

## Acquisition Management Policy - (10/2020)

---

- [4 Policy for Critical Lifecycle Management Functions and Disciplines](#) Revised 1/2012
  - [4.1 Configuration Management](#)
    - [4.1.1 Scope](#) Revised 1/2008
      - [4.1.1.1 Configuration Identification](#)
      - [4.1.1.2 Configuration Status Accounting](#)
      - [4.1.1.3 Configuration Control Boards](#)
      - [4.1.1.4 Commercial Off-The-Shelf, Non-Developmental Items, and Commercially Available Software](#)
    - [4.1.2 Application](#) Revised 1/2008
    - [4.1.3 Structure and Responsibilities](#) Revised 11/2009
    - [4.1.4 Activities](#) Revised 11/2009
    - [4.1.5 Commercial Off-The-Shelf, Non-Developmental Items, and Commercially Available Software](#) Revised 1/2008
    - [4.1.6 Local Changes](#) Added 1/2008
    - [4.1.7 Operational Configuration Management Policy](#) Added 1/2008
    - [4.1.8 Mission Support IT CM for Enterprise Data Centers and Other IT Facilities](#) Added 1/2008
  - [4.2 Reserved](#) Revised 10/2020
  - [4.3 Integrated Logistics Support](#)
    - [4.3.1 Principles](#) Revised 4/2013
    - [4.3.2 Standard Elements of Integrated Logistics Support](#) Revised 10/2007
    - [4.3.3 Logistics Management During the AMS Lifecycle](#) Revised 10/2007
      - [4.3.3.1 Service Analysis](#) Added 10/2007
      - [4.3.3.2 Concept and Requirements Definition](#) Revised 4/2013
      - [4.3.3.3 Investment Analysis](#) Revised 4/2019
      - [4.3.3.4 Solution Implementation](#) Revised 10/2007
      - [4.3.3.5 In-Service Management](#) Revised 10/2007
    - [4.3.4 Who Does It?](#) Revised 10/2007
  - [4.4 Test and Evaluation](#) Revised 7/2016
    - [4.4.1 Service Analysis, Concept and Requirements Definition, and Investment Analysis](#) Revised 4/2019
    - [4.4.2 Solution Implementation](#) Revised 7/2020
    - [4.4.3 In-Service Management](#) Revised 7/2016
  - [4.5 Independent Operational Assessment](#) Revised 4/2018
  - [4.6 Deployment Planning](#) Revised 4/2009
  - [4.7 Human Factors](#)
  - [4.8 Environmental, Occupational Safety and Health, and Energy Considerations](#) Revised 4/2019
  - [4.9 Information Technology](#)
  - [4.10 System Engineering](#)
  - [4.11 Security](#) Revised 1/2019
  - [4.12 National Airspace System Safety Management System](#) Revised 1/2012
  - [4.13 Risk Management](#) Revised 4/2019
  - [4.14 Data Standardization and Management](#) Revised 7/2008
  - [4.15 Post Implementation Review and Operational Analysis](#) Revised 11/2009
    - [4.15.1 Post-Implementation Review](#) Revised 1/2020

[4.15.2 Operational Analysis](#) Revised 11/2009

[4.16 Earned Value Management](#) Revised 7/2016

[4.16.1 Program EVM Requirements](#) Revised 7/2016

[4.16.2 Contractor EVM Requirements](#) Revised 7/2016

[4.16.3 Contractor Management Control System Certification](#) Revised 2/2015

---

## **4 Policy for Critical Lifecycle Management Functions and Disciplines Revised 1/2012**

Sound acquisition management requires that service organizations integrate and manage many critical functions and disciplines working to the common purpose of fielding high-quality, trouble-free products and services. These disciplines vary, depending on the type of investment program, but typically include configuration management, real property, integrated logistics support, test and evaluation, independent operational assessment, deployment planning, human factors, environmental, occupational safety and health, and energy considerations, information technology, systems engineering, security, system safety management, risk management, and data standardization. The following specific policy requirements apply to these functional disciplines. FAST contains additional guidance.

### **4.1 Configuration Management**

#### **4.1.1 Scope Revised 1/2008**

Configuration management applies to all systems, sub-systems, equipment, components, and assets captured in the FAA Enterprise Architecture. This includes all NAS and Mission Support information technology hardware, software, firmware, documentation, interfaces, standards, test and support equipment, facility space, spares, training and courseware, and manuals.

Configuration management begins with the baselining of requirements documentation and ends with decommissioning of physical assets or the termination of services. Before introducing new equipment or software, the responsible solution provider must prepare a change proposal and have it approved by the appropriate configuration control board. This is required for expenditure of both operations and facilities and equipment funding. Configuration management of FAA systems and equipment complies with all agency safety and security requirements. Detailed lifecycle configuration management policy and procedures are in [FAA Order 1800.66](#).

##### **4.1.1.1 Configuration Identification**

Service organizations, regions, and other solution providers must identify configuration items and must develop appropriate configuration documentation to define each configuration item. This activity includes the development of a product top-down structure that summarizes the total units and configuration documentation for the system or configuration item, and the assignment of unique identifiers, which identify units, and groups of units, in a product. Configuration identification and product information must be maintained and readily available to all FAA decision-makers. Baselined documentation must be provided to the appropriate program, service organization, or national program support library, and must be maintained with all necessary links to the CM information management system. To ensure configuration management information is available to all decision-makers and CM practitioners in the FAA community, the central configuration management authority must be responsible for providing the necessary facilities and electronic tools to document, monitor, and CM information in the NAS.

##### **4.1.1.2 Configuration Status Accounting**

Service organizations, regions, and other solution providers must develop and maintain

configuration information for their configuration items or products in a systematic and disciplined manner in accordance with this policy and national configuration management process and procedures. Status accounting information includes developing and maintaining site configuration data, and the incorporation of modification data on systems and configuration items. This configuration information must be available for use by decision-makers over the lifecycle of the product.

#### **4.1.1.3 Configuration Control Boards**

A configuration control board with an approved charter and operating procedures will be the official FAA-wide forum used to establish configuration management baselines and to approve / disapprove subsequent changes to those baselines. Proposed changes to configuration management baselines must be submitted to the appropriate configuration control board on the FAA-approved case file - NAS Change Proposal (NCP) form. A configuration control board must document its approval / disapproval decision on the FAA-approved configuration control decision form.

#### **4.1.1.4 Commercial Off-The-Shelf, Non-Developmental Items, and Commercially Available Software**

After FAA acceptance, Commercial Off-The-Shelf (COTS), Non-Developmental Items (NDI), and Commercially Available Software (CAS) systems must be maintained under configuration control. This control must entail the management of a performance specification, and a data package, if available. Control will require the establishment and maintenance of records indicating the version of COTS / NDI / CAS at specific locations. When identifying COTS as a proposed solution, Service organizations and other solution providers must analyze and consider the impacts of vendor modification of COTS / NDI / CAS products during vendor production and routine vendor maintenance. Appropriate constraints and notification requirements of vendor changes must be incorporated into purchase agreements to enable management of product changes to the maximum extent possible.

#### **4.1.2 Application Revised 1/2008**

A configuration control board with an approved charter and operating procedure is the official agency-wide forum for establishing configuration management baselines and approving or disapproving changes to those baselines. Configuration control board charters and operating procedures record board membership and the programs and configuration items managed by the board. Proposed changes and associated decisions to configuration management baselines are submitted to the appropriate configuration control board on the appropriate agency-approved form.

#### **4.1.3 Structure and Responsibilities Revised 11/2009**

FAA configuration management has an enterprise-wide, multi-layer structure with each layer managing an increasing level of detail. The specific responsibilities of each layer are as follows:

#### FAA Configuration Management Authority:

- Coordinates the development and establishment of FAA configuration management policy, processes, and guidance;
- Assists lines of business, staff offices, service organizations, service areas, and other solution providers with development of CCB charters and operating procedures;
- Provides training, facilities, and electronic tools to document, monitor, and report configuration management information;
- Maintains a mechanism for assigning hardware names, asset tags, and identifiers for systems, interface documentation, and system documentation;
- Make accessible the NAS-MD-001, NAS Master Configuration Index Subsystem Baseline Configuration and Documentation Listing, using data available from the CM information management system. All configuration control boards follow the direction of the FAA Configuration Management Authority regarding the type, content, and availability of information in the information management system to ensure validity of data in NAS-MD-001.

A cross-functional team comprised of senior managers advises the Configuration Management Authority, serves as forum for addressing and resolving issues, and assists in the implementation of configuration management policy and solutions.

#### NAS Configuration Control Board:

- Controls changes to NAS systems and associated documentation not assigned to a lower-level CCB or not identified for control by the Joint Resources Council;
- Baselines Interface Requirements Documents and controls non-FAA or non-baseline system interfaces to the NAS;
- Approves service organization, service area, and other solution provider CCB charters and updates;
- Resolves problems regarding NAS system requirements among service organizations or other solution providers;
- Approves changes to NAS technical documentation and ensures traceability of requirements from the NAS level to the system and subsystem level;
- Manages changes to the final program requirements document, and notifies the investment decision authority if those changes affect cost, schedule, or performance.

#### Service Organization Configuration Control Boards:

- Approve or disapprove proposed changes to configuration items under their purview for the lifecycle of the configuration item;
- Ensure all changes have been fully analyzed and coordinated with all organizations affected by the change;
- Refer to the NAS Configuration Control Board proposed changes that exceed their approval authority;
- Establish functional, allocated, product, and operational baselines for all NAS systems;
- Manage the site configurations of FAA facilities in accordance with FAA-STD-058, FAA Standard Facility Configuration.

#### Service-Area Configuration Control Boards:

- Control changes to facility equipment layout drawings, critical power panel designations, and unique regional equipment, as identified in their charters;
- Regularly validate the accuracy of baselined facility space and power panel documentation.

The service-area configuration management plan identifies the facilities that are subject to verification and audit and specifies the audit interval. The plan also documents the configuration management program, including the methodology and processes used to accomplish service-area configuration management tasks.

Mission Support Information Technology Configuration Control Board:

- Manages Mission Support information technology systems and associated documentation not assigned to a lower-level CCB or not identified for control by the Joint Resources Council except for data exchange standards;
- Baselines Interface Requirements Documents to Mission Support systems;
- Approves line of business staff office and other solution provider CCB charters and updates;
- Approves changes to Mission Support information technology technical documentation and ensures the traceability of requirements;
- Baselines the final program requirements document or specification.

Mission Support Line of Business Staff Office or Solution Provider Configuration Control Boards:

- Approve or disapprove proposed changes to configuration items under their purview for the lifecycle of the items;
- Ensures all changes are fully analyzed and coordinated with all organizations affected by the change;
- Refers changes to the Mission Support IT CCB proposed changes that exceed their approval authority;
- Establish functional, allocated, product and operational baselines for all Mission Support systems. This includes establishing and documenting site configurations, including as-built equipment layout drawings and critical power panel designations, and creating baseline documentation for FAA information technology facilities.

NAS and Mission Support Information Technology Acquisition-Level Configuration Management:

Service organizations, LOB staff offices, and other solution providers charged with providing solutions to Enterprise Architecture requirements do the following:

- Establish, implement, and maintain configuration management plan(s) that document the configuration management program, including the methodology and processes used to accomplish configuration management tasks;
- Include requirements for configuration management planning, process, procedures and products in all acquisition contracts;
- Document transition plans and activities for field organizations; and
- Manage the lifecycle of configuration items and associated baseline documentation, which may include training material, courseware, and logistics support documentation assigned to them.

#### 4.1.4 Activities Revised 11/2009

FAA lines of business, staff offices, service organizations, service areas, and other solution providers develop the infrastructure, processes, and documentation necessary to conduct the following configuration management activities:

**Planning and Management:** Plan, coordinate, document, and manage all tasks necessary to manage the configuration of assigned enterprise architecture products throughout all phases of the lifecycle management process. A configuration management plan formalizes processes and procedures and roles and responsibilities, and ensures continuity of configuration management practices at all levels of management.

**Configuration Identification:** Identify the configuration items of the total product and develop documentation to define each. This activity includes development of a top-down configuration management structure for the product, and the assignment of unique identifiers for the units and groups of units in the product. Configuration identification and product information is maintained and be readily available to all FAA decision-makers.

**Baseline Management:** Establish and maintain a configuration baseline that represents technical aspects of approved product requirements. Baselined documentation is maintained by the appropriate line of business program office, staff office, or service organization, and is accessible in a secure environment through the program support library.

**Configuration Change Management:** Identify, document, coordinate, evaluate, and adjudicate proposed changes to a configuration baseline. Approved changes are documented, implemented, verified, and tracked to ensure incorporation into all impacted assets and their support infrastructure.

**Configuration Status Accounting:** Capture, store, and access the configuration information needed to manage products and product information. Configuration information must be electronically available for use by decision-makers over the lifecycle of the asset.

**Configuration Verification and Audit:** Periodically audit operational products to ensure consistency between the product and its baseline documentation. This activity includes verification of facility baselines, the incorporation of approved modifications, and product audits after commissioning.

Information/Data Management: Manage configuration data and information according to requirements in FAA Order 1375.1, Information/Data Management Policy.

#### 4.1.5 Commercial Off-The-Shelf, Non-Developmental Items, and Commercially Available Software Revised 1/2008

Commercial off-the-shelf, non-developmental items, and commercially available software are maintained under configuration control after acceptance into use by the FAA. This control requires management of the performance specification and data package, if available, and the establishment and maintenance of records indicating the version at specific locations. When identifying COTS as

a proposed solution, FAA lines of business, staff offices, service organizations, and other solution providers must analyze and consider the impact of vendor modification of products throughout the intended service life. Appropriate constraints and notification requirements of vendor changes must be incorporated into purchase and maintenance agreements.

#### **4.1.6 Local Changes Added 1/2008**

Local changes affecting in-service baselined systems must be evaluated by the appropriate line of business, staff office, or service organization and can be authorized only by the responsible configuration control board.

#### **4.1.7 Operational Configuration Management Policy Added 1/2008**

AMS configuration management policy applies to all operational assets. Detailed operational NAS configuration management policy is in Order 1800.66, paragraph III-4. Detailed operational Mission Support IT configuration management policy is in paragraph III-4.

#### **4.1.8 Mission Support IT CM for Enterprise Data Centers and Other IT Facilities Added 1/2008**

Line of business/staff office configuration management personnel validate, on a regular basis, baselined facility space and power panel documentation for accuracy. The line of business/staff office configuration management plan identifies the baselined facilities subject to verification and audit and specifies the audit interval. The plan also documents the configuration management program, including the methodology and processes used to accomplish IT facility configuration management tasks.

### **4.2 Reserved Revised 10/2020**

### **4.3 Integrated Logistics Support**

#### **4.3.1 Principles Revised 4/2013**

Integrated logistics support is the critical functional discipline that plans, establishes, and maintains an integrated logistics support system for the lifecycle all FAA products and services. The objective is to provide the required level of service to the end user at optimal lifecycle cost to the FAA for new investment programs and the sustainment of fielded products and services.

#### **Principles include:**

*Centralized management of integrated logistics policy and guidance* with the Vice President of Technical Operations serving as the key executive and the Associate Administrator for Regions and Centers providing support

*Logistics managers within each service team* responsible for defining, documenting, obtaining, and managing integrated logistics support for service-team products and services over their lifecycle

*Logistics managers document planning for integrated logistics support in an integrated logistics support plan*

**Collaborative logistics decision-making based on business case analysis results** to achieve high performance and best value for the agency

*Integration of operations and support requirements early in the program lifecycle* using the program requirements document

*Long-term strategic partnerships with suppliers and contractors* to achieve full lifecycle support for operational assets

*Managing and integrating supply support across the agency* to improve efficiency, save money, and minimize ownership costs

*Continuously measuring logistics performance against key organizational measures* to drive corporate decisions and tactically manage logistics services

*Training and certification of logistics specialists* so the best logistics systems can be determined, implemented, and operated over the service life of operational assets

*Developing and using logistics databases and tools* to manage assets, track outages and service delays, control inventory, and identify opportunities for improving logistics support

#### **4.3.2 Standard Elements of Integrated Logistics Support Revised 10/2007**

The standard elements of integrated logistics support are:

- Maintenance planning;
- Maintenance support facility;
- Direct-work maintenance staffing;
- Supply support;
- Support equipment;
- Training, training support, and personnel skills;
- Technical data;
- Packaging, handling, storage, and transportation;
- Computer resources support.

A definition of each element is in Appendix C.

#### **4.3.3 Logistics Management During the AMS Lifecycle Revised 10/2007**

Logistics elements are addressed during each phase of the AMS lifecycle management process (service analysis, concept and requirements definition, investment analysis, solution implementation, and in-service management). This entails managing the interdependencies

among logistics elements; integrating the acquisition and lifecycle management of logistics support with the investment product or service; and adhering to the principles of supply chain management throughout.

#### **4.3.3.1 Service Analysis Added 10/2007**

The service team logistics manager analyzes support data collected on operational assets to determine logistics trends and service needs. Results are fed into service analysis by each service organization that determines and prioritizes overall service and infrastructure needs. Service analysis results across service organizations are integrated into the enterprise architecture roadmaps, which specify when highest priority service needs enter into the appropriate solution-oriented lifecycle management phase (e.g., concept and requirement definition, investment analysis, or solution implementation).

#### **4.3.3.2 Concept and Requirements Definition Revised 4/2013**

The service team logistics manager works with the CRD team to define preliminary logistics requirements and a maintenance concept of operation for the preliminary program requirements document. Preliminary requirements are not solution-specific and do not limit the search for alternative solutions to mission need.

#### **4.3.3.3 Investment Analysis Revised 4/2019**

The service-team logistics manager is a core member of the investment analysis team throughout initial and final investment analysis. During initial investment analysis, the logistics manager evaluates the maintenance concept of each alternative solution and reports implications to lifecycle support costs and benefits in the business case analysis report. Trade-off among RMA parameters (as lifecycle cost-reduction measures) is encouraged so long as minimum service performance thresholds are not breached.

During final investment analysis, the logistics manager:

Develops logistics elements for any screening information request issued by the service team in support of final investment analysis;

- Evaluates the logistics and support elements of contractor responses;
- Assists the investment analysis team in defining:
  - ILS-specific baseline measures for the acquisition program baseline or execution plan;
  - Final logistics requirements in the program requirements document;
- Detailed logistics activities and milestones in the implementation strategy and planning attachment.
- Advises on preliminary disposal planning for the asset(s) under consideration for replacement;
- Identifies activities and establishes milestones for integrated logistics support elements of the In-Service Review (ISR) checklist; and

- Tracks completion of logistics support activities prerequisite to the final investment decision.  
During competitive procurements, offerors are evaluated on the suitability of their maintenance and support plans and demonstrated ability to support other fielded systems, as well as compliance with contract technical specifications.

#### **4.3.3.4 Solution Implementation Revised 10/2007**

During solution implementation, the logistics manager verifies that contractor logistics product development and field installation are consistent with contract requirements and user needs through commissioning. The logistics manager also assists the service team in verifying that logistics-related activities in the ISR checklist are complete and the product or service is operationally suitable at the in-service decision.

#### **4.3.3.5 In-Service Management Revised 10/2007**

The logistics manager assists the service organization and its systems engineering efforts throughout in-service management in the collection and assessment of operational data for use in evaluating product or service effectiveness. These activities include:

- Tracking and evaluating RMA performance and supportability issues of fielded assets;
- Analyzing supportability issues caused by market-driven product, system, or subsystem obsolescence;
- Determining the most cost-effective means for avoiding supportability shortfalls;
- Assessing the logistics impact of obsolescence-driven product changes;
- Evaluating the impact of engineering changes, performance shortfalls, or technological opportunities on the integrated logistics support of operational products and services.

The logistics manager also participates in disposal activities of products scheduled for removal from service.

#### **4.3.4 Who Does It? Revised 10/2007**

Each line of business manages integrated logistics support for the products and services for which it is responsible. The ATO Technical Operations organization is the office with primary responsibility for logistics policy and guidance. The ARC organization provides in-house integrated supply chain management, depot support, and logistics services. The logistics manager is the focal point for logistics planning, implementation, and in-service management within the service team. The ARC logistic-element management team supports service-team logistics managers in logistics planning and management.

#### **4.4 Test and Evaluation Revised 7/2016**

Test and evaluation is planned and conducted in accordance with the guidelines, standards, and

practices found on the FAA Acquisition System Toolset (FAST) to:

- Provide essential information in support of decision-making for investment programs;
- Provide essential information for assessing technical and investment risks;
- Verify the attainment of technical performance specifications and objectives; and
- Verify and validate that systems, solutions, and capabilities are operationally effective and suitable for the intended use.

The types of test and evaluation standards and processes to be followed for each investment program are based on the milestones and decision points they support and the type of investment program. These test and evaluation standards and processes address: NAS new investment, NAS modifications, and Mission Support programs.

The high-level test strategy is defined in the implementation strategy and planning document. The program management plan specifies how the test strategy will be executed. Based on complexity and criticality, new investments may be required to deliver a test and evaluation master plan (TEMP), as indicated on the ACAT designation form. For designated investment initiatives, the TEMP provides more detail than the ISPD and the PMP on contractor and FAA test needs, scope, planning and reporting.

The test and evaluation approach, level of analysis, and test criteria are determined by reporting requirements for program milestones and decisions. The requirements that need to be verified and validated form the basis for test criteria. The risks and complexity of the system, solution, or capabilities being tested drive the scope and robustness of evaluation methods, test cases, and reporting structure.

#### **4.4.1 Service Analysis, Concept and Requirements Definition, and Investment Analysis**

**Revised 4/2019**

During service analysis, test and evaluation activities help identify and prioritize critical FAA service needs. During concept and requirements definition, test and evaluation helps to identify the best alternative solutions to those needs. During investment analysis, the criteria for testing operational effectiveness and suitability are expressed as critical performance requirements and critical operational issues in the program requirements document.

For investment programs designated to have a test and evaluation master plan a preliminary TEMP (pTEMP) is developed during initial investment analysis based on the concepts and functions documented in the preliminary program requirements document to support the initial investment decision. An initial TEMP (iTEMP) is developed during final investment analysis once program requirements are finalized and the identity of the most promising solution is known. The iTEMP describes the test program and establishes the basis for test requirements in the request for offer to industry and test costs/and schedules in the acquisition program baseline or execution plan. The iTEMP is required to support the final investment decision. The ISPD and PMP define the plan and schedule for delivery of the final TEMP (fTEMP).

#### **4.4.2 Solution Implementation Revised 7/2020**

Solution implementation activities follow documented and structured T&E processes appropriate to the systems, solutions, and capabilities being tested. Early test and evaluation activity assesses potential operational, safety, and security risks and identifies opportunities for risk mitigation. Later test and evaluation examines performance and operational readiness (suitability and effectiveness) in support of decision-makers at the production, deployment, and in-service decisions.

Each test and evaluation program consists of developmental, operational and site testing as specified in the fTEMP and associated PMP and ISPD, as well as independent operational assessment for designated programs (see AMS Section 4.5). Developmental testing verifies requirements, functional design, and integration of the system, solution, or capability. Operational testing validates achievement of operational needs, as well as the effectiveness and suitability of the solution. For deployable products site testing verifies and validates requirements, design, and suitability of the solution in the fielded environment and configuration. As part of site testing, field familiarization testing may be required to support the site operational readiness decision.

#### **4.4.3 In-Service Management Revised 7/2016**

Developmental, operational and site testing are performed in accordance with documented, structured test processes defined by each in-service management organization in accordance with FAA Orders and Acquisition Management System Policy guidance. This applies to development and implementation of all NAS and Mission Support modifications during the in-service management lifecycle phase. In-service management test processes include standard test approaches that define the phases and detailed activities to be included during testing. These processes also support/and ensure that safety risk management and information system security requirements are addressed.

#### **4.5 Independent Operational Assessment Revised 4/2018**

The FAA is committed to verifying that new solutions are operationally effective, suitable, and safe before deployment. The Chief Operating Officer, through the Vice President for Safety and Technical Training, designates solutions on which to conduct independent operational assessment. The decision to designate a solution for independent operational assessment is based on such factors as complexity, operational criticality, lifecycle cost, interoperability, and safety risk.

During the early stage of solution implementation, the Independent Safety Assessment Team identifies potential operational and safety risks and communicates them to the acquisition organization. Once acquisition test activities are complete and the solution is operational at the key site(s), the Vice President of the acquisition organization will declare in writing to the Vice President of Office of Safety and Technical Training, via the Independent Operational Assessment Readiness Declaration, the readiness of the solution to enter independent operational assessment. Independent operational assessment provides an independent determination of operational readiness in support of deployment decisions (such as an in-service decision).

#### **4.6 Deployment Planning Revised 4/2009**

Deployment planning prepares for and assesses the readiness of a solution to be implemented

into the National Airspace System. Deployment planning is part of a continuous in-service review process that begins early in the lifecycle management process, usually during the development of requirements. All programs undergo some degree of deployment planning to ensure key aspects of fielding a new capability are planned and implemented, as well as to ensure the deployment does not create a critical deficiency in the National Airspace System. The level of authority for deployment readiness assessment and in-service decision (ISD) may vary from the service organization leader to the Joint Resources Council, chaired by the head of the sponsoring line of business.

The conduct of deployment planning involves coordination among and participation by many critical functional disciplines. Trade-offs among cost, schedule, performance, and benefits relative to these functional disciplines must also include the impact of deployment and implementation considerations. Deployment planning tools (such as a tailored in-service review checklist) must be used to assist in identifying, documenting, and resolving deployment and implementation issues. Methods and techniques include, but are not limited to, a tailored application of generic tools, the integration of checklist issues with other emerging issues (such as program trouble reports from test and evaluation), development of action plans for resolution of checklist and other items, and documentation of the results of issue resolution and mitigation. Consistent deployment planning must be visible in contractor "statement of work" and associated efforts. The status of deployment planning (and issue resolution) activities are briefed periodically (e.g. at service-level reviews), presented at the ISD meeting, summarized in the ISD memorandum, and audited during the post implementation review. The implementing service organization is responsible for the successful completion of deployment planning activities. The operating service organization provides guidance and technical expertise related to ISR issues or other factors that may affect the ability to deploy and support the intended service, product, or requirement. All lines of business will resolve and close their respective ISR issues.

#### **4.7 Human Factors**

Human factors are a *critical* aspect of aviation safety and effectiveness. Service organizations must assure that planning, analysis, development, implementation, and in-service activities for equipment, software, facilities, and services include human factors engineering to ensure performance requirements and objectives are consistent with human capabilities and limitations. Human factors engineering should be integrated with the systems engineering and development effort throughout the lifecycle management process, starting with concept and requirements definition and continuing through solution implementation and in-service management ([Human Factors Guidelines](#)).

#### **4.8 Environmental, Occupational Safety and Health, and Energy Considerations**

**Revised 4/2019**

FAA investment programs must comply with relevant federal, state, and local regulations, and FAA orders, specifications, and standards pertaining to environmental and occupational safety and health (EOSH) requirements, and energy and water requirements. FAA lines of business and staff offices must comply with all applicable requirements of the National Environmental Policy Act (NEPA) in accordance with the current version of FAA Order 1050.1, *Environmental Impacts: Policies and*

*Procedures.* Service organizations responsible for implementing investment programs must consider EOSH and energy and water requirements, and address them throughout the lifecycle management process in order to:

- Ensure the installation and operation of systems, equipment, facilities, and related program activities will not adversely impact personnel safety and health or the environment; and
- Ensure the acquisition program baseline or execution plan of the investment initiative reflects the schedule and cost of EOSH requirements.

Questions on the applicability of state and local EOSH requirements to federal acquisitions should be referred to the Office of the Chief Counsel for an evaluation of the supremacy clause and sovereign immunity implications.

#### **4.9 Information Technology**

Information technology represents a significant financial investment for the FAA, as well as a set of essential tools and services that support multiple FAA missions, functions, and activities. To develop, deploy, and manage information technology effectively, service organizations must apply sound information and engineering principles to the lifecycle planning and acquisition of information technology. Service organizations must also continuously involve users in the development, operation, and maintenance of information and application systems. Service area plans should leverage corporate information technology capabilities such as FAA telecommunications, emphasize the use of open systems and shared data, implement recognized information technology standards, and take advantage of economies of scale.

#### **4.10 System Engineering**

Systems engineering management is conducted and documented throughout the lifecycle management process at all levels of management and integration, from individual investment programs to the National Airspace System as a whole. At the NAS-level, systems engineering management integrates across investment programs to achieve an efficient and fully interoperable National Airspace System. At the program level, it optimizes performance, benefits, operations, and lifecycle cost.

All organizations responsible for the development, implementation, and lifecycle management of FAA investment programs must develop and institute a systems engineering management program consistent with guidance in FAST [[system engineering guidance](#)]. This includes organizations responsible for integrating investment programs into larger "system of systems" such as the National Airspace System. The systems engineering management program of each organization must apply systems engineering activities such as functional analysis, requirements management, synthesis, and validation and verification throughout the lifecycle management process, consistent with the specific functions and responsibilities of the organization.

#### **4.11 Security Revised 1/2019**

## **Introduction**

Service organizations and program offices must allow sufficient time and resources to address security laws, policies, and orders including the cost of implementing required security controls into acquired components. Security policy within the FAA is divided into information security; physical security, facility security, and personnel security; and sensitive information and personally identifiable information. There is overlap between the disciplines (for example, physical security is employed to protect classified materials), so all areas of security policy must be evaluated to ensure full compliance with the various orders and policies.

## **Information Security and Privacy Policy**

The Federal Information Security Modernization Act, 2014 (FISMA), Office of Management and Budget Circular A-130, Management of Federal Information Resources, National Institute of Standards and Technology (NIST) guidance, and other federal, departmental, and agency-level guidance and standards as amended, describe information security & privacy (IS & P) needed for all FAA information systems. FAA information systems reside in one of three domains: national airspace system (NAS), mission support/administrative, and research and development. They may consist of government-owned/managed components, contractor-owned/managed components, or combinations of these types. They are segregated into infrastructure for air traffic operations and infrastructures for information technology administrative support. The infrastructures exchange information via authorized security gateways.

FAA IS & P requirements are derived from NIST special publications and federal information processing standards. The FAA Office of Information Security and Privacy (AIS) defines and maintains the agency enterprise information security and privacy policy. Because the NAS is classified as critical infrastructure, NAS systems must comply with additional ISS requirements as defined by Air Traffic Organization Policies. These ATO policies can be found on the FAA's Website under policy and guidance and are designated with the letters "JO".

To receive a successful in-service decision, all FAA investment programs must undergo a security authorization that assesses outputs and products against mandatory security requirements. The security authorization process is defined in FAA Order 1370.121 FAA Information Security and Privacy Program & Policy. The Security Authorization Handbook details the process for compliance with ISS requirements during solution implementation and in-service management. Investment programs must consult the Information Security Guidance for System Acquisitions (ISGSA) at each planning phase of the AMS lifecycle to ensure information security requirements and related information are included in acquisition artifacts, and to ensure the investment program is on track for a successful security authorization.

## **Physical, Facility and Personnel Security Policy**

The FAA must conform with national policy related to physical security of the aviation infrastructure including leased and owned facilities, the security of all information associated with operation of the FAA and aircraft operations, and personnel security. The FAA is also obligated to protect proprietary information to which it has access. Physical security is directly applicable to

aviation industry operations and activities, and to supporting infrastructure such as communications, sensors, and information processing. FAA Order 1600.69C, Facility Security Management Program, establishes both policy and guidance for physical security.

FAA Order 1600.1, Personnel Security Program, establishes both policy and guidance for FAA personnel security. In addition, detailed guidance to implement personnel security with respect to contractors is in FAA Order 1600.72, Contractor and Industrial Security Program.

### **Classified National Security Information (CNSI) and Sensitive Unclassified Information (SUI) Policy**

In order to meet the spirit of Executive Order 13526 and 32 CFR Part 2001 to protect classified national security information from unauthorized disclosure, systems containing or processing classified data are managed by the FAA Office of Security and Hazardous Materials Safety in accordance with FAA Order 1600.2F, Safeguarding Classified National Security Information. FAA Order 1600.75 Protecting Sensitive Unclassified Information (SUI) is in effect at [https://employees.faa.gov/tools\\_resources/orders\\_notices/index.cfm](https://employees.faa.gov/tools_resources/orders_notices/index.cfm) (FAA only).

The Privacy Act of 1974 and the E-Government Act of 2002 (Public Law 107-347) mandate protection of an individual's right to privacy and the prevention of unauthorized dissemination of personal information. FAA Order 1370.121 Appendices 19-26 establishes the policy and guidance for handling Personally Identifiable Information (PII). The FAA Privacy Office will handle all privacy issues.

### **4.12 National Airspace System Safety Management System Revised 1/2012**

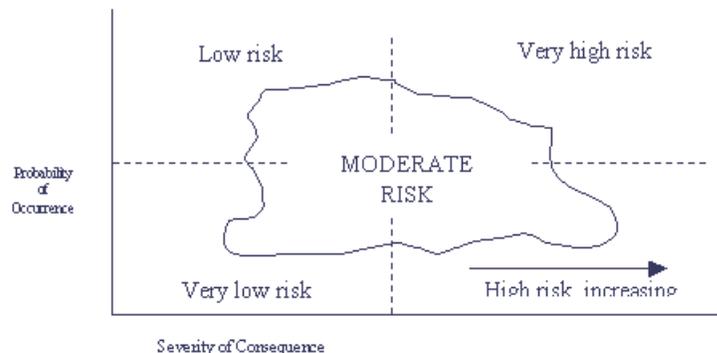
When new capital investments are determined to have an effect on the safety of the National Airspace System, safety management must be conducted and documented throughout the lifecycle of a product or service in accordance with the FAA Safety Management System (SMS). The safety management system requires use of safety risk management to identify safety risks to the National Airspace System and to conduct product development at a rigor commensurate with the severity of the resultant hazard should that product experience failure. For software-intense systems, the establishment of a development assurance program in accordance with RTCA Document (DO) 278A, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management Systems, RTCA, Inc., is one acceptable means to demonstrate that a software product was developed at the appropriate level or rigor.

Critical safety issues identified during service analysis are further addressed in: (1) an operational safety assessment; (2) a system safety assessment of alternative solutions to mission need reported in the business case; and (3) when service organizations provide program-specific safety risk management planning in the implementation strategy and planning document.

Each service organization involved in acquisition management must institute a system safety program that includes at a minimum: hazard identification, hazard classification (severity of consequences and likelihood of occurrence), measures to mitigate hazards or reduce risk to an acceptable level, verification that mitigation measures are incorporated into product design and implementation, and assessment of residual risk. Status of system safety must be presented at all decision points and investment reviews. Detailed guidelines for safety management are found in

### 4.13 Risk Management Revised 4/2019

Risk management is applied throughout the lifecycle management process to identify and mitigate risks associated with achieving FAA goals and objectives. Each line of business must institute risk management processes that: (1) identify and assess risk areas; (2) develop and execute risk mitigation or elimination strategies; (3) track and evaluate mitigation efforts; and (4) continue mitigation activity until risk is eliminated or its consequences reduced to acceptable levels.



**Figure 4.13-1 Risk Characterization**

Risk management applies to all levels of FAA activity, from small projects to large programs. It applies to such risk areas as cost, schedule, technical, system safety, all security disciplines, human factors, operability, producibility, supportability, benefits, management, funding, and stakeholder satisfaction (e.g., Congressional and aviation community priorities; union concerns). The following examples illustrate key elements of risk management:

- **Service-level risk management.** Risk management during service analysis identifies and characterizes risks to the FAA's ability to execute its legislated responsibilities and satisfy customer demands for service. Typically, these risks arise from changes in the operational environment and shortfalls in operational capability.
- **Investment analysis risk management.** Risk management during investment analysis must ensure primary risks associated with alternative solutions to mission need are identified and evaluated fully. Sufficient time and money must be included in the acquisition program baseline or execution plan of a solution selected for implementation to mitigate risk and achieve program success.
- **Program risk management.** Service organizations must apply risk management throughout the lifecycle of their products and services. The focus is on early detection and reduction of risk to avoid the greatly increased cost of dealing with the consequences of risk later in the lifecycle. Risk management planning and risk-mitigation actions are documented in the OMB Major IT Business Case and the implementation strategy and planning document. Appropriate risk management requirements and activities are also included in any prime contract for products or services. Risk management continues throughout in-service management, with the

assessment and adjustment of mitigation efforts to reduce the consequences of risk to an acceptable level.

- **Security Risk Management.** Vulnerabilities and risks within FAA programs must be reduced to acceptable levels for all identified threats that could result in quantifiable injury to personnel, loss or destruction of critical assets, or disruption of FAA information systems, including mission-critical NAS operational systems and mission support and administrative systems. Offices sponsoring or executing programs must implement and maintain lifecycle security risk management for each investment program. Lifecycle security risk management must be an integral part of program concept, planning, engineering design, and implementation, and must be maintained and modified throughout the lifecycle, as required. The methodology for quantifying and measuring asset criticality, along with identifying levels of vulnerability and risk must meet or exceed the lifecycle risk management process guidance in FAST.
- **Human factors risk management.** Human factors risk management must ensure effective human / system interaction and performance. Human issues such as usability, operational suitability, personnel and training costs, and user performance must be evaluated during concept and requirements definition and investment analysis as FAA needs are defined and alternative solutions are evaluated. During solution implementation, human factors must be fully integrated into planning and execution of the overall program to foster safe, effective human / product performance and ensure user acceptance of the final product.

#### **4.14 Data Standardization and Management Revised 7/2008**

The FAA applies data standards to facilitate data sharing across systems, programs, government agencies, and industry. Data standardization improves the transportability of data, facilitates cost-effective development and re-engineering, and improves the quality, utility, and integrity of FAA information products and resources. The FAA data management program consists of data registration, data standardization, data certification, and lifecycle data management. Policy is in FAA Order 1375.1, FAA Information and Data Management. Guidelines and tools are in FAST.

#### **4.15 Post Implementation Review and Operational Analysis Revised 11/2009**

##### **4.15.1 Post-Implementation Review Revised 1/2020**

The post-implementation review determines the following:

- Are actual costs, schedule, performance, and benefits achieving baseline expectations and if not, why not?
- Is the asset enabling the agency to provide the intended service or are changes required?
- Are there any systemic issues that need to be fixed
- Are there any process or implementation issues that need to be strengthened or improved?

The scope and content of each post-implementation review is defined in the PIR strategy submitted prior to the Final Investment Decision. The PIR may include the examination of requirements, customer feedback, and outcomes including cost, schedule, performance, strategic initiatives, and benefits. PIRs may be conducted on related investment programs intended to

achieve composite service outcomes, as directed by the Joint Resources Council or Director of the performing organization.

Prior to PIR conduct, investment programs participate in an assessment to determine the progress made in implementing the PIR strategy. This assessment is the Post-Implementation Review Data Readiness Assessment. The assessment is conducted in two parts; a self-assessment is conducted by the investment program and an independent assessment is conducted by the PIR Quality Officer or designee. The PIR Quality Officer or designee develops findings and recommendations for the assessment and works with the investment program to develop a corrective action plan to satisfy data requirements for PIR conduct.

The PIR is typically conducted 6 to 24 months after an asset first goes into operational service or as determined by the Joint Resources Council for related investment programs. The Director of the performing organization funds the review, determines the measures that comprise the review, staffs the review team, plans the review, and executes PIR processes. The Director of the performing organization develops a plan of action and milestones to address findings of the review and coordinates with the Director of the sponsoring organization, as applicable.

The PIR Quality Officer ensures the review is planned and conducted in an unbiased manner and consistent with agency standards. The PIR Quality Officer participates in PIR processes and maintains agency records of PIR strategies, data readiness assessments, plans, reports, and plans of action and milestones. Go to Post-Implementation Review Data Readiness Assessment Guidance to find out how to ensure that the PIR's data requirements will be satisfied in preparation for PIR conduct. Go to [Post-Implementation Review Guidance](#) to find out how to conduct a PIR and report results.

#### **4.15.2 Operational Analysis Revised 11/2009**

Operational analysis is the process by which FAA evaluates the ability of in-service assets to continue to provide the service for which they were procured. It answers the following questions:

- Are actual operating costs comparable to estimates in the business case analysis report?
- Is the asset operating with a sustainable design?
- Can the asset continue to meet the business needs and performance goals of the agency?
- Is the asset continuing to meet stakeholder needs?

Operational analysis consists of gathering and analyzing reliability, maintainability, and availability data (using the National Airspace System Performance Analysis System); managing supportability information to determine whether an operational asset can continue to provide the expected service for its intended life, monitoring cost data to ensure actual costs are in line with planned costs; and managing asset viability against stakeholder needs. Results are fed into the FAA's planning and investment analysis processes by the Directorate, when warranted, as a basis for determining whether an asset may need to be modernized, replaced, or removed from service. Operational analysis begins when an asset first goes operational and continues until it is removed from service. Operational analysis data is also used in the evaluation of asset readiness status. Operational analysis is the responsibility of the Directorate of the performing/service organization. Go to [Operational Analysis Guidance](#) to find out how to conduct operational

analysis and report results.

#### **4.16 Earned Value Management Revised 7/2016**

Organizations responsible for FAA capital investment programs that involve development must comply with federal regulations as required by OMB Circular A-11 and other relevant OMB Memoranda regarding earned value management (EVM) as it applies to both government and contractor development efforts regardless of contract type. The FAA uses EVM to manage development activities by providing timely, accurate, and integrated cost, schedule, and technical performance information.

EVM requirements are documented in the EVM Determination for each program by the EVM Focal Point prior to a Joint Resources Council (JRC) Investment Analysis Readiness Decision (IARD), Initial Investment Decision (IID), Final Investment Decision (FID) or Baseline Change Decision (BCD). However, the JRC may designate any program for the implementation of EVM at the program level or to any type of development contract based on an assessment of cost, schedule, and technical risk of each effort.

##### **4.16.1 Program EVM Requirements Revised 7/2016**

All FAA programs identified as major programs for reporting to OMB must establish a program management and control system using the principles of an EVMS in Electronic Industries Alliance (EIA)-748. EVM data is extracted from the management and control system and reported to DOT for submission to OMB on a monthly basis. The program EVM system must be consistent with the program management and control strategy in the JRC approved implementation strategy and planning document. The program must create the necessary program management information, including the Program level Performance Measurement Baseline (PMB) and supporting documentation for its program integrated baseline review (IBR). The program will facilitate the conduct of the IBR which will be overseen by an FAA team of subject matter experts formed and led by the EVM Focal Point as part of the oversight role.

The EVM Focal Point conducts program level surveillance on all major programs.

##### **4.16.2 Contractor EVM Requirements Revised 7/2016**

Implementation of EVM on development contract efforts is based on an assessment of cost, schedule, and technical performance risk of each contract. Implementation must be consistent with the program and contract management strategy in the implementation strategy and planning document.

Contractors are required to apply earned value management to development contracts over \$50 million and use a certified/validated EVM system (EVMS) for reporting. For development contracts between \$20 and \$50 million, the contractor management control system must comply with the EIA-748 guidelines as tailored by the program manager, contracting officer, and EVM Focal Point but a certification/validation of the contractor EVM system is not required.

The JRC may designate the application of earned value management to any development contract based on an assessment of cost, schedule, and technical risk of each contract. The contractor must provide an Integrated Program Management Report (IPMR) and participate in government led integrated baseline reviews.

The EVM Focal Point conducts contractor EVMS surveillance.

#### **4.16.3 Contractor Management Control System Certification Revised 2/2015**

The contracting officer assisted by the EVM Focal Point validates the contractor management control system as meeting contract management control requirements. The EVM Focal Point assesses contractor implementation of its management control system and monitors application to ensure compliance. Contractors not in compliance with the EVM requirements of a contract are subject to payment withholding in accordance with AMS clause 1.13-7 “Earned Value Management System – Withholding of Payment”. The EVM Focal Point determines whether a contractor requires an EVM system certification review or whether an existing certification is acceptable. The EVM Focal Point establishes agreements with other government agencies to recognize contractor EVM certifications and surveillance reports.

---