linked functions within the overall framework of program and project management. Along with the disciplines of project management, CM and LCM complete a cycle necessary to ensure that organizational goals and objectives, not technical capabilities, are paramount. LCM is the highest level of organizational control over a project. It is the process of making a decision to continue, change, or end an AIS at selected points in the life cycle of that system. In summary, LCM is a decision making process. CM is a change control, documentation, and review process.

B. INFORMATION RESOURCE MANAGEMENT ROLES IN OSWER

2.1 Program Offices

Each program office in OSWER has responsibilities for information resources management (IRM). These include the requirement to define its information needs, to monitor the effectiveness of each AIS supporting these needs, and to specify the requirements for each new AIS or changes to existing systems as these needs evolve over time. The primary point of contact in each program office is the Information Management Coordinator (IMC).

The IMC is an EPA employee, usually a line supervisor, who performs the technical oversight of his/her office's compliance with CM guidance. AIS Project Administrators usually report to the IMC or work closely with the IMC regardless of organizational lines of authority.

The Project Administrator (PA) usually is the project manager for an AIS, or several AIs, depending on program office priorities and staff assignments. The PA is responsible for day-to-day management of the AIS in terms of costs, schedules, staffing, and overall technical performance of the system.

2.2 OSWER Managers

OSWER senior managers are the standing members of the IM Steering Committee (SC). The SC provides guidance on policy, scheduling, program impacts, and direction on the development and implementation of OSWER automated information systems and the technologies to support them.

2.3 Configuration Management Boards

Configuration Management Boards (CMB) have direct oversight responsibility for the development and operation of an AIS. The scope of activities includes implementation of this guidance for all AIs in OSWER. This includes mission critical systems as well as cross-cutting administrative systems. Each CM Board will have a charter describing the authority, membership, review and decision making processes, as well as recordkeeping functions necessary to support its operations. A sample charter is included in Part III of this guidance.

CMBs are established for each major programmatic area. A separate Board executes configuration management of cross-cutting administrative systems. Program specific systems are reviewed by program specific CM Boards, whose members are appointed by their respective office directors. Permanent members of the cross-cutting administrative systems board are appointed by the Chairman of the Steering Committee. Other members of the CM Board serve whenever their particular applications are on the agenda. The PA for an application always attends when his/her application is on the agenda as does the IMC for the office(s) involved.

OSWER AIS CONFIGURATION MANAGEMENT RESPONSIBILITIES

OSWER LCM

ENSURES THAT:

- THE NEED FOR THE AIS IS VALID
- THE METHOD CHOSEN TO MEET THE NEED IS APPROPRIATE
- THE DESIGNED, DEVELOPED, AND IMPLEMENTED AIS MEETS THE NEED
- THE AIS CONTINUES TO MEET THE NEED OVER ITS OPERATIONAL LIFE

PROJECT ADMINISTRATOR

ENSURES THAT:

- THE AIS IS PROPERLY DESIGNED TO MEET THE NEED
- THE AIS IS DEVELOPED AND IMPLEMENTED ACCORDING TO THE DESIGN
- AS THE AIS EVOLVES AND CHANGES, IT STILL MEETS ITS DESIGN CRITERIA

OSWER CM

ENSURES THAT:

- THE CONTRACTOR MAINTAINS ADEQUATE CONTROLS OVER ALL AIS CHANGES
- THE TECHNICAL AND PERFORMANCE STATUS OF THE AIS IS KNOWN AT ALL TIMES
- ALL CHANGES TO THE AIS BENEFIT OSWER
- THERE ARE NO UNAUTHORIZED CHANGES TO THE AIS

Each CMB is responsible for establishing system baselines and authorizing changes to the AIS. The CMB reviews all system documentation prepared by the Project Administrator prior to its submission to the Steering Committee for approval of a System Decision Paper. The Configuration Management Board makes technical judgments that the products of an AIS correctly descend from and satisfy the AIS Mission Element Needs Statement and its supporting functional requirements. These are not subjective or value judgments, but are determinations that the actual component-by-component, program-by-program performance of the parts of an AIS produce the specified system or end-product output.

C. CM FUNCTIONS AND BASELINES DEFINED

3.1 Functions

There are four primary functions in the configuration management process:

- o Configuration Identification: This process identifies all components of the system being managed. These are the items of the system identified for configuration management and are referred to as "configuration items" (CIs). The result of this process is the identification of the controllable components of an AIS; e.g. the hardware, software, and documentation.
- o Configuration Change Control: This process is used to evaluate whether changes to a component of an AIS should be approved or disapproved.
- o Configuration Status Accounting: This is the process by which changes made to a particular item are recorded. This bookkeeping process denotes what changes have been made, the impact of future changes, and it also includes a schedule for making future changes to the AIS. It is the process of tracking each configuration item through all of its changes and modifications.
- o Configuration Auditing: This is a detailed review of the performance of all configuration items that constitute an AIS. The audit function is a process that assures compliance with organizational standards for the AIS.

3.2 Baselines

The key to configuration management is the establishment of technical control points called "baselines." In its most fundamental aspects, CM is the systematic evaluation, coordination, and disposition of all proposed changes to these baselines. The baseline, plus approved changes, provide an up-to-date description of an automated information system. There are four CM baselines that Project Administrators must develop.

- o Functional - represents the approved functional system requirements and associated documentation of these requirements (i.e., functional and data requirements documents).
- o Allocated/Design - represents the approved specifications (such as system specification, design specification, or program specifications for ADP and data communications) of the system. The allocated baseline documentation specifies the design and test criteria of every item subject to configuration change control.
- o Product - represents the approved detailed design of each configuration item and all supporting documentation (operators manual, program maintenance manual, users manual, etc.) along with the updated versions of the specifications.
- o Operational - represents all the approved system CIs, documentation, and procedures required to operate and maintain the AIS effectively.

D. INTEGRATING LIFE CYCLE AND CONFIGURATION MANAGEMENT

The functions and baselines of configuration management relate to the phases of Life Cycle Management in the following manner.

4.1 CM and LCM

Life Cycle Phases 1 & 2: the MENS and Concept Development, define the functional requirements of an AIS. Once these are approved by the Steering Committee, they become the basis for the "Functional Baseline" established in CM. The CMB controls and monitors the effects of changes to a baseline to provide confidence that the AIS satisfies the need identified in the MENS. At project initiation, the CMB reviews the contractor's CM plan, which is the only basis for determining that CM as a discipline will be effective for this AIS.

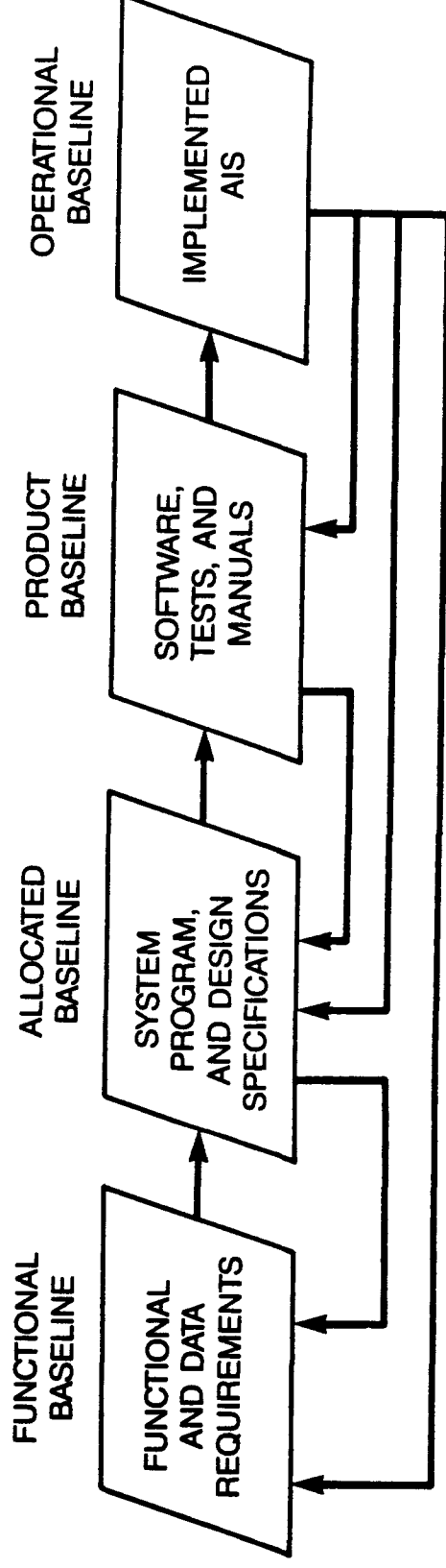
THE CMB MONITORS THE ENTIRE AIS LIFE CYCLE

LCM PHASE 1		LCM PHASE 2	LCM PHASE 3	LCM PHASE 4	LCM PHASE 5
PROJECT INITIATION		CONCEPT DEVELOPMENT	DESIGN	DEVELOPMENT	OPERATION
MENS ANALYSIS					
FUNCTIONAL CONFIGURATION AUDIT		ALLOCATED CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	
			CHANGE CONTROL		
			CI REVIEW AND AUDIT		
			BASELINE CONTROL		

CMB CONTROL OF CHANGES AND MONITORING OF BASELINES PROVIDE LIFE CYCLE MANAGEMENT ASSURANCE THAT THE AIS SATISFIES NEEDS IDENTIFIED IN THE MENS.

CONFIGURATION MANAGEMENT CREATES A FEEDBACK LOOP TO CONTROL CHANGES

WITHOUT CONFIGURATION MANAGEMENT
COMPLEX SYSTEMS COULD NOT BE PERMITTED TO EVOLVE



NECESSARY CHANGES CONTROLLED AT ALL STAGES TO PROTECT AIS INTEGRITY

Life Cycle Phase 3: the System Program and Design Specifications, once approved by the Steering Committee, establish the basis for the "Allocated Baseline" established in CM. The CMB determines a point in the design to begin control of design documentation. It continues to control that documentation throughout the life of the AIS. All systems undergo changes. Change control ensures that all changes are necessary, beneficial, and can be implemented without adverse effects on any other part of the AIS.

Life Cycle Phase 4: Software System Tests, Technical, and User Manuals, once approved by the Steering Committee, establish the basis for the "Product Baseline" in CM.

Life Cycle Phase 5: the Operational AIS, establishes the basis for the "Operational Baseline" in CM. The CIs for a fully implemented system include every aspect of that system including the hardware, system software, peripherals, as well as third party software, e.g., the application.

E. CM CHANGE CONTROL

5.1 Change Classification

Changes to an established baseline are classified as:

Class I - changes affect the operational capability of the AIS as specified in the baseline. It may also be a change required to maintain the compatibility of interfaces with equipment, software programs, or support facilities.

Class II - changes may be implemented without further approval. These include editorial changes, corrections in coding of computer programs, and other changes of a minor nature.

Class III - changes which simply make a Ci what it was intended to be, e.g., deletion of redundant lines of code.

5.2 Change Procedures

Class I changes require a formal, documented change proposal, an impact assessment, and coordination and review by the Configuration Management Board. Class II changes are also reported in a formal document that references the affected baseline(s), includes a description of the change, and a justification of why it is a Class II change. Examples of change control forms are included in Part III of this guidance.

CMB CHANGE CONTROL PERMITS ORDERLY DEVELOPMENT

PROJECT INITIATION MENS ANALYSIS CM PLAN APPROVAL	CONCEPT DEVELOPMENT		DESIGN	DEVELOPMENT	OPERATION
	LCM BASELINE SUPPORT				
	FUNCTIONAL CONFIGURATION AUDIT	ALLOCATED CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	
			CHANGE CONTROL		
			CI REVIEW AND AUDIT		
			BASELINE CONTROL		

THE CMB DETERMINES A POINT IN DESIGN TO BEGIN CONTROL OF DESIGN DOCUMENTATION AND CONTINUES THAT CONTROL THROUGHOUT THE LIFE OF THE AIS.

ALL SYSTEMS UNDERGO CHANGES. CHANGE CONTROL ENSURES THAT ALL CHANGES ARE NECESSARY, BENEFICIAL, AND CAN BE IMPLEMENTED WITHOUT HARM TO THE REST OF THE SYSTEM.

5.3 Reviews and Audits

A series of reviews must be scheduled at significant points in the developmental process for an AIS. These reviews provide control points for the design and implementation of the AIS. CM typically requires the following formal reviews:

System Requirements Review (SRR): a formal review of the functional requirements of an AIS.

System Design Review (SDR): a formal review of the system design approach for an AIS.

Preliminary Design Review (PDR): a formal review of the subsystem design approach for each configuration item.

Critical Design Review (CDR): a formal review conducted at the end of the definition and design phase and before the translation of the logic and algorithms to coded instructions.

Functional Configuration Audit (FCA): the formal examination of each configuration item to verify that the performance specified in the system specifications has been achieved.

Physical Configuration Audit (PCA): the formal examination of the coded version of a computer program configuration item against its technical documentation.

5.4 Configuration Status Accounting

This is the reporting and documenting of all proposed changes. Accounting procedures ensure that baselines are maintained accurately and changes to them are recorded in a timely manner. This is accomplished by the PA through the documenting of proposed or actual changes to baselines, designs, software, or data structures.

THE CMB MONITORS THE ENTIRE DEVELOPMENT CYCLE

PROJECT INITIATION MENS ANALYSIS CM PLAN APPROVAL	CONCEPT DEVELOPMENT	DESIGN	DEVELOPMENT	OPERATION
	LCM BASELINE SUPPORT			
	FUNCTIONAL CONFIGURATION AUDIT	ALLOCATED CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT
			CHANGE CONTROL	
			CI REVIEW AND AUDIT	
			BASELINE CONTROL	

AUDITS BY THE CMB PROVIDE LIFE CYCLE MANAGEMENT ASSURANCE THAT THE AIS SATISFIES NEEDS IDENTIFIED IN THE MENS. CMB CONTROL OF BASELINES ENSURES THAT THE AIS MEETS ALL OF ITS SPECIFICATIONS AND PERFORMANCE REQUIREMENTS.

CONFIGURATION MANAGEMENT
GUIDANCE
PART II

CONFIGURATION MANAGEMENT

PART II

GUIDANCE

A. SCOPE OF CONFIGURATION MANAGEMENT

1.1 Configuration Management Plan

The scope of configuration management as applied to OSWER automated information systems includes software development and system operation. Configuration management begins with a "Configuration Management Plan" for controlled development of an AIS. The Configuration Management Plan presents the procedures and control points for each identified CM function. The plan is prepared by the Project Administrator and defines the participation of the organizations concerned with development of an AIS. An outline of the required elements of a Configuration Management Plan is included in Part III of this guidance. After a Configuration Management Plan is developed, the Configuration Management Board ensures that the plan is implemented and followed in proper detail and that all substantive changes to the AIS are approved.

The size and complexity of an AIS will determine the degree of formal configuration management that will be required, but certain actions, such as the use of a Data Element Dictionary, are always required. The performance of the AIS is the primary concern of configuration management. System documentation is the formal record of that performance.

B. CM RESPONSIBILITIES

2.1 Roles of Participants

The primary participants and their responsibilities in the CM process are as follows:

Project Administrator: The PA is responsible for the documentation that defines and describes total AIS development as well as single components of a system. The PA ensures the system supports the mission need and is developed and implemented according to the design.

In this guidance, configuration management is referred to as a PA responsibility, even though actual performance may be by a contractor, a government agency, or an internal OSWER staff. Oversight of the PA in terms of quality assurance is also performed by the OSWER Information Management Coordinator (IMC) for the office responsible for the AIS. The IMC is a permanent member of the CMB reviewing the AIS.

THE CM PLAN IS CRITICAL

PROJECT INITIATION		CONCEPT DEVELOPMENT	DESIGN	DEVELOPMENT	OPERATION	
						MENS ANALYSIS
		LCM BASELINE SUPPORT				
		FUNCTIONAL CONFIGURATION AUDIT	ALLOCATED CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	PHYSICAL CONFIGURATION AUDIT	
				CHANGE CONTROL		
				CI REVIEW AND AUDIT		
		BASELINE CONTROL				

AT PROJECT INITIATION, THE CMB DEFINES THE CM REQUIREMENT AND APPROVES THE CONTRACTOR'S CM PLAN.

THE AIS CONTRACTOR'S CONFIGURATION MANAGEMENT PERFORMANCE WILL ONLY BE AS GOOD AS THE ORIGINAL PLAN.

Configuration Management Board (CMB): CMBs are established for each major programmatic area. A separate board executes configuration management of cross-cutting administrative systems. Each CMB is responsible for establishing system baselines and authorizing changes to their AISSs. Each board has oversight responsibility for the development and operation of all AISSs within its jurisdiction. The role of the CMB is to ensure the AIS continues to meet the mission need and fulfills its design criteria as it evolves and changes over time. The CMB reviews and delivers any documentation for system development or operation of an AIS that requires a decision by the Steering Committee.

Steering Committee: It is the policy making body for information resources management issues. The Steering Committee reviews plans and budgets, and makes system development and operation decisions based on documentation produced by the Project Administrator and reviewed by the CMB. The Steering Committee delegates authority for implementation of CM for specific AISSs to the Project Administrator. The PA is accountable for the quality of his/her work to the IMC and to the CMB.

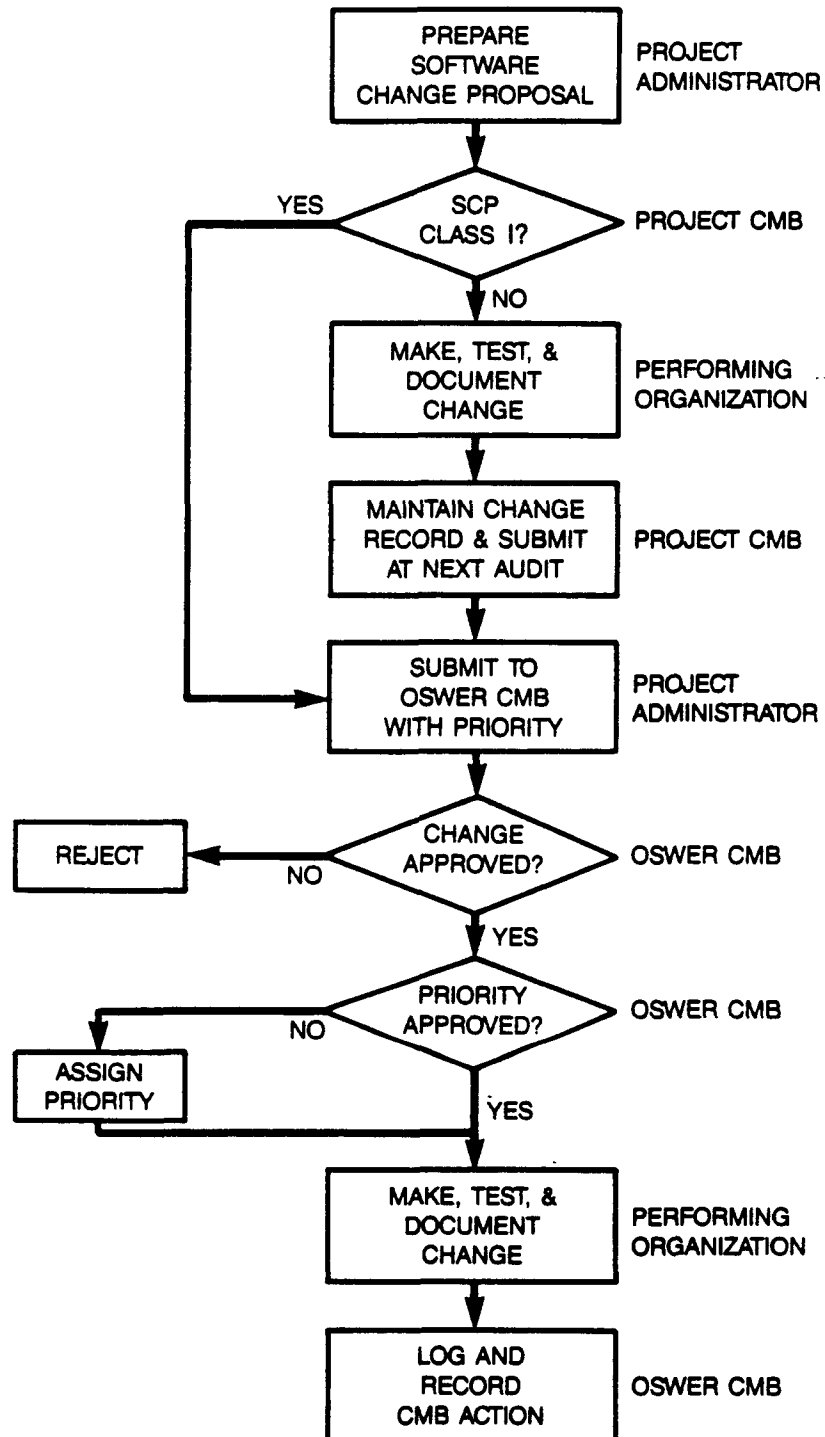
C. CONFIGURATION MANAGEMENT FUNCTIONS

3.1 Configuration Management Board

Duties and Responsibilities:

- a. Review and approve the CM Plan
- b. Review the AIS baseline prepared at the time the project is initiated as well as prior to the presentation of System Decision Paper I to the Steering Committee. Review subsequent System Decision Papers as they are prepared by the PA.
- c. Ensure that the PA maintains proper files and records on the baselines established for the AIS.
- d. Review the PA's change control procedures and ensure they are implemented at the appropriate points in the development of the AIS.
- e. Approve all Class I changes and monitor the quality of system change documents.
- f. Conduct configuration audits including key configuration item reviews, which are the "Preliminary Design Review" and the "Critical Design Review."

OSWER CONFIGURATION CHANGE MANAGEMENT



g. Conduct baseline audits at each stage in the life cycle of the AIS including:

- LCM Phases 1 & 2: Functional Requirements Baseline audit
- LCM Phase 3: Allocated (Design) Baseline audit
- LCM Phase 4: Product Configuration audit
- LCM Phase 5: Physical Configuration audit

3.2 CMB Responsibilities at Project Initiation

The CMB has a number of important responsibilities at the initiation of an AIS. First, the CMB must review the statement of work, the project plan, and the PA's Configuration Management Plan. Second, the CMB must approve a calendar of configuration management meetings related to the development schedule of the AIS. All members of the CMB must commit themselves to keeping this calendar. The size and complexity of the AIS will determine the scope of the Configuration Management Plan. However, the use of a Data Element Dictionary will always be a required element of a CM Plan.

3.3 CMB Baseline Management Responsibilities

The CMB has the primary responsibility for reviews and audits of the baselines of an AIS. The PA has the technical management responsibility for developing and operating the AIS. The CMB is accountable to the Steering Committee for ensuring that the PA has developed an AIS that satisfies the "Mission Element Needs Statement" (MENS) at each baseline. This is accomplished through its oversight role in reviewing the documentation for the AIS.

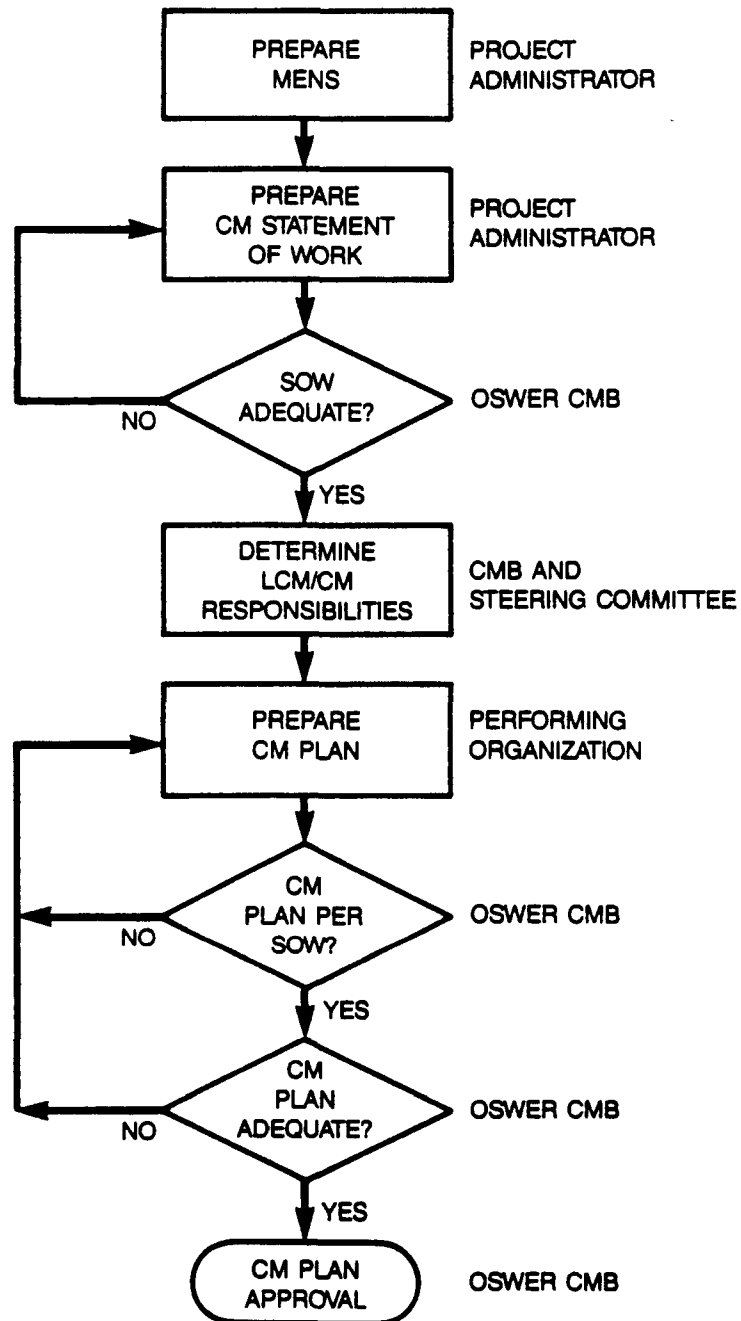
The CMB is also responsible for maintaining the integrity of the AIS baselines during its control of changes to those baselines. Once the CMB has approved a baseline, that baseline cannot be changed without further approval of the CMB.

3.4 CMB Change Control Responsibilities

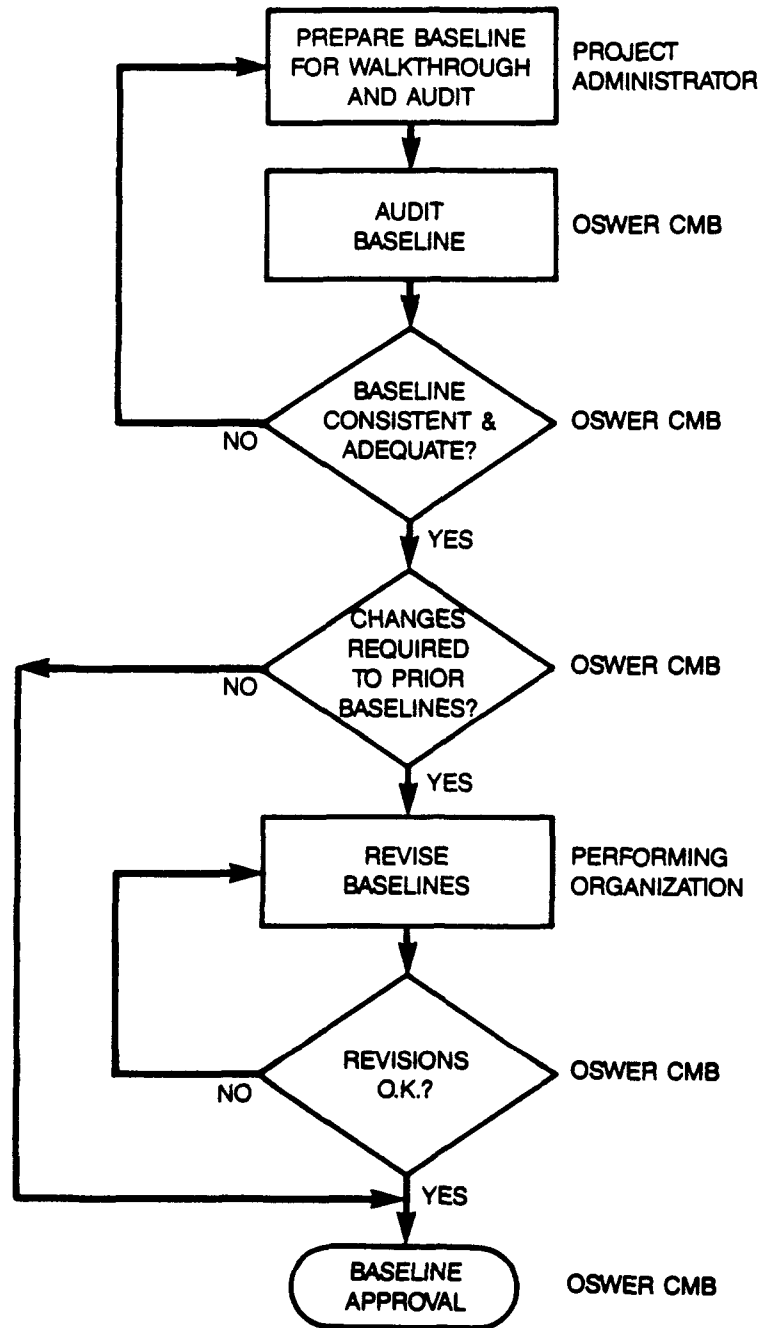
The CMB has the authority, derived from the Steering Committee, and responsibility to approve all Class I changes to configuration items. A change can be classified as Class I if it meets one or more of the following criteria:

- the change will cause increases in the cost of the AIS or the time for completion of components or the entire system;
- the change will affect test procedures or schedules;
- the change involves interfaces with other computer systems;

OSWER CONFIGURATION MANAGEMENT AT PROJECT INITIATION



OSWER BASELINE MANAGEMENT



-- the change will affect computer performance, disk storage, memory requirements, or other critical system performance parameters; or

-- the change will affect privacy, security, or data validity.

Class I changes are reviewed based on their priority. There are three priorities for review of Class I changes.

Priority 1 Emergency: The system is down and no alternative method exists for accomplishing the necessary functions. The Chairperson of the CMB, or in that person's absence, the Director, Information Management Staff, may authorize the action required to bring the AIS back to fully operational status. A followup, complete justification for the action and report on the emergency must be submitted to the CMB as quickly as is practical. All affected configuration items must be reviewed by the PA and the CMB to ensure the integrity of the AIS's baselines.

Priority 2 Urgent: A "work around" solution to a job has caused operational or unintended problems that cannot be resolved without further changes to the AIS. Documentation of the problem and system testing are a priority and the CMB must be briefed as to why an unauthorized "work around" was attempted that disrupted the integrity of the AIS. The CMB will submit a report on any unauthorized actions to the Chairman of the Steering Committee.

Priority 3 Routine: The CMB is responsible for prompt resolution of proposed changes to an AIS baseline. However, routine change requests should be handled in a manner that does not interfere with other, higher priority activities.

3.5 CMB Reviews of the AIS

The configuration items that make up a baseline are reviewed and the baseline as a whole is audited. Because configuration items are reviewed during major life cycle phases, a CI may be examined several times during its development in increasing levels of detail. Before a set of configuration items is accepted as a baseline, a formal examination is performed. There are two review processes: preliminary and critical; and four audits: functional requirements, allocated (design), product configuration, and physical configuration. The following paragraphs describe these reviews and audits.

Preliminary Reviews: These are conducted by the Project Administrator and usually include a structured walkthrough of the configuration item. The goals of this review are to:

- o assure that the system designers thoroughly understand the configuration items to be developed;
- o keep the system designers from expending effort in the wrong direction;
- o provide management with an understanding of the system design which may be useful in guiding other configuration items or in achieving smooth system integration; and,
- o communicate design detail between system development team members.

Critical Reviews: These are initiated by the Project Administrator after a major portion of the work has been completed and an initial version of each configuration item has been developed and implemented. At this point, the PA and the Configuration Management Board jointly perform the review. Again, the PA may be asked to present a structured walkthrough of the configuration item. This critical review, which is more formal and detailed, identifies specific shortcomings of each configuration item that require further attention in order to produce a satisfactory result. Specific goals of the critical review are to:

- o ensure that the configuration item, as implemented, conforms to all preceding approved documentation;
- o ensure that any additional specific guidance provided by management (privately or through the preliminary review) is reflected in the product; and,
- o ensure that the item conforms to project and agency standards.

3.6 Configuration Audits

A baseline audit is a detailed technical analysis of all configuration items developed during implementation of each life cycle phase of an AIS. It ensures that each CI conforms to the specifications set forth as well as all documentation that is under configuration control in the current baseline.

Because of the broad scope of a baseline audit, it may be repetitive with initial examination resulting in modification and subsequent followup review of configuration items. The PA will perform such modifications in order to make the CI conform to the specifications. The PA ensures that any modification representing a change in specifications is handled through the configuration control procedures.

The computer programs that make up the operational AIS go through the life cycle phases that create the CM baselines. These phases include: 1) concept development; 2) definition and design; 3) system development; and 4) operation, maintenance, and evaluation. Baseline audits are performed after each of these four phases.

The baselines and their corresponding audits are listed below.

<u>Baseline</u>	<u>Audit</u>
Functional	Functional Requirements
Allocated/Design	Allocated (Design)
Product	Product Configuration
Operational	Physical Configuration

Functional Requirements Audit: This takes place at the end of Life Cycle Phases 1 & 2 (MENS and Concept Development). It constitutes a necessary review by the CMB of System Decision Paper I prior to its presentation to the Steering Committee. The functional requirements audit consists of a detailed examination of the functional description, the data requirements, and the Configuration Management Plan (CMP). Approval of documentation during the functional requirements audit provides the basis for identification of a series of configuration items to be developed during the definition and design phase of the AIS. A general description of these CI's must be included in the CM Plan. Results of this audit establish the functional baseline.

Allocated/design Audit: This takes place near the end of Life Cycle Phase 3 (Design). It constitutes a necessary review by the CMB of System Decision Paper II prior to its presentation to the Steering Committee. The allocated/design audit is conducted at the completion of the definition and design phase of the AIS. It is a detailed examination of the documentation of the CI's to be developed during this phase. This audit assures that these configuration items conform to the functional design of the system as provided by the original Mission Elements Needs Statement and as modified by functional changes approved by the CMB and the Steering Committee.

There are two types of CI documentation audited at this point: first is computer software definition; second is specification of the elements of the AIS data base that are to be manipulated by the software. The allocated/design audit ensures the required consistency and coordination between these two types of documentation. Results of this audit establish the allocated/design baseline.

Product Configuration Audit: This takes place near the end of Life Cycle Phase 4 (System Development). It constitutes a necessary review by the CMB of System Decision Paper III prior to its presentation to the Steering Committee. The product configuration audit is a technical audit of the results of baseline testing and test data. The CMB conducts this audit prior to installation of an updated version of the AIS. This audit and the physical configuration audit are the only audits that are repeated during the life of the system. They also are the only audits in which the CMB does not confine itself to a review of documentation.

In this audit, all configuration items that have been changed or implemented since the last audit are reviewed. This includes acceptance testing of software. The methodology and procedures for these tests are included in the PA's system test plan, which is a configuration control item. It is also desirable to test and examine all programs that have not themselves been changed, but may be affected by the changes to other CIs. For example, if a program creating a reference table is modified, any program or subsystem reading that table must be retested.

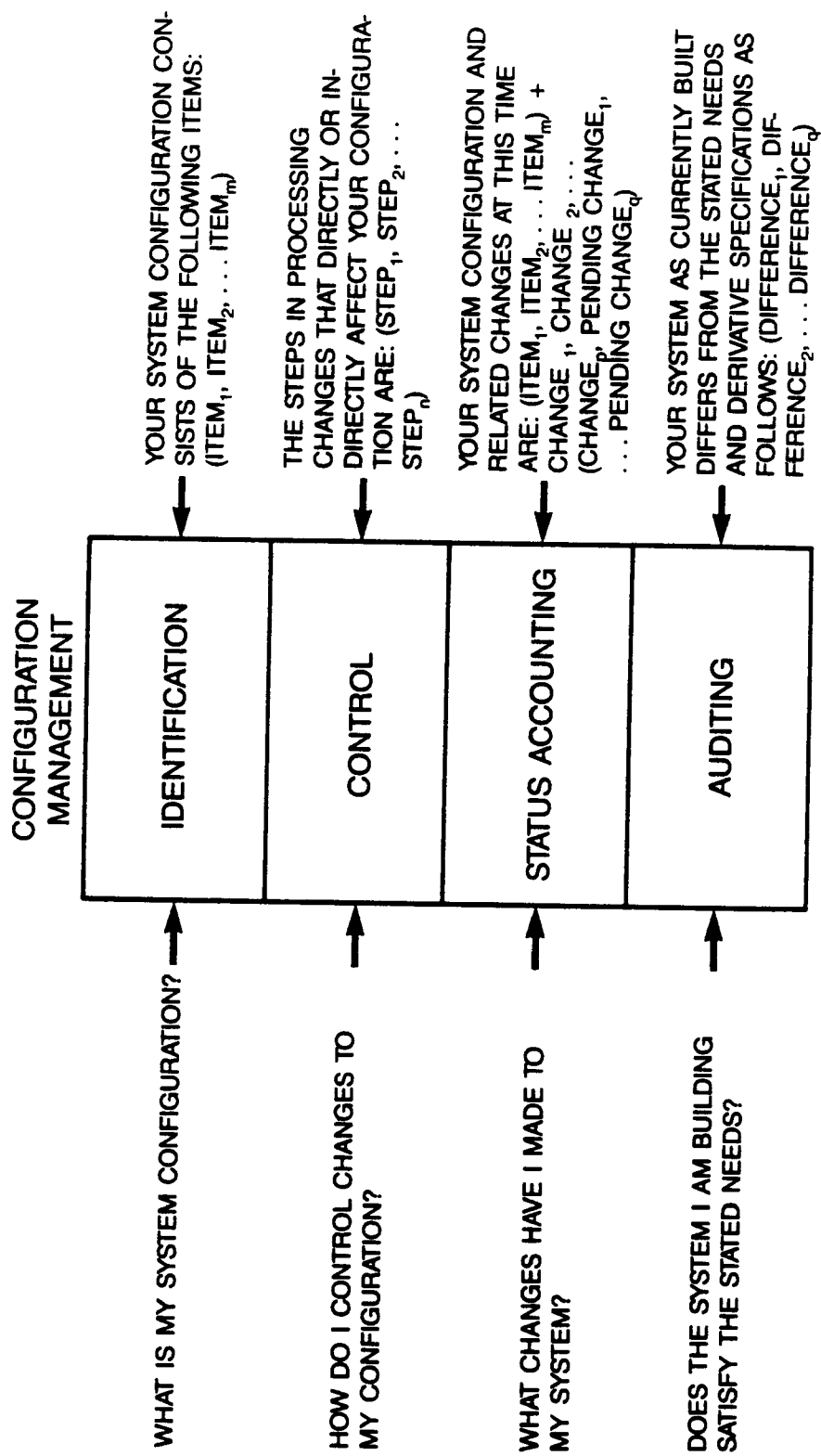
The product configuration audit assures that all software, documentation, and procedures accurately reflect the system specifications as modified through configuration change control. At the conclusion of this audit, the PA develops a checklist for use in the physical configuration audit.

Physical Configuration Audit: This takes place near the end of Life Cycle Phase 5 (Operations). It constitutes a necessary review by the CMB of System Decision Paper IV prior to its presentation to the Steering Committee. The physical configuration audit is a formal examination by the Configuration Management Board to determine that the fully developed AIS conforms in all respects with its specifications, tests, and requirements documentation.

The PA's system test plan contains the procedures, descriptions of test software, and acceptable performance criteria that prove the AIS or any of its subsystems fully satisfy the intended need. The PA ensures that the user(s) of the system sign off on the test plan and the CMB ensures this action. The physical configuration audit:

- o ensures operational soundness of software, hardware, and documentation;
- o reviews documentation to verify all changes are included;
- o ensures that each configuration item in the baseline is performing as intended and that the baseline as a whole is meeting the requirement for which it was established; and
- o ensures the system is still meeting requirements of the MENS.

THE FOUR COMPONENT ELEMENTS OF CM



SUMMARY OF CM FUNCTIONS

Configuration Identification

ISSUE: What is my system configuration?

FUNCTION: It is the process of identifying the controllable components of an AIS by defining and documenting measurable characteristics of hardware, software, and documentation. The identified components become individually controlled "configuration items" (CI). A particular CI may be a hardware or software item or a document. Thus, a system is composed of CIs and the management of each CI constitutes management of the configuration of the total system. Each CI is documented in specifications or other types of documentation. When this documentation is approved, usually at management reviews, the total group of CIs becomes the foundation for establishing a baseline.

PA ROLE: Prepare the Statement of Work
Prepare the Configuration Management Plan

CMB ROLE: Review the Mission Element Needs Statement
Review and approve the Statement of Work
Review and approve the Configuration Management Plan

The Configuration Management Plan, prepared by the Project Administrator, provides and manages configuration control over the development or operation and maintenance of an AIS. The plan:

- o presents the procedures for each identified CM function;
- o identifies configuration items;
- o specifies what CM baselines should be established and at what points of development;
- o identifies documentation requirements for each baseline;
- o defines the participation of the organization concerned with development of the AIS: names the participants and defines their roles on the CMB; and,
- o lists the CM schedule.

The CMB will review the MENS before submitting it to the Steering Committee for approval. If the AIS is approved, the CMB will review the requirements expressed in the Project Administrator's statement of work and will approve them for the particular application.

Note: A complete checklist to be used by the CMB in assessing the adequacy of the Configuration Management Plan is included in Appendix A of this guidance.

Configuration Change Control

ISSUE: How do I control changes to my system's configuration?

FUNCTION: This is the systematic evaluation, coordination, and approval or disapproval of proposed changes to any baseline. Formal control of the configuration of a system begins with the definition and approval of a baseline for the system and continues throughout the system's life cycle. All changes to a baseline must be proposed on a system change request form (SCR) that describes the change and its impacts on all affected CIs.

PA ROLE: Determines class status and priority of proposed changes.
Maintains change records.

CMB ROLE: Reviews the Mission Element Needs Statement.
Approves class status changes and priorities.
Maintains logs of CMB actions.

The Configuration Management Plan defines the procedures for configuration change control including type of change, source of change, sample forms, submission criteria, and implementation requirements. The plan also defines CMB procedures for screening, coordination, evaluation, and disposition of proposed changes. All proposed changes will be evaluated to determine if they:

- o correct deficiencies;
- o satisfy need and operation requirements;
- o effect substantive life cycle cost savings; and,
- o prevent schedule slippage.

The Project Administrator screens all change proposals to determine the class status and priority of the change. The CMB has the authority and responsibility to approve all class status changes to configuration items and approve the priority under which changes are to be implemented.

Note: A complete description of class status and priorities is given in Part III of this guidance.

Configuration Status Accounting

ISSUE: What changes have I made to my system?

FUNCTION: The activity here is to record and track the "approved configuration baseline" and the implementation status of changes being made to the baseline. This documentation is the means through which actions affecting individual configuration items are recorded and reported to the appropriate managers of the AIS. It is the bookkeeping part of configuration management that provides feedback information to determine whether decisions of the Configuration Management Board are being implemented as directed.

PA ROLE: Performs status tracking and provides required reports.

CMB ROLE: Reviews and approves status accounting reports.

Status accounting is the recording of how the AIS evolved and where the system is at any time relative to what appears in the published baseline documentation. It is the administrative tracking and reporting of all configuration items formally identified and controlled. It also involves the maintenance of records to support software configuration auditing. Although administrative in nature, status accounting is a function that increases in complexity as the system life cycle progresses. This complexity generally results in large amounts of data being recorded and reported. In particular, configuration status accounting encompasses reporting and recording the following:

- o the time at which each to-be-established baseline and update came into being;
- o descriptive information for each configuration item;
- o descriptive information about each change;
- o status of each change to a configuration item;

- o status of technical and administrative documentation associated with a baseline or update (such as a plan prescribing tests to be performed on a baseline for updating purposes); and,
- o deficiencies in a to-be-established baseline uncovered during a configuration audit.

Configuration Auditing

ISSUE: Does the system I am building satisfy the stated needs?

FUNCTION: This is the quality assurance activity for configuration management. It is a detailed process used to examine all configuration items in a baseline or the baseline as a whole to assure that the functional and physical state of the configuration item or baseline complies with the documentation approved by the CMB. This process provides management with a capability to direct the technical activity of system development along the required path.

PA ROLE: Provides agenda for reviews and baseline audits.
Conducts preliminary configuration item reviews.

CMB ROLE: Reviews Mission Element Needs Statement.
Performs critical reviews of CIs.
Performs audits of AIS baselines.
Maintains logs of audit and review actions.
Reports audit concerns to PA and Steering Committee.

The Configuration Management Plan includes a schedule of audits and reviews in the development and implementation of the AIS. The Configuration Management Board is responsible to the Steering Committee for ensuring that the system satisfies the approved MENS at each baseline.

CONFIGURATION MANAGEMENT
DOCUMENTATION REQUIREMENTS
AND
CONTROL PROCEDURES
PART III

CONFIGURATION MANAGEMENT

DOCUMENTATION REQUIREMENTS AND CONTROL PROCEDURES

PART III

Each major OSWER program office designates a Configuration Management Board with oversight responsibility for the automated information systems used to support their program missions. This part of the guidance contains the documentation requirements and control procedures to implement configuration management in the development of those AISs.

The following is a list of activities in the configuration management process and the documentation or procedures required to achieve each step. Except for change control, which can occur anytime after the establishment of the first baseline, the CM process follows a natural progression that is based on the life cycle decisions being made.

A. CONFIGURATION MANAGEMENT BOARD

1.1 Establishment

Each Configuration Management Board will be established by charter with membership consisting of "standing members" drawn from the program offices, the OSWER Information Management Staff, and the Office of Information Resources Management. Standing members of program specific CMBs are appointed by their respective office directors. Standing members may appoint ad hoc members representing specific AIS constituencies. Both standing members and ad hoc members have equal vote on the Board. Each member or approved alternate will attend all meetings and participate in reviews or audits. A sample CMB charter is in the appendix.

1.2 Meetings

CMB meetings are used to review the status of the AIS, its baselines, and configuration items. They provide a forum for routine review of Class II and Class III changes made since the previous meeting, give the CMB an opportunity to resolve trouble reports submitted as well as consider new non-emergency change proposals, change requests, and trouble reports. These meetings also serve to notify the CMB of any changes in review and audit schedules.

In addition, the CMB can hold three types of special meetings:

- o A kickoff meeting to review the technical description of the AIS and a draft outline of the Configuration Management Plan;

- o A meeting to approve the PA's Configuration Management Plan; and,
- o AIS trouble or emergency meetings to make decisions that cannot wait until the next scheduled meeting.

In a "kickoff" meeting, the CMB will determine whether the draft outline of the Configuration Management Plan implies a level of effort on the part of the PA that is excessive for the AIS. If so, the Board may recommend, for non-complex AISs, that the PA be required to submit a less complex "CM Plan" so that CM is tailored to the realities of the AIS effort. A special meeting also will be held to approve the PA's final CM Plan.

Special meetings also may be called in response to emergencies that require immediate action or special situations which, although not emergencies, require action before the next scheduled CMB meeting in order to avoid disruption of the AIS developmental or operational effort. A major feature of emergency meetings is the establishment of the schedule for documentation, review, and audit, if any of these need to be performed after-the-fact to meet the emergency. Where possible, such deferral is to be avoided.

1.3 Minutes

Each Configuration Management Board meets as necessary to monitor the status of the AIS. It is a requirement of CM that minutes of every meeting be kept. The minutes of each meeting are the primary product generated and may be in any format determined by the chairman of the CMB. The minutes provide a history of all AIS decisions by:

- o listing all actions taken and the reasons for CMB decisions;
- o listing all documentation submitted in support of statements and proposals; and,
- o recording the schedule for implementation of approved changes as part of the CMB monitoring function.

B. CONFIGURATION MANAGEMENT PLAN

2.1 Approval

The PA's plan must ensure that the CMB can execute its responsibilities in configuration management. It is the responsibility of the PA to devise a plan that is satisfactory to the CMB. It is the CMB's responsibility to verify that the plan is fully in compliance with this guidance.

The CMB approves the Project Administrator's plan by memorandum, to which is attached a copy of the executed plan checklist. A sample checklist is included in the appendix. The flow of activity begins with initial establishment of the level at which configuration management will be pursued in project development and ends with approval of the plan.

Responsibility for providing the CMB with adequate understanding of the nature and complexity of the system rests with the PA, as does initial screening of the plan against the checklist. To the greatest extent possible, existing CM procedures will be used (to avoid unnecessary costs), but the provisions of the checklist should be present in the plan.

Regardless of the complexity of the AIS, the CMB will ensure that the following minimum requirements are met:

- Organization: CMB decisions must be independent of project administration and the Board must have sufficient authority to enforce CM requirements.
- Configuration Identification: The plan must identify a set of configuration items which, taken together, adequately define the AIS, its baselines, and its documentation. An identification or numbering scheme must be used that permits not only hierarchical relation of the CI's but "horizontal" relation as well.
- Data Element Dictionary (DED): In addition to use of the OSWER DED, it is preferable that the project utilize a dedicated automated system. Regardless of whether a manual or an automated CM system is used, the DED must have provisions to control all data elements, algorithms, interfaces, specifications, documentation, test parameters, and data relationships.
- Configuration Control: The configuration control process must encompass baselines, versions, documentation, software at and below the CI level, specifications, and Class I, Class II, and Class III changes.
- Configuration Status Accounting: The accounting methods must ensure currency and accuracy of the status of all controlled configuration items, a method for dissemination of status information to all project personnel and users.
- Reviews and Audits: In addition to appropriate provisions for internal reviews and audits, the configuration management process must permit CMB review and audit that minimizes the time OSWER personnel spend in reviewing and auditing, while at the same time maximizing OSWER CMB oversight and control functions.

- Software Library: The AIS must have provisions for control and storage of master copies of all software during both development and operational phases.

C. CONFIGURATION CHANGE CONTROL

As with other configuration management functions, the CMB has oversight responsibility for change control of developmental or operational AISs, but does not have technical responsibility for the changes and their management. Nevertheless, the CMB must have (through the Board itself or the IMS acting in a staff and advisory role) the technical knowledge necessary to evaluate the merit of proposed changes and to determine that the PA has considered the appropriate ramifications of any proposed change.

3.1 Classes of Change

Changes are identified by classes (Class I - Formal, Class II - Informal, and Class III - Technical). The CMB has the authority and responsibility to approve all Class I changes to configuration items. Changes to Classes II and III do not need to be approved by the CMB.

Class I (Formal) changes are major changes that affect operational capability as specified in the baseline, or is a change required to maintain the capability of interfaces with systems equipment, computer programs or facilities. Class I changes to CI's are those which:

- o cause cost increase or schedule delays;
- o require any change in test procedures or schedules;
- o involve interfaces with other systems;
- o change system timing or memory storage/reserve requirements;
- o reduce, degrade, or modify substantially any operational capability as specified in baseline specifications or other documents;
- o impact privacy, security, or data validity; or,
- o have any impact on OSWER organizational matters, including personnel utilization, personnel qualifications, operational procedures, maintenance, or training.

Class II (Informal) changes are modifications within a CI that do not change the controlled characteristics of the CI -- input, output, interfaces, use, or test documentation -- but does change the CI internally in such a way that program listings are changed, future modifications or maintenance would require knowledge of the change, or processing steps have been substantially modified even though they produce the same result. If the old CI and the modified CI are not interchangeable in the operational AIS, the change cannot be Class II. The most common Class II changes are those made to improve system efficiency or to comply with quality assurance standards.

Class III (Technical) changes are those which simply make the CI do what it was intended to do in the manner originally specified. An example would be the deletion of redundant lines of code. Technical changes are rigorously documented by the PA (as are Class I and Class II changes) because what may seem to be a routine technical change may, in fact, have much greater ramifications, making it necessary to return to the condition prior to the change to correct a problem.

3.2 Change Control Documentation

The change control procedures presented in the approved Configuration Management Plan are accomplished through the use of forms designed for the purpose. Types of forms used would be:

- Log of CMB Actions and Minutes of Meetings
- System Change Requests
- Document Change Requests
- Software Change Proposal
- Software Trouble Reports
- Change Request Status Reports
- Technical Change Requests
- Technical Change Summaries
- Emergency Change Requests
- Problem Resolution Summaries

Information that the PA must ensure appears on these forms should include at a minimum:

- Performing organization name
- AIS name and identifying number
- Title of the change request
- Type and priority of change (Class I, Emergency)
- Identity of CI's to be changed
- Justification for change
- Performance requirements
- Impact of change on performance and on other CI's
- Interface requirements
- Cost to implement change
- Work plan and schedule for change

The system change request documents major changes that affect functionality of a configuration item. There also are document and technical change requests that improve but do not modify functionality, i.e., clarifying report headers, adding a date on a printout, etc. Document and technical change requests are retained by the PA for review by the CMB.

Software Trouble Reports: These ordinarily come to the CMB only as backup to a change request. The Board may wish to examine them in connection with a pending change approval action. The project trouble report system must provide a means for users and system maintainers to bring problems to the attention of the Board so that authorization may be granted to examine the problem in detail and determine the appropriate resolution.

The Configuration Management Board change log serves a historical purpose in addition to permitting the CMB to track the progress of changes it has authorized. A change log form will be maintained for each AIS. Prior to each regular CMB meeting, the secretary will determine the status of all changes that are still in progress or have not been formally approved and update the change log accordingly.

Version Control: A "version" may correspond to a baseline configuration but it can also refer to individual CI's within a baseline in instances where major revisions have been made. Control of software and documentation versions is the responsibility of the PA.

The CMB must authorize acceptance and implementation of each new version of software or documentation. The PA will present a description of the new version, including a listing and description of all changes incorporated, an analysis of the impact of the changes, and a report on testing and auditing of the version. Once the CMB accepts the version, the PA establishes an implementation schedule (based on user requirements) and reports to the CMB any problems encountered during implementation or in attempting to use the new version after its implementation. If major changes are made to the version, the normal change control procedure will be followed. If required changes are minor or technical, the PA will make them and report completion to the CMB.

3.3 Reviews and Audits

The Configuration Management Board may determine at any time that it should conduct informal or formal reviews or audits of configuration items or baselines. Generally, the review and audit responsibility of the CMB will be discharged at the scheduled points established in the accepted Configuration Management Plan.

Reviews: The preliminary and critical reviews provide early evaluations of AIS configuration items in order to identify and anticipate problems so there is sufficient time to take action economically. The CMB will depend on the PA to conduct the preliminary review. This review will evaluate the overall approach to the CI design and adequacy for the AIS. It checks the involvement and impact on other CI's.

The critical review is performed by the PA and CMB. Each CI is reviewed as part of the system, subsystem or program specifications development tasks. The reviewable item will be a preliminary draft of the specification itself. For software CI's, the product reviewed will be an error-free compilation or tested version of the computer program. The PA will present a structured walkthrough.

Audits: The audits are: functional requirements audit, allocated (design) audit, product configuration audit and, physical configuration audit. These audits are described in Part II of this guidance. Prior to each scheduled audit, the PA will forward a checklist of audit parameters and a set of brief functional descriptions of the AIS and its major subsystems to the CMB. At this time, the CMB also may request copies of the current versions of the AIS specifications and the requirements documentation to assist them in determining that the checklist provided is adequate for the audit.

Also, the PA will submit a proposed audit agenda listing documents to be reviewed, demonstrations to be performed, and test reports to be analyzed. The agenda will include provisions for description of the AIS at a given baseline as compared to the AIS at the previous baseline. Deficiencies as well as improvements shall be cited. The CMB may require additions to the audit procedure. In particular, it may require detailed walkthroughs, repeats of critical tests, validation of maintenance and recovery procedures, and demonstration of user operation of the AIS.

At the conclusion of the formal audit, the CMB may, at its discretion, retain copies of all documentation and test reports and may require that demonstration software remain available (along with any hardware to support it) for further analysis. The CMB may not take longer than 10 working days, either to accept the AIS baseline under audit, or to require changes to make the baseline acceptable.

Any changes made to resolve problems found during the audit must be accepted by the CMB before the baseline can be approved. This acceptance may require a repeat of the audit, or it may consist merely of formal acceptance of a report from the PA that the change has been made and tested satisfactorily, depending on the circumstances of the rejection of the baseline. Any changes or updates made to a baseline after it has been established must go through the configuration change control procedures.

3.4 Prototyping and Fourth Generation Languages

CMB procedures and requirements do not change with the choice of prototyping or with the use of fourth generation software languages in the development of an AIS. A prototype development CM plan shall meet all of the requirements of this guidance and demonstrate to the CMB that full configuration control will be maintained over the AIS throughout its life cycle.

CM PLAN CONDENSED OUTLINE

CONFIGURATION MANAGEMENT PLAN

1. PURPOSE
2. MANAGEMENT
 - A. ORGANIZATIONAL RELATIONSHIPS
 - B. REFERENCES
3. CONFIGURATION IDENTIFICATION
 - A. IDENTIFICATION
 - B. BASELINES
4. CONFIGURATION CONTROL
 - A. CONFIGURATION MANAGEMENT BOARD
 - B. CHANGE PROCEDURES
5. CONFIGURATION STATUS ACCOUNTING
6. CONFIGURATION AUDITS

OSWER CM PLAN CHECKLIST

- a. Is the plan well organized, clearly written, and appropriately illustrated?
- b. Is the plan tailored to the proposed development task, with sufficient attention to special requirements?
- c. Do CM functions interface properly with other project functions?
- d. Will proposed CMB involvement satisfy OSWER and OIRM requirements?
- e. Does the plan include provision for adequate data management support of CM activities?
- f. Do scheduled CM activities mesh with design reviews and other project activities and events?
- g. Does the plan reflect a solid foundation of proven CM techniques and procedures?
- h. Are the schedule and procedures for delivery, approval, and update of the plan in compliance with OSWER requirements?

SECTION 1. INTRODUCTION

States purpose of CM plan and briefly describes its contents.

SECTION 2. PROJECT ORGANIZATION

Identifies the organizational level of the PA and his/her responsibilities.

- 2a. Is the Project Administrator at a suitable level in the OSWER office structure?
- 2b. Are the PA's responsibilities clearly defined?
- 2c. Does the PA have sufficient expertise, staff, and resources to perform the required configuration management tasks?
- 2d. Is the chairman of the CMB at a suitable level in the OSWER office structure?
- 2e. Is the project adequately represented on the CMB?
- 2f. Is the experience with CM and understanding of CM convincingly described?
- 2g. Do the PA and his staff have suitable backgrounds?

SECTION 3. CONFIGURATION IDENTIFICATION

Identifies the specifications for the software products under development and describes how these specifications establish and control assessment of cost, schedule, and performance impacts. Specifies review and delivery schedule. Also describes contents and schedules of other technical documentation.

- 3a. Does the CM plan clearly identify the configuration baselines?
- 3b. Does it identify the documents that establish the baselines?
- 3c. Are the procedures for preparing and approving baseline documents clearly defined?
- 3d. If the contract is large enough to warrant a specification tree, is one included, complete and clearly presented, and does it adequately indicate the specifications in the CM process?
- 3e. Is the preparation of documentation at least as cost-effective as methods generally employed?
- 3f. Does the documentation schedule meet project requirements?
- 3g. Does the plan include an appropriate numbering scheme for the software products and documents produced?

SECTION 4. CONFIGURATION CONTROL

Defines procedures for control of product configuration identification and for processing changes to configuration items. Includes control of technical interfaces between the PA and OSWER.

- 4a. Does the CM plan include an adequate change control system for Class I and II changes?
- 4b. Is a method provided for controlling the interfaces between elements of the software product during development and testing?
- 4c. Does the plan identify methods for complying with OSWER requirements for controlling interfaces with external software and hardware items?
- 4d. Is the change control process clearly described, with flow charts and sample forms?

SECTION 5. CONFIGURATION STATUS ACCOUNTING

Describes recording and reporting procedures and forms to be used for configuration status accounting. Defines any automated methods to be used in status reporting.

- 5a. Does the CM plan identify the data required for configuration status accounting and the methods for recording it?
- 5b. Does it identify the status accounting reports required and state their frequency and distribution?
- 5c. Is integration of subcontractor data included in the status accounting procedure?
- 5d. Are adequate forms for recording and reporting of status accounting data included?

SECTION 6. SOFTWARE CONTROL

Describes techniques and facilities for project software control as well as procedures for safe storage of master copies. Identifies responsibility for withdrawal and changing of copies. Describes reproduction and destruction capability, library services, protection against physical loss and damage, disaster file, and purging policy.

- 6a. Is an adequate procedure described for storage and physical control of software products and documents?
- 6b. Is an adequate procedure described for release of software products and documents into a controlled environment?

SECTION 7. REVIEWS AND AUDITS

Describes plans for conducting or supporting reviews and audits over the software development cycle. Defines products and documents to be reviewed or audited, reviewing authority, method for handling deviations or waivers, change procedures and forms, and numbering changes. Discusses relationship of reviews and audits to development cycle, with focus on tracking, correlation, and completeness of reviews.

- 7a. Does the CM plan describe the relationship of design and configuration reviews and audits to the configuration process?
- 7b. Are the software products and documents required for reviews and audits identified?

- 7c. Are the procedures for conducting reviews and audits defined?
- 7d. Does the plan provide for minutes of the reviews and audits and define the procedure for submittal and approval of the minutes?
- 7e. Is a method defined for using review and audit results to update the software products and documents?
- 7f. Will the review and audit approach described be flexible enough to accommodate major action items?
- 7g. Will the project review and audit personnel adequately represent the interests of the project personnel?

SECTION 8. SUBCONTRACTOR CONTROL

Defines proposed methods for control over subcontractors, insofar as control impacts project CM commitments to OSWER. Explains methods used to determine subcontractor's CM capability. Establishes requirements for performance, testing, and quality of the subcontract software products and documentation.

- 8a. Are proposed subcontractor relationships adequate to meet customer requirements?
- 8b. Is provision made for control and integration of subcontractor technical data?
- 8c. Are procedures adequate for change control of subcontractor products and documentation?

G L O S S A R Y

OSWER

**Life Cycle Management
and
Configuration Management**

Life Cycle and Configuration Management

GLOSSARY

ADP - Automated Data Processing

Acceptance Testing - Formal testing to determine that an AIS is satisfactory for use in the operating environment.

Acquisition - The process of acquiring software and hardware for an AIS.

Acquisition Strategy - The procedures and timing, including phased funding and identification of budget categories, to be followed in acquiring an AIS.

AIS - Automated Information System

Allocated/Design Baseline - The AIS baseline established by system, program, and test specifications; usually the second baseline in an AIS project, coming at the end of system design.

Allocated/Design Audit - the detailed examination of the documentation items to be developed during the definition and design phase of the AIS.

Annual Continued Operation - The one-year authorization by the Steering Committee for use of the AIS. The authorization is granted after review of the continued need for and of the on-going performance of the AIS.

Audit - Examination of software and documentation products to verify that they conform to specifications.

Automated Information System (AIS) - The aggregate of personnel, procedures, equipment, software, data, communications, maintenance, training, and support, using automated data processing equipment, through which an ongoing information task is accomplished.

Baseline - The configuration of an AIS as defined by the accepted and approved requirements documents, specifications, user and maintenance manuals, training materials, test plans and reports, data element definitions, and software. See:

- Functional Baseline
- Allocated/Design Baseline
- Product Baseline
- Operational Baseline

CMB - Configuration Management Board

Certification Testing - Formal testing to certify that an AIS meets all contract provisions prior to contract sign-off.

Change - In configuration management, any alteration, deletion, or addition to a configuration item.

Class I - The category of change which must be approved by the Configuration Management Board before its implementation. Within OSWER, Class I changes are those which:

- o Increase cost or schedule,
- o Cause changes in test provisions,
- o Involve interfaces,
- o Change system timing or storage requirements,
- o Reduce or degrade capability,
- o Impact privacy, security, or validity, or
- o Impact organizational matters.

Class II - The category of change which does not satisfy the criteria for Class I but which must be reflected through some part of the hierarchy of configuration items in order for the AIS to be properly operated and maintained.

Class III - These are technical changes which involve modifications of a configuration but which do not change the controlled characteristics of the configuration item.

CM - Configuration Management

CM Plan - Configuration Management Plan

Concept Development - The AIS LCM phase which follows Project Initiation and produces feasibility information and economic analyses to permit the Steering Committee to choose which answer to the mission need will be pursued.

Configuration Audit - Detailed review by a Configuration Management Board of a configuration item or baseline to assure that the actual functional and physical state of each complies with all approved documentation.

Configuration Change Control - The evaluation, coordination, and approval by the Configuration Management Board of proposed changes to a baseline.

Configuration Management Board (CMB) - The board, appointed by the Steering Committee, which oversees AIS configuration management and provides the Steering Committee with appraisals of project documentation.

Configuration Identification - The process of defining and documenting measurable characteristics of hardware, software, and documentation, including all linkages, of a configuration item.

Configuration Management - The rigorous methodology to assist a project in controlling the total development of an AIS.

Configuration Management Plan - A plan for the controlled development of an AIS; including procedures and control points for each CM activity.

Configuration Status Accounting - The recording and monitoring of the status of all configuration items and baselines and all changes to them.

Contractor - Private contractor or intra-Government organization performing AIS definition, design, development or implementation for OSWER.

Cost-Effective - The concept that low cost must be examined against total value of a system over the entire life of its use.

Critical Review - Examination in detail of the performance of a completed and tested configuration item.

DAA, OSWER - Deputy Assistant Administrator, OSWER

Data Element Dictionary (DED) - A formal repository of definitions of all AIS entities, in which an entity is defined as a data base class, element, or attribute; an algorithm or system utility; a software program or identifiable part of a program (module); a subsystem; a test plan or specification; a software specification; a manual; a change request or authorization; a change summary; or any other entity or characteristic deemed important by the system developer.

Definition and Design - The third AIS LCM phase, in which the AIS constraints, parameters, and characteristics are fully defined and the AIS is designed to meet them.

Desirable AIS Features - Those features which are good and valuable but which are neither necessary nor essential.

Document Change Request - A formal request to incorporate a change to a controlled AIS document.

EA - Economic Analysis

Economic Analysis - The process, as defined in Federal Information Processing Standard 38 (FIPS PUB 38), which analyzes the cost to acquire and operate an AIS over its projected life and compares that cost with the probable cost of performing the mission element needs function without the AIS.

Enhancement - The addition of capabilities to an existing AIS.

Essential AIS Features - Those without which an AIS cannot function, such as a computer of a given capacity.

Federal Information Processing Standards Publications (FIPS PUBS) - These are the official publications within the Federal government used for establishing new standards and making changes or updates to existing standards for computer hardware, software, applications, and data administration.

Functional Baseline - The baseline established for an AIS by functional, data, and information requirements documents; usually the first formal baseline in AIS development.

Functional Requirements Audit - The formal examination of each configuration item to verify that the performance specified in the system specifications has been achieved.

Functional Requirements - The defined set of input and output requirements which an AIS must meet to satisfy its purposes.

IMC - Information Management Coordinator

Information Management Coordinator - The designated individual in an OSWER organization with responsibility for the AIS activities of the organization.

IMS - Information Management Staff

Information Management Staff - The OSWER office responsible to the Assistant Administrator for technical oversight of OSWER ADP activities.

Information Management Steering Committee - The committee chaired by the DAA, OSWER, and made up of the Directors of the OSWER program Offices and of Information Management Staff, which determines long-range OSWER ADP policy and is the LCM authority.

Interface - Any dependent connection between separate parts of an AIS, between an AIS and other systems, or involving data communications.

Interoperability - The ability to pass data or information from one system to another.

Item Review - A review conducted by configuration management prior to critical review of a configuration item for the purpose of providing a higher level of confidence that the final configuration will be acceptable.

Hardware - AIS processors, terminals, communication devices, and peripheral equipment.

LCM - Life Cycle Management

LCM Phase - Divisions of an AIS life cycle corresponding to required LCM decision points.

Life Cycle - The sequence of events and actions beginning with perception of a need and continuing until phase-out, through which a system is designed, developed, implemented, and used.

Life Cycle Management - The management decision methodology by which organizations determine the need for systems and decide upon system evolution, growth, and elimination.

Logistics - The support in terms of material, facilities, maintenance, personnel, and training required to enable an AIS to function.

Mandatory AIS Requirements - Those which originate in legislation, court decisions, Federal regulations, or the Office of the Administrator.

Manuals - Those documents which support the users of an operational AIS. Three groups of users are usually provided with manuals appropriate to their individual functions: system operators, programmer/analysts involved in software maintenance and end users of the system and its outputs.

MENS - Mission Element Needs Statement

Mission Element Needs Statement - A statement of problems to be resolved by development of an information system.

Modifications - Changes to an AIS which do not result in added capabilities.

Module - A separately identifiable segment of software which performs a specifiable function.

Necessary AIS Features - Those without which an AIS would have to function in a different, perhaps less effective manner, but which could be compensated for at some cost in system performance.

Need - A requirement that an ongoing information task be performed to satisfy an OSWER mission.

Operating Environment - The actual OSWER personnel, policies, practices, procedures, facilities, and organization within which an AIS must function.

Operational Baseline - The AIS baseline established by the updated software and documentation as the AIS used in the operational environment.

Operational Life - The period during which an AIS is in use.

OSWER - The EPA Office of Solid Waste and Emergency Response.

Parameter - An attribute which defines an AIS characteristic.

Pilot Development - Proving an AIS's readiness for full implementation by first operating a scaled-down version in an OSWER operating environment.

Physical Configuration Audit - An audit conducted by the OSWER CMB to determine that the fully developed AIS conforms in all respects with its specifications, tests, and requirements documentation.

Preliminary Review - A courtesy review provided by configuration management personnel to give developers an objective review of development efforts, particularly as they affect configuration items and baselines.

Problem Resolution Summary - A brief document informing the Configuration Management Board of actions taken and their results in response to a problem with an AIS.

Privacy - OSWER provisions to prevent unauthorized access to or any disclosure of personal information as defined by the Privacy Act, EPA policy, or ethical considerations. The provisions apply to EPA personnel, other Government personnel, contractors, and the public.

Private System - (Also called "Fugitive system") an AIS developed outside Steering Committee cognizance.

Product Baseline - The AIS baseline established by all final project documentation and software.

Product Configuration Audit - A technical audit of the results of baseline testing and test data.

Program Specification - A subset of the system or subsystem specification for an individual computer program.

Project Administrator - The official who manages the accomplishment of the project under the authority of the IMC.

Project Initiation - The first LCM AIS phase, in which an OSWER Office formally identifies a need for an information system and the Steering Committee authorizes project continuation. The principal products of this phase are a Mission Element Needs statement and a preliminary plan for managing the project.

Project Management Plan - The PA's or the contractor's plan for accomplishing the project.

Project Manager - Within OSWER, the Project Administrator.

Prototype Development - A method of AIS development in which design, specifications, software, and documentation are developed concurrently. OSWER considers prototype development incomplete if any of the concurrent elements are missing.

Quality Assurance - The part of AIS management that ensures that appropriate and accepted standards are met in development of an AIS.

Requirement - Often synonymous with "need"; an internally or externally generated set of actions which must be performed to meet an OSWER mission.

Risk Analysis - Analysis of the susceptibility of an AIS to improper use or unauthorized access.

SDP - System Decision Paper

SDP I - SDP issued at the conclusion of the AIS Concept Development phase.

SDP II - SDP issued at the conclusion of the AIS Definition and Design phase.

SDP III - SDP issued at the conclusion of the AIS Development phase.

SDP IV - SDP issued annually to document the Steering Committee decision to continue use of the AIS or phase it out.

Security - OSWER provisions to prevent unauthorized access to or any inadvertant or improper disclosure of data or information classifiable as "sensitive" or "confidential" under EPA policy.

Software Change Request - A formal request to incorporate a change to controlled AIS software.

Software Control - the establishment and maintenance of a secure location for all computer source code associated with the AIS.

Software Trouble Report - A document generated by a user, operator, or maintainer requesting that the Configuration Management Board require investigation and resolution of a problem with the software of an AIS.

Steering Committee - The Information Systems Steering Committee.

Stress - The provisions in software testing that demonstrate the ability of the AIS to function in conditions of highest expected volume, system degradation, partial outage, or other possible extreme conditions.

Subsidiary AIS - An AIS adjunct to or contained within a hierarchically superior AIS.

System Change Request - A request for a change to any AIS, presented by the Project Administrator to the Configuration Management Board.

System Decision Paper - The document which contains background information to support a Steering Committee AIS phase decision; this document is initially prepared by the PA and serves as authority to proceed after Steering Committee approval.

System Development - The AIS LCM phase in which the AIS software and documentation are produced and tested in full operational configuration.

System Specification - The document detailing the precise operating parameters and constraints of an AIS.

Task Order - A separately identified work effort under a master contract or agreement.

Test Plan - The document containing the procedures, descriptions of test software, and acceptable performance criteria to prove that an AIS or its subsystems fully satisfy their specifications.

Test Specification - The specification that implements a test plan.

UAC - Users Advisory Committee

Update - To revise data, software, or documentation to reflect current status.

User/Sponsor - The OSWER Office which is the principal user of an AIS and which determines the AIS functional and operational requirements.

Users Advisory Committee - The committee which represents Regional interests in OSWER ADP planning.

Walkthrough - A demonstration, using documentation, procedures, and software appropriate for a particular AIS stage of development, conducted with representative User personnel as participants, to determine that the AIS will function as required and specified in the OSWER environment.

APPENDIX



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

FEB 25 1986

OFFICE OF
SOLID WASTE AND EMERGENCY RESPONSE

MEMORANDUM

SUBJECT: Initiation of Configuration Management Boards for Automated Information Systems in OSWER

FROM: *Jack W. McGraw*
Jack W. McGraw
Deputy Assistant Administrator

TO: OSWER Office Directors

ATTN: Information Management Coordinators: See Below

This memorandum establishes configuration management (CM) boards for RCRA, CERCLA, and cross-cutting automated information systems (AIS's) in OSWER. The boards will be responsible to the OSWER Information Management Steering Committee for proper configuration management of the AIS's.

NEED FOR THE CM BOARDS

OSWER is making major investments in AIS and equipment. Our programs are expected to grow by large orders of magnitude. We cannot achieve the results we seek without cost-effective automated support. Our use of CM is consistent with the Federal Information Processing Standards Publications (FIPS PUBS) as specified in OMB Circular A-130. It is a standard tool used throughout the Federal Government, civilian, and military services, for guiding the development and maintenance of large and small AIS's.

SCOPE OF ACTIVITIES

CM is a rigorous process with the objective of ensuring that all components of an AIS are fully defined in terms that can be examined, measured, and verified. CM provides a formal management structure, process, and procedure for controlling changes to an AIS. CM requires that any changes to the AIS be well defined along with identification of the impacts of these changes and how they will be handled.

OSWER currently is working with CM interim guidance which is being revised based on comments from your respective offices. The scope of activities for CM boards includes implementation of CM guidance for major OSWER systems, e.g., HWDMS, RCRIS, CERCLIS, ORMS, and OASIS; as well as other mission critical systems in each Program Office. The CM boards will not review systems on personal computers except where these systems are critical to the fulfillment of the mission of the office or OSWER.

Initially, there will be three CM boards in OSWER. One will be for RCRA and RCRA enforcement AIS's; one for CERCLA and CERCLA enforcement AIS's; and one for cross-cutting administrative AIS's. Cross-cutting administrative systems are those that serve all OSWER office functions regardless of legislative or regulatory mandate under RCRA and CERCLA. These systems support such functions as finance, budget, contracts, property, correspondence control, and general office automation.

The Project Administrator (PA) for each AIS will establish and maintain technical baselines for new or existing AIS's. Baselines are collections of information describing the technical characteristics of each computer system, e.g., design, performance, test results, user results, etc. Each CM board will review the PA's baselines and authorize proposed changes to them as the system evolves over time.

CHARTERS

Each CM board will have a charter that describes the authority, scope, membership, decision-making process, and recordkeeping procedures necessary to support its operations. A sample charter is attached to this memorandum.

DUTIES AND RESPONSIBILITIES

The duties and responsibilities of the CM boards are described in detail in the interim OSWER guidance on Configuration Management, Section 2.2, page II-11 to II-23. Additional copies of the CM guidance are available from Dan Yurman, IMS/OPBPM, 475-6754.

ORGANIZATION MEETINGS

Organizational meetings will be held at the call of the Chairperson for each CM board.

Attn: Jeff Byron - OERR
Steve Levy - OSW
Kate Bouve - OWPE
Art Pergam - OUST
Burnell Vincent - GWTF

cc: Ed Hanley, OIRM
Mike McNeill, OPBPM
OSWER Division Directors

CONFIGURATION MANAGEMENT BOARD

SAMPLE CHARTER

AUTHORITY

The Configuration Management Board (CMB) is established under the authority and mandate of the OSWER Information Management Steering Committee (SC).

GOAL

The goal of OSWER configuration management policies and procedures is to provide technical assurance that each OSWER automated information system (AIS) supports the programmatic functions for which it is intended throughout its life cycle, from initiation through termination.

SCOPE

All OSWER mission critical, major, sensitive, or cross-cutting AIS's are under the jurisdiction of the CMB.

MEMBERSHIP

"Standing members" of each Board will be as follows:

RCRA CMB — RCRA Information Management Specialist, Information Management Staff (IMS); Information Management Coordinator, Office of Solid Waste (OSW); Information Management Coordinator, Office of Waste Programs Enforcement (OWPE); and, Chief, System Development Branch, Office of Information Resources Management (OIRM).

CERCLA CMB — CERCLA Information Management Specialist, IMS; Information Management Coordinator, Office of Emergency and Remedial Response (OERR); Information Management Coordinator, OWPE; and, Chief, System Development Branch, OIRM.

Administrative (Cross-cutting) CMB — Information Management Specialist for Administrative (Cross-cutting) Systems, IMS; Information Management Coordinators from each OSWER Program Office (OSW, OWPE, OERR, Office of Underground Storage Tanks, and the Hazardous Waste Ground Water Task Force); PRIME System Administrators from each OSWER Program Office; and a representative from the appropriate office in OIRM.

Each Board is chaired by the IMS representative.

Each CMB may appoint ad hoc membership, representing specific AIS constituencies, by consensus.

MEETINGS

Meetings will be called as necessary by the Chairperson or upon the request of any member.

RESPONSIBILITIES

The CMB is responsible for reviewing and certifying to the IM Steering Committee that:

- o the specifications for the system "environment" e.g., hardware, software, telecommunications, and documentation, are defined;
- o changes to the system environment are described and have an acceptable impact on the system's operation; and,
- o the system performs properly, in a manner consistent with the documented specifications.

CERTIFICATIONS

A majority of the Board members must be present for any certification. All CMB certifications are given with majority assent of both standing and AIS-specific ad hoc members. Minority dissent may be presented to the SC in writing under the signature of dissenting members.

CONFIGURATION MANAGEMENT

